II

(Незаконодателни актове)

РЕГЛАМЕНТИ

РЕГЛАМЕНТ ЗА ИЗПЪЛНЕНИЕ (ЕС) 2016/799 НА КОМИСИЯТА

от 18 март 2016 година

за прилагане на Регламент (ЕС) № 165/2014 на Европейския парламент и на Съвета по отношение на определянето на изискванията за конструкцията, изпитването, монтирането, експлоатацията и ремонта на тахографите и техните компоненти

(текст от значение за ЕИП)

ЕВРОПЕЙСКАТА КОМИСИЯ,

като взе предвид Договора за функционирането на Европейския съюз,

като взе предвид Регламент (ЕС) № 165/2014 на Европейския парламент и на Съвета от 4 февруари 2014 г. относно тахографите в автомобилния транспорт ([1]), и по-специално член 11 и член 12, параграф 7 от него,

като има предвид, че:

(1) Регламент (ЕС) № 165/2014 въведе цифровите тахографи от второ поколение, наричани „интелигентни тахографи“, които включват свързване към глобалната навигационна спътникова система („GNSS“), устройство за връзка с цел ранно откриване от разстояние и интерфейс с интелигентни транспортни системи. Следва да бъдат създадени спецификации за техническите изисквания за конструкцията на интелигентните тахографи.

(2) Устройството за ранно откриване от разстояние, въведено с член 9, параграф 4 от Регламент (ЕС) № 165/2014, следва да предава до служител за пътна проверка данните от цифровия тахограф и информацията относно масата и масите върху осите на пълния състав от превозни средства (влекач и ремаркета или полуремаркета) в съответствие с Директива 96/53/ЕО на Европейския парламент и на Съвета ([2]). Това следва да даде възможност за ефективна и бърза проверка на превозните средства от контролните органи с по-малко електронни устройства в кабината на превозното средство.

(3) В съответствие с Директива 96/53/ЕО устройството за ранно откриване от разстояние следва да използва стандартите на CEN за DSRC ([3]), посочени във въпросната директива, в радиочестотната лента 5 795—5 805 MHz. Тъй като тази радиочестотна лента се използва за електронно таксуване за изминато разстояние, както и за да се избегнат взаимни смущения между таксуването за изминато разстояние и приложенията за контролиране, служителите на контролните органи не трябва да използват устройството за ранно откриване от разстояние на пункт за таксуване за изминато разстояние.

(4) С интелигентния тахограф следва да бъдат въведени нови механизми за сигурност за поддържане на нивото на сигурност на цифровите тахографи с цел да се преодолеят настоящите слабости по отношение на сигурността. Една от тези слабости е липсата на срокове на валидност на цифровите сертификати. За да се осигури съответствие с най-добрите практики в областта на сигурността, се препоръчва да се избягва използване на цифрови сертификати без срок на валидност. Нормалният срок на валидност на действието на бордовите устройства следва да бъде 15 години, считано от датата на издаване на цифровите сертификати на бордовото устройство. След този срок на валидност бордовите устройства следва да бъдат заменяни.

([1]) ОВ L 60, 28.2.2014 г., стр. 1.

([2]) Директива 96/53/ЕО на Съвета от 25 юли 1996 г. относно максимално допустимите размери в националния и международен трафик на някои пътни превозни средства, които се движат на територията на Общността, както и максимално допустимите маси в международния трафик (ОВ L 235, 17.9.1996 г., стр. 59).

([3]) Стандарти на Европейския комитет за стандартизация (CEN) за специализирани съобщителни системи с малък обсег на действие EN 12253, EN 12795, EN 12834, EN 13372 и ISO 14906.

(5) Осигуряването на сигурна и надеждна информация за местоположението е съществен елемент на ефективната работа на интелигентните тахографи. Следователно е целесъобразно да се гарантира тяхната съвместимост с услугите с добавена стойност, предоставяни от програмата „Галилео“ и предвидени в Регламент (ЕС) № 1285/2013 на Европейския парламент и на Съвета ([1]), за да се подобри сигурността на интелигентните тахографи.

(6) В съответствие с член 8, параграф 1, член 9, параграф 1 и член 10, параграфи 1 и 2 от Регламент (ЕС) № 165/2014 механизмите за сигурност, въведени с този регламент, следва да се прилагат 36 месеца след влизането в сила на необходимите актове за изпълнение, за да се даде възможност на производителите да разработят интелигентни тахографи от ново поколение и да получат своите сертификати за одобрение на типа от компетентните органи.

(7) В съответствие с Регламент (ЕС) № 165/2014 превозните средства, регистрирани за първи път в държава членка 36 месеца след влизането в сила на настоящия регламент на Комисията, следва да бъдат оборудвани с интелигентен тахограф, отговарящ на изискванията на настоящия регламент на Комисията. Във всеки случай всички превозни средства, експлоатирани в държава членка, различна от държавата членка на регистрацията им, следва да бъдат оборудвани с интелигентен тахограф 15 години след датата на прилагане на въпросните изисквания.

(8) В Регламент (ЕО) № 68/2009 на Комисията ([2]) се разрешава по време на преходен период, който изтича на 31 декември 2013 г., да се използва адаптер, за да стане възможно монтирането на тахографи в превозни средства тип M1 и N1. Поради технически трудности, свързани с намирането на алтернатива на използването на адаптера, експертите от автомобилния и тахографския отрасъл съвместно с Комисията стигнаха до заключението, че не съществува алтернативно решение на адаптера, което да не води до високи разходи за промишлеността, непропорционални на размера на пазара. По тази причина използването на адаптер в превозни средства от тип M1 и N1 следва да бъде разрешено за неограничен период от време.

(9) Мерките, предвидени в настоящия регламент, са в съответствие със становището на комитета по член 42, параграф 3 от Регламент (ЕС) № 165/2014,

ПРИЕ НАСТОЯЩИЯ РЕГЛАМЕНТ:

Член 1

Предмет и обхват

1. С настоящия регламент се определят разпоредбите, необходими за еднаквото прилагане на следните аспекти относно тахографите:

а) регистриране на местоположението на превозното средство в определени точки през периода на дневното работно време на водача;

б) ранно откриване от разстояние на възможна манипулация или злоупотреба с интелигентни тахографи;

в) интерфейс с интелигентни транспортни системи;

г) административните и техническите изисквания за процедурите за одобрение на типа на тахографи, включително механизмите за сигурност.

2. Конструкцията, изпитването, монтирането, проверката, експлоатацията и ремонтът на интелигентните тахографи и техните компоненти трябва да отговарят на техническите изисквания, формулирани в приложение 1B към настоящия регламент.

3. Що се отнася до конструкцията, изпитването, монтирането, проверката, експлоатацията и ремонта, тахографите, различни от интелигентните тахографи, трябва да продължават да отговарят на изискванията или на приложение 1, или на приложение 1Б към Регламент (ЕИО) № 3821/85 на Съвета ([3]), според случая.

([1]) Регламент (ЕС) № 1285/2013 на Европейския парламент и на Съвета от 11 декември 2013 г. за изграждане и експлоатация на европейските навигационни спътникови системи и за отмяна на Регламент (ЕО) № 876/2002 на Съвета и на Регламент (ЕО) № 683/2008 на Европейския парламент и на Съвета (ОВ L 347, 20.12.2013 г., стр. 1).

([2]) Регламент (ЕО) № 68/2009 на Комисията от 23 януари 2009 г. за адаптиране за девети път към техническия прогрес на Регламент (ЕИО) № 3821/85 на Съвета относно контролните уреди за регистриране на данните за движението при автомобилен транспорт (ОВ L 21, 24.1.2009 г., стр. 3).

([3]) Регламент (ЕИО) № 3821/85 на Съвета от 20 декември 1985 г. относно контролните уреди за регистриране на данните за движението при автомобилен транспорт (ОВ L 370, 31.12.1985 г., стр. 8).

4. За целите на ранното откриване на измами, съгласно член 10г от Директива 96/53/ЕО на Европейския парламент и на Съвета устройството за ранно откриване от разстояние трябва да предава също и данните за масите, предоставяни от вътрешна бордова система за претегляне.

Член 2

Определения

За целите на настоящия регламент се прилагат определенията, формулирани в член 2 от Регламент (ЕС) № 165/2014.

Освен това се прилагат и следните определения:

1) „цифров тахограф“ или „тахограф от първо поколение“ е цифров тахограф, различен от интелигентен тахограф;

2) „външно устройство за GNSS“ е устройство, което съдържа приемника на сигнали от GNSS, когато бордовото устройство не е отделно устройство, както и други компоненти, необходими за защитата на съобщаването на данни за местоположението към останалата част на бордовото устройство;

3) „информационно досие“ е цялостното досие в електронен вид или на хартия, съдържащо цялата информация, предоставена от производителя или негов представител на органа по одобряването на типа за целите на одобряването на типа на тахограф или компонент от него, включително сертификатите, посочени в член 12, параграф 3 от Регламент (ЕС) № 165/2014, както и за извършването на изпитванията, определени в приложение 1В към настоящия регламент, както и чертежи, снимки и други съответни документи;

4) „информационен пакет“ е информационното досие в електронен вид или на хартия, придружено от всякакви други документи, добавени от органа по одобряването на типа към информационното досие по време на осъществяване на функциите му, включително, в края на процеса на одобряване на типа, ЕО сертификата за одобрение на типа на тахографа или на негов компонент;

5) „указател на информационния пакет“ е документът, в който се изброява номерирано съдържанието на информационния пакет с посочване на всички части на пакета. Форматът на този документ трябва да разграничава последователните етапи в процеса на ЕО одобряване на типа, включително датите на всякакви преразглеждания и актуализации на пакета;

6) „устройство за ранно откриване от разстояние“ е оборудването на бордовото устройство, което се използва за извършването на целенасочени пътни проверки;

7) „интелигентен тахограф“ или „тахограф от второ поколение“ е тахограф, отговарящ на членове 8, 9 и 10 от Регламент (ЕС) № 165/2014, както и на изискванията от приложение 1В към настоящия регламент;

8) „компонент на тахограф“ или „компонент“ е всеки от следните елементи: бордовото устройство, датчикът за движение, тахографската карта, тахографският лист, външното устройство за GNSS и устройството за ранно откриване от разстояние;

9) „орган по одобряването на типа“ е органът на държава членка, компетентен да извършва одобряването на типа на тахографа или на компонентите му, процедурата по разрешаване, издаването и, при необходимост, отнемането на сертификати за одобрение на типа, изпълняващ ролята на звено за връзка с органите по одобряването на тип на други държави членки и гарантиращ, че производителите изпълняват своите задължения, свързани със съответствието с изискванията на настоящия регламент.

Член 3

Услуги, свързани с определянето на местоположението

1. Производителите гарантират, че интелигентните тахографи са съвместими с услугите за определяне на местоположението, предоставяни от системите на „Галилео“ и Европейската геостационарна служба за навигационно покритие (EGNOS).

2. В допълнение към системите, посочени в параграф 1, производителите могат да решат да осигурят съвместимост с други системи за спътникова навигация.

Член 4

Процедура за одобряване на типа на тахографи и компоненти на тахографи

1. Производителят или неговият представител подава заявление за одобряване на типа на тахограф или на някой от неговите компоненти или група от компоненти до органите по одобряването на типа, определени от всяка държава членка. То се състои от информационно досие, съдържащо информацията за всеки от въпросните компоненти, включително, когато е приложимо, сертификатите за одобряване на типа на други компоненти, необходими за окомплектуване на тахографа, както и всякакви други съответни документи.

2. Държавата членка издава одобрение на типа на всеки тахограф, компонент или група от компоненти, които отговарят на административните и техническите изисквания, посочени в член 1, параграф 2 или 3, според случая. В такъв случай органът по одобряването на типа издава на заявителя сертификат за одобрение на типа в съответствие с образеца в приложение II към настоящия регламент.

3. Органът по одобряването на типа може да поиска от производителя или неговия представител да предостави допълнителна информация.

4. Производителят или неговият представител предоставя на органите по одобряването на типа, както и на организациите, отговарящи за издаването на сертификатите, посочени в член 12, параграф 3 от Регламент (ЕС) № 165/2014, толкова на брой тахографи или компоненти на тахографи, колкото са необходими, за да може процедурата за одобряване на типа да се извърши по задоволителен начин.

5. Когато производителят или неговият представител има за цел одобряване на типа на определени компоненти или групи от компоненти на тахограф, той предоставя на органите по одобряването на типа другите компоненти, чийто тип е вече одобрен, както и други части, необходими за конструкцията на окомплектувания тахограф, за да могат въпросните органи да проведат необходимите изпитвания.

Член 5

Изменения на одобрения на типа

1. Производителят или неговият представител информира незабавно органите по одобряването на типа, издали първоначалното одобрение на типа, за всяка промяна в програмното осигуряване (софтуера) или апаратната част (хардуера) на тахографа или в естеството на материалите, използвани за производството му, които са записани в информационния пакет, и подава заявление за изменение на одобрението на типа.

2. Органите по одобряването на типа могат да преразгледат или разширят съществуващо одобрение на типа, или да издадат ново одобрение на типа в зависимост от естеството и характеристиките на измененията.

„Преразглеждане“ се прави, когато органът по одобряването на типа счете, че промените в програмното осигуряване или в апаратната част на тахографа или в естеството на материалите, използвани за производството му, са незначителни. В такива случаи органът по одобряването на типа издава преразгледани документи от информационния пакет, като посочва естеството на направените изменения и датата на одобряването им. За спазването на това изискване се счита за достатъчна актуализирана версия на информационния пакет в консолидиран вид, придружена от подробно описание на направените изменения.

„Разширение“ се прави, когато органът по одобряването на типа счете, че промените в програмното осигуряване или в апаратната част на тахографа или в естеството на материалите, използвани за производството му, са значителни. В такива случаи той може да изиска да бъдат извършени нови изпитвания и да информира за това производителя или представителя му. Ако изпитванията са задоволителни, органът по одобряването на типа издава преразгледан сертификат за одобрение на типа, съдържащ номер, съответстващ на издаденото разширение. В сертификата за одобрение на типа се посочват причината за разширението и датата на издаването му.

3. В указателя към информационния пакет се посочва датата на най-новото разширение или преразглеждане на одобрението на типа или датата на най-новото консолидиране на актуализираната версия на одобрението на типа.

4. Когато заявените изменения на тахограф от одобрен тип или на неговите компоненти биха довели до издаване на нов сертификат за сигурност или за оперативна съвместимост, е необходимо ново одобрение на типа.

Член 6

Влизане в сила

Настоящият регламент влиза в сила на двадесетия ден след деня на публикуването му в *Официален вестник на Европейския съюз*.

Той се прилага от 2 март 2016 г.

Приложенията обаче се прилагат от 2 март 2019 г., с изключение на допълнение 16, което се прилага от 2 март 2016 г.

Настоящият регламент е задължителен в своята цялост и се прилага пряко във всички държави членки.

Съставено в Брюксел на 18 март 2016 година.

За Комисията

Председател

Jean-Claude JUNCKER

ПРИЛОЖЕНИЕ I B

Изисквания за конструиране, изпитване, монтаж и контрол

ВЪВЕДЕНИЕ

Цифровата тахографска система от първо поколение е въведена от 1 май 2006 г. Тя може да бъде използвана до края на експлоатационния ѝ срок за вътрешен транспорт. За международен транспорт обаче 15 години след влизането в сила на настоящия регламент на Комисията всички превозни средства трябва да са оборудвани с интелигентни тахографи от второ поколение, съответстващи на изискванията, въведени с настоящия регламент.

Настоящото приложение съдържа изискванията за уредите за регистриране на данните за движението и за тахографските карти от второ поколение. Започвайки от датата на въвеждането им, уредите за регистриране на данните за движението от второ поколение се монтират в превозни средства, регистрирани за първи път, като се издават тахографски карти от второ поколение.

С цел да се насърчи безпроблемното въвеждане на тахографската система от второ поколение,

— тахографските карти от второ поколение трябва да са проектирани така, че да се използват и в бордови устройства от първо поколение,

— на датата на въвеждането не се изисква замяна на валидни тахографски карти от първо поколение.

Това ще позволи на водачите да запазят своята уникални карта на водач и да я използват и с двете системи.

Уредите за регистриране на данните за движението от второ поколение обаче се калибрират само с използване на карти за монтаж и настройка от второ поколение.

В настоящото приложение се съдържат всички изисквания, свързани с оперативната съвместимост между тахографските системи от първо и от второ поколение.

В допълнение 15 се съдържат допълнителни подробности относно управлението на съвместното съществуване на двете системи.

Списък на допълненията

1 ОПРЕДЕЛЕНИЯ

В настоящото приложение:

а) „активиране“ означава:

фазата, по време на която тахографът става напълно работоспособен и може да извършва всички функции, включително и свързаните със сигурността, чрез използването на карта за монтаж и настройки;

б) „удостоверяване на самоличността“:

функция, предназначена да установи и провери определена самоличност;

в) „автентичност“ означава:

характеристиката определена информация да произлиза от страна, чиято самоличност може да бъде проверена;

г) „вградена функция за изпробване“:

изпробвания, които могат да се пускат по заявка, задействани от оператора или от външна апаратура;

д) „календарен ден“ означава:

ден, който обхваща времето от 00.00 часа до 24.00 часа. Всички календарни дни са свързани с координираната универсална скала за време (UTC);

е) „калибриране“ на интелигентен тахограф означава:

обновяване или потвърждаване на записаните в паметта данни за параметрите на превозното средство. Параметрите на превозното средство включват параметри за неговата идентификация (идентификационен номер, регистрационен номер и държава членка, извършила регистрацията) и характеристиките на превозното средство (w, k, l, размер на гумите, настройка на ограничителя на скоростта (ако има), текущо координирано универсално време (UTC), текущо показание на километражния брояч); по време на калибриране на уреди за регистриране на данните за движението, типовете и идентификаторите на всички пломби, свързани с одобрението на типа, също трябва да се записват в паметта за данни;

всяко актуализиране или потвърждаване само на координираното универсално време се счита за сверяване на часовника, а не за калибриране, при условие че това не противоречи на изискване 409;

калибрирането на уреди за регистриране на данните за движението изисква използването на карта за монтаж и настройки;

ж) „номер на картата“ означава:

16-позиционен буквено-цифров код, който представлява уникалният идентификационен номер на тахографска карта в определена държава членка. Номерът на картата съдържа индекс за пореден номер (при необходимост), индекс за замяна на картата и индекс за подновяване на валидността на картата.

По този начин всяка карта се идентифицира от кода на държавата членка, която я е издала, и от картовия номер.

з) „индекс за пореден номер на картата“ означава:

14-ят буквено-цифров символ от номера на картата, използван за различаване на картите, издадени на даден превозвач, сервиз или контролен орган, имащи право да използват няколко тахографски карти. Превозвачът, сервизът или контролният орган се идентифицират еднозначно чрез първите 13 символа на картовия номер;

и) „индекс за подновяване на валидността на картата“ означава:

16-ят буквен или цифров символ от картовия номер, който се увеличава с едно при всяко подновяване на валидността на тахографската карта;

й) „индекс за замяна на картата“ означава:

15-ят буквен или цифров символ от картовия номер, който се увеличава с едно при всяка замяна на тахографската карта;

к) „характеристичен коефициент на превозното средство“ означава:

цифровата характеристика, която посочва стойността на изходния сигнал, излъчен от тази част на превозното средство, която го свързва с уредите за регистриране на данните за движението (изходящ вал на скоростната кутия или ос), докато превозното средство изминава разстояние от един километър при стандартни условия на изпитване, както е определено в изискване 414. Характеристичният коефициент се изразява в импулси на километър (w: … имп./km);

л) „карта на превозвач“ означава:

тахографска карта, която се издава от органите на държава членка на транспортно предприятие, което трябва да експлоатира превозни средства, оборудвани с тахограф, и която идентифицира транспортното предприятие и служи за показване, изтегляне и разпечатване на данните, съхранени в паметта на тахографа, достъпът до които е бил ограничен от съответното транспортно предприятие;

м) „константа на уредите за регистриране на данните за движението“ означава:

цифровата характеристика, която дава стойността на входния сигнал, необходим за показване и записване на изминато разстояние един километър; тази константа се изразява в импулси на километър (k = … имп./km);

н) „време за непрекъснато управление на МПС“ се изчислява от уредите за регистриране на данните за движението като ([1]):

времето на непрекъснато управление на МПС се изчислява като натрупаните времена на управление на МПС от даден водач от края на последния му период НА РАЗПОЛОЖЕНИЕ, на ПРЕКЪСВАНЕ/ПОЧИВКА или на НЕИЗВЕСТНА ДЕЙНОСТ ([2]) от 45 или повече минути (този период може да е разделен в съответствие с Регламент (ЕО) № 561/2006 на Европейския парламент и на Съвета ([3])). При изчисленията се държи сметка, ако е необходимо, за предишните дейности, записани на картата на водач. Когато водачът не е вкарвал картата си, изчисленията се основават на данните, записани в паметта по време на текущия период, през който не е била вкарвана никаква карта, като се отнасят към съответното четящо устройство;

о) „контролна карта“ означава:

тахографска карта, издадена от органите на държава членка на национален компетентен контролен орган, която идентифицира контролния орган и евентуално — конкретния негов служител, и която осигурява достъп до данните, съхранени в паметта на тахографа или в картата на водач, и евентуално — в картите за монтаж и настройки, с цел тяхното прочитане, разпечатване и/или изтегляне.

Тя следва също така да дава достъп до функцията за пътна проверка на калибрирането и до данните на четеца за връзка с цел ранно откриване от разстояние.

п) „общото време на прекъсване“ се изчислява в уредите за регистриране на данните за движението като ([1]):

общото време на прекъсване в управлението е сумата от периодите НА РАЗПОЛОЖЕНИЕ, на ПРЕКЪСВАНЕ/ПОЧИВКА или на НЕИЗВЕСТНА ДЕЙНОСТ ([2]) от 15 или повече минути на даден водач от края на последния му период НА РАЗПОЛОЖЕНИЕ, на ПРЕКЪСВАНЕ/ПОЧИВКА или на НЕИЗВЕСТНА ДЕЙНОСТ ([2]) от 45 или повече минути (този период може да бъде разделен в съответствие с Регламент (ЕО) № 561/2006).

При изчисленията се държи сметка, ако е необходимо, за предишните дейности, записани на картата на водач. Периодите на неизвестна дейност с отрицателно времетраене (начало на периода с неизвестна дейност > края на периода с неизвестна дейност) поради припокриване на времеви периоди между два различни уреда за регистриране на данните за движението не се вземат предвид при изчисленията.

Когато водачът не е вкарвал картата си, изчисленията се основават на данните, записани в паметта по време на текущия период, през който не е била вкарвана никаква карта, като се отнасят към съответното четящо устройство;

([1]) Този начин на изчисляване на времето на непрекъснато управление на МПС и на общото време на прекъсване служи в уредите за регистриране на данните за движението за изчисляване на предупреждението за времето на непрекъснато управление на МПС. Той не предопределя юридическото тълкуване на тези периоди. Може да бъдат използвани алтернативни начини за изчисляване на времето на непрекъснато управление на МПС и на общото време на прекъсване в замяна на тези определения, ако те са остарели вследствие на актуализиране на останалото законодателство в дадената област.

([2]) Периодите на НЕИЗВЕСТНА ДЕЙНОСТ съответстват на периодите, през които картата на водача не е била вкарвана в уред за регистриране на данните за движението и за които няма извършено ръчно въвеждане на дейностите на водача.

([3]) Регламент (ЕО) № 561/2006 на Европейския парламент и на Съвета от 15 март 2006 година за хармонизиране на някои разпоредби от социалното законодателство, свързани с автомобилния транспорт, за изменение на Регламенти (ЕИО) № 3821/85 и (ЕО) № 2135/98 на Съвета и за отмяна на Регламент (ЕИО) № 3820/85 на Съвета (ОВ L 102, 11.4.2006 г., стр. 1).

р) „памет за данни“ означава:

електронно устройство за съхраняване на данни, вградено в уредите за регистриране на данните за движението;

с) „електронен подпис“ означава:

данните, прибавени към блок от данни, или негово криптографско преобразуване, което позволява на получателя на този блок да получи доказателство за неговата автентичност и достоверност;

т) „изтегляне на данни“ означава:

копиране, заедно с електронния подпис, на част или на пълен набор файлове с данни, записани в паметта за данни на бордовото устройство или в паметта на тахографската карта, при условие че при този процес не се изменят или изтриват записани данни;

Производителите на интелигентни тахографи за превозни средства и производителите на оборудване, конструирано и предназначено за изтегляне на файлове с данни, трябва да предприемат всички подходящи мерки, за да гарантират, че изтеглянето на съответните данни може да бъде извършено с минимална загуба на време от страна на транспортните предприятия или водачите.

Изтеглянето на файла с подробни данни за скоростта на движение може да не е необходимо за установяване на съответствие с разпоредбите на Регламент (ЕО) № 561/2006, но може да бъде използвано за други цели, като например разследване на злополуки;

у) „карта на водач“ означава:

тахографска карта, издадена от органите на държава членка на конкретен водач, която идентифицира водача и служи за съхраняване на данни за дейността на водача;

ф) „действителна обиколка на колелата“ означава:

средната стойност от разстоянията, изминати от всяко от колелата, задвижващи превозното средство (двигателните колела) за времето на едно пълно завъртане. Измерването на тези разстояния се извършва при стандартни условия на изпитване, както е определено съгласно изискване 414, и се изразява във вида „l = … mm“. Производителите на превозни средства могат да заменят измерването на тези разстояния с теоретично изчисление, при което се взема предвид разпределението на теглото на превозното средство върху осите в състояние без товар и в готовност за движение ([1]). Методите на това теоретично изчисление подлежат на одобряване от компетентен орган на държава членка и могат да бъдат приложени само преди пускането на тахографа;

х) „събитие“ означава:

ненормално действие, отчетено от интелигентния тахограф, което може да е резултат от опит за измама;

ц) „външно устройство за GNSS“ означава

устройство, което съдържа приемника на сигнали от GNSS, когато бордовото устройство не е отделно устройство, както и други компоненти, необходими за защитата на съобщаването на данни за местоположението към останалата част на бордовото устройство;

ч) „неизправност“ означава:

ненормално действие, открито от интелигентния тахограф, което може да се дължи на нарушено функциониране или повреда на уредите;

ш) „приемник на сигнали от GNSS“ означава:

електронно устройство, което получава и обработва по цифров път сигналите от един или повече спътници на Глобална навигационна спътникова система (на английски — GNSS) с цел осигуряване на информация за местоположението, скоростта и времето.

щ) „монтиране“ означава:

монтирането на тахограф в превозно средство;

([1]) Регламент (ЕС) № 1230/2012 на Комисията от 12 декември 2012 година за прилагане на Регламент (ЕО) № 661/2009 на Европейския парламент и на Съвета във връзка с изискванията за одобрение на типа по отношение на масите и размерите на моторните превозни средства и техните ремаркета и за изменение на Директива 2007/46/ЕО на Европейския парламент и на Съвета (ОВ L 353, 21.12.2012 г., стр. 31).

ъ) „оперативна съвместимост“ означава:

способността на системите и съответните стопански процеси за обмен на данни и споделяне на информация;

ю) „интерфейс“ означава:

междусистемно устройство, осигуряващо средствата, чрез които системите могат да се свържат и да взаимодействат;

я) „местоположение“ означава:

географските координати на превозното средство в даден момент;

аа) „датчик за движение“ означава:

частта от тахографа, подаваща сигнал, който е показателен за скоростта и/или изминатото разстояние от превозното средство;

бб) „невалидна карта“ означава:

карта, която се възприема като дефектна или при която първоначалното удостоверяване на самоличността е било неуспешно, чиято дата за начало на валидността все още не е достигната или за която е изтекъл срокът на валидност;

вв) „отворен стандарт“ означава:

стандарт, който според описанието в стандартен документ за спецификация се предоставя безплатно или срещу символична такса и който всички могат да възпроизвеждат, разпространяват или използват без такса или срещу символична такса.

гг) „извън обхвата“ означава:

всички случаи, в които използването на уредите за регистриране на данните за движението не е необходимо съгласно Регламент (ЕО) № 561/2006;

дд) „превишаване на скоростта“ означава:

всяко превишаване на допустимата за съответното превозно средство скорост за време над 60 секунди, през което измерената скорост на превозното средство надвишава зададената в Директива 92/6/ЕИО на Съвета ([1]), както е последно изменена;

ее) „периодичен технически преглед“ означава:

набор от действия, извършвани, за да се провери дали тахографът работи правилно, дали неговите настройки отговарят на параметрите на превозното средство, както и дали към тахографа няма прикачени устройства за манипулиране;

жж) „печатащо устройство“ означава:

компонент на уредите за регистриране на данните за движението, който осигурява разпечатки на записаните в паметта данни;

зз) „връзка с цел ранно откриване от разстояние“ означава:

комуникация между устройството за връзка с цел ранно откриване от разстояние и четеца за връзка с цел ранно откриване от разстояние по време на целенасочени пътни проверки с цел дистанционно откриване на евентуална манипулация или злоупотреба с уреди за регистриране на данните за движението;

ии) „устройство за връзка с цел ранно откриване от разстояние“ означава:

използваното за извършването на целенасочени пътни проверки оборудване в бордовото устройство;

([1]) Директива 92/6/ЕИО на Съвета от 10 февруари 1992 г. относно монтирането и използването на устройства за ограничаване на скоростта за някои категории моторни превозни средства в Общността (ОВ L 57, 2.3.1992 г., стр. 27).

йй) „четец за връзка с цел ранно откриване от разстояние“ означава:

системата, използвана от служителите на контролните органи за извършването на целенасочени пътни проверки;

кк) „подновяване“ означава:

издаването на нова тахографска карта, когато срокът на валидност на съществуваща карта изтича или тя не функционира правилно и е била върната на органа, който я е издал; подновяването предполага гаранцията, че не могат да съществуват едновременно две валидни карти;

лл) „ремонт“ означава:

всякакъв ремонт на датчик за движение, на бордово устройство или на кабел, който налага прекъсване на неговото електрическо захранване, прекъсване на връзката с други компоненти на тахографа или отваряне на тахографа или бордовото устройство;

мм) „замяна на картата“ означава:

издаването на тахографска карта, която заменя съществуваща карта, която е обявена за изгубена, откраднатa или за неправилно функционираща и която е била върната на органа, който я е издал. Замяната води винаги до опасността едновременно да съществуват две валидни карти;

нн) „сертифициране по отношение на сигурността“:

процесът, чрез който организация за сертифициране по единни критерии удостоверява, че уредите за регистриране на данните за движението (или компонент от тях) или изследваната тахографска карта отговарят на изискванията за сигурност, формулирани в съответните профили за защита;

оо) „самоизпробване“ означава:

изпробвания, извършвани периодично и автоматично от уредите за регистриране на данните за движението с цел откриване на неизправности;

пп) „измерване на времето“ означава:

непрекъснат цифров запис на координираното универсално време и дата (UTC);

рр) „сверяване на часовника“ означава:

автоматично сверяване на текущото време през равни интервали при максимално допустимо отклонение от една минута или сверяване, извършено при калибриране;

сс) „размери на гумите“ означава:

указването на размерите на гумите (външни задвижващи колела) в съответствие с Директива 92/23/ЕИО на Съвета ([1]), както е последно изменена;

тт) „идентификация на превозното средство“ означава:

номерата, позволяващи идентифицирането на превозното средство: регистрационният номер (VRN) с указване на държавата членка, извършила регистрацията, и идентификационният номер на превозното средство (VIN) ([2]);

уу) за целите на изчисленията в уредите за регистриране на данните за движението „седмица“ означава:

период между 00.00 часа UTC в понеделник и 24.00 часа UTC в неделя;

([1]) Директива 92/23/ЕИО на Съвета от 31 март 1992 година относно гумите за моторни превозни средства и техните ремаркета, както и тяхното монтиране (ОВ L 129, 14.5.1992 г., стр. 95).

([2]) Директива 76/114/ЕИО на Съвета от 18 декември 1975 година за сближаването на законодателствата на държавите-членки относно задължителните регистрационни табели и обозначения на моторни превозни средства и техните ремаркета, тяхното разположение и метод на закрепване (ОВ L 24, 30.1.1976 г., стр. 1).

фф) „карта за монтаж и настройки“ означава:

тахографска карта, която се издава от органите на държава членка на определен за целта персонал на производител на тахографи, монтьор, производител на превозни средства или сервиз, одобрени от въпросната държава членка, чрез която се идентифицира титулярят на картата и която служи за изпитване, калибриране и активиране на тахографите и/или за изтегляне на данни от тях;

хх) „адаптер“ означава:

устройство, което подава сигнал в постоянно съответствие със скоростта на превозното средство и/или изминатото разстояние, различно от използваното за независимо откриване на движение, и което е:

— монтирано и се използва само в превозни средства от типове M1 и N1 (както са определени в приложение II към Директива 2007/46/ЕО на Европейския парламент и на Съвета ([1]), както е последно изменена), пуснати в движение след 1 май 2006 г.

— монтирано в случаите, в които технически не е възможно монтирането на друг тип съществуващ датчик за движение, който вече е в съответствие с разпоредбите на настоящото приложение и допълнения 1 — 15 към него,

— монтирано между бордовото устройство и мястото, в което се генерират импулсите за скорост/разстояние от вградени датчици или от алтернативни интерфейси,

— по отношение на бордовото устройство поведението на адаптера е същото, като при свързване към бордовото устройство на датчик за движение, който е в съответствие с разпоредбите на настоящото приложение и допълнения 1 — 16 към него;

използването на такъв адаптер в описаните по-горе превозни средства трябва да позволява монтажа и правилната употреба на бордово устройство, което е в съответствие с всички изисквания на настоящото приложение,

при тези превозни средства интелигентният тахограф включва кабели, адаптер и бордово устройство;

цц) „цялост на данните“ означава:

точността и непротиворечивостта на записаните данни, указани от липсата на каквато и да е промяна в данните между две обновявания на запис от данни. Целостта означава, че данните са точно копие на оригиналната версия, напр. че не са били повредени в процеса на записване и прочитане от тахографската карта или специално оборудване или при предаване по канал за връзка;

чч) „неприкосновеност на данните“ означава:

общите технически мерки, взети, за да се гарантира правилното прилагане на принципите, формулирани в Директива 95/46/ЕО на Европейския парламент и на Съвета ([2]), както и на формулираните в Директива 2002/58/ЕО на Европейския парламент и на Съвета ([3]);

шш) интелигентна тахографска система означава:

уредите за регистриране на данните за движението, тахографските карти и наборът от всякакво пряко или непряко взаимодействащо с тях оборудване по време на тяхното производство, монтаж, използване, изпитване и проверка, като например карти, четец за връзка с цел ранно откриване от разстояние и всякакво друго оборудване за изтегляне на данни, анализ на данни, калибриране, генериране, управление или въвеждане на защитни елементи и т.н.;

щщ) дата на въвеждане:

36 месеца след влизането в сила на подробните разпоредби, посочени в член 11 от Регламент (ЕС) № 165/2014 на Европейския парламент и на Съвета ([4]).

([1]) Директива 2007/46/ЕО на Европейския парламент и на Съвета от 5 септември 2007 година за създаване на рамка за одобрение на моторните превозни средства и техните ремаркета, както и на системи, компоненти и отделни технически възли, предназначени за такива превозни средства (Рамкова директива) (ОВ L 263, 9.10.2007 г., стр. 1).

([2]) Директива 95/46/ЕО на Европейския парламент и на Съвета от 24 октомври 1995 г. за защита на физическите лица при обработването на лични данни и за свободното движение на тези данни (ОВ L 281, 23.11.1995 г., стр. 31).

([3]) Директива 2002/58/ЕО на Европейския парламент и на Съвета от 12 юли 2002 година относно обработката на лични данни и защита на правото на неприкосновеност на личния живот в сектора на електронните комуникации (Директива за правото на неприкосновеност на личния живот и електронни комуникации) (ОВ L 201, 31.7.2002 г., стр. 37).

([4]) Регламент (ЕС) № 165/2014 на Европейския парламент и на Съвета от 4 февруари 2014 година относно тахографите в автомобилния транспорт, за отмяна на Регламент (ЕИО) № 3821/85 на Съвета относно контролните уреди за регистриране на данните за движението при автомобилен транспорт и за изменение на Регламент (ЕО) № 561/2006 на Европейския парламент и на Съвета за хармонизиране на някои разпоредби от социалното законодателство, свързани с автомобилния транспорт (ОВ L 60, 28.2.2014 г., стр. 1).

Това е датата, след която превозни средства, регистрирани за първи път:

— *се оборудват с тахограф, свързан към услуга за определяне на местоположението посредством спътникова навигационна система,*

— *се оборудват, за да могат при целенасочени пътни проверки да подават данни на компетентните контролни органи, докато превозното средство е в движение,*

— *и могат да бъдат оборудвани със стандартизирани интерфейси, позволяващи регистрираните или генерираните от тахографите данни да се използват в работен режим от външно устройство.*

ъъ) защитен профил означава:

документ, който се използва като част от процедура за сертифициране в съответствие с общите критерии, в който е дадена независима от приложението спецификация на изискванията за сигурност по отношение на гарантирането на информацията;

ююю) точност на GNSS:

в контекста на регистриране с тахографи на местоположението от Глобална навигационна спътникова система (GNSS) означава стойността на фактора на намаляване на точността при определяне на местоположението в хоризонталната равнина (HDOP), изчислявана като минималните стойности на HDOP, натрупани на наличните системи GNSS.

2 ОБЩИ ХАРАКТЕРИСТИКИ И ФУНКЦИИ НА УРЕДИТЕ ЗА РЕГИСТРИРАНЕ НА ДАННИТЕ ЗА ДВИЖЕНИЕТО

2.1 **Общи характеристики**

Функцията на уредите за регистриране на данните за движението е да се записва, съхранява, изобразява, отпечатва и да се предоставят данни относно дейностите на водача.

Всяко превозно средство, оборудвано с уреди за регистриране на данните за движението съгласно разпоредбите на настоящото приложение, трябва да има скоростомер и километражен брояч. Тези функции може да бъдат включени в уредите за регистриране на данните за движението.

01) уредите за регистриране на данните за движението включват кабели, датчик за движение и бордово устройство.

02) Интерфейсът между датчиците за движение и бордовите устройства трябва да са в съответствие с изискванията, специфицирани в допълнение 11.

03) Бордовото устройство трябва да има връзка с глобална навигационна спътникова система(и), както е посочено в допълнение 12.

04) Бордовото устройство трябва да комуникира с четците за връзка с цел ранно откриване от разстояние, както е специфицирано в допълнение 14.

05) Бордовото устройство може да включва интерфейс с ITS, който е специфициран в допълнение 13.

Уредите за регистриране на данните за движението могат да имат връзка с други устройства чрез допълнителни интерфейси и/или посредством незадължителния интерфейс с ITS.

06) Всяко вмъкване или свързване на функция или устройство(а), одобрено(и) или не, във или към уреди за регистриране на данните за движението, не трябва да предизвиква смущения или да бъде в състояние да смущава правилната и сигурна работа на уредите за регистриране на данните за движението, или да бъде в противоречие с разпоредбите на настоящия регламент.

Потребителите на уредите за регистриране на данните за движението указват своята самоличност посредством тахографски карти.

07) Уредите за регистриране на данните за движението дават избирателни права за достъп до данните и функциите според типа и/или самоличността на потребителя.

Уредите за регистриране на данните за движението записват и съхраняват данни в своята памет, в устройството за комуникация от разстояние и в тахографски карти.

Това се извършва в съответствие с Директива 95/46/ЕО от 24 октомври 1995 г. за защита на физическите лица при обработването на лични данни и за свободното движение на тези данни ([1]), с Директива 2002/58/ЕО от 12 юли 2002 г. относно обработката на лични данни и защита на правото на неприкосновеност на личния живот в сектора на електронните комуникации ([2]) и в съответствие с член 7 от Регламент (ЕС) № 165/2014.

2.2 **Функции**

08) Уредите за регистриране на данните за движението трябва да осигуряват следните функции:

— следене на поставянията и изважданията на картите,

— измерване на скорост, разстояние и определяне на местоположение,

— измерване на времето,

— следене на дейностите, извършвани от водача,

— следене на състоянието при управление на МПС,

— ръчно въвеждане на данни от водача:

  — въвеждане на местоположението в началото и/или в края на дневните периоди на работа,

  — ръчно въвеждане на дейностите на водача,

  — въвеждане на особени условия,

— управление на блокировките, наложени от превозвача,

— следене на контролните дейности,

— откриване на събития и/или на неизправности,

— вградени функции за изпробване и самоизпробване,

— четене на данни от паметта,

— записване и съхраняване на данните в паметта,

— четене от тахографските карти,

— записване и съхраняване на данните в тахографските карти,

— изобразяване на данните,

— отпечатване,

— предупреждаване,

— прехвърляне на данни към външни носители,

— връзка от разстояние за извършване на целенасочени пътни проверки,

— данни, прехвърляни към допълнителни устройства,

— калибриране,

— пътна проверка на калибрирането,

— сверяване на часовника.

([1]) ОВ L 281, 23.11.1995 г., стр. 31.
([2]) ОВ L 201, 31.7.2002 г., стр. 37

2.3 **Режими на работа**

09) Уредите за регистриране на данните за движението трябва да осигуряват следните четири режима на работа:

— работен режим,

— контролен режим,

— режим на калибриране,

— режим „превозвач“.

10) Уредите за регистриране на данните за движението трябва да превключват към следните режими на работа според валидната тахографска карта, вкарана в интерфейсното устройство за карта: За определянето на режима на работа, поколението на тахографската карта е без значение, при условие че вкараната карта е валидна. Една карта за монтаж и настройки от първо поколение винаги се счита за невалидна, когато се вкара в бордово устройство от второ поколение.

Режим на работа		Процеп за карта на водач				
		Няма карта	Карта на водач	Контролна карта	Карта за монтаж и настройки	Карта на превозвач
Процеп за карта на втория водач	Няма карта	Работен	Работен	Контролен	Калибриране	Предприятие
	карта на водач	Работен	Работен	Контролен	Калибриране	Предприятие
	Контролна карта	Контролен	Контролен	Контролен (*)	Работен	Работен
	Карта за монтаж и настройки	Калибриране	Калибриране	Работен	Калибриране (*)	Работен
	Карта на превозвач	„Предприятие“	„Предприятие“	Работен	Работен	„Предприятие“ (*)

(*) В тези ситуации уредите за регистриране на данните за движението трябва да използват само тахографската карта, поставена в процепа за карта на водач.

11) Уредите за регистриране на данните за движението трябва да отхвърлят вкарани невалидни карти, като обаче позволяват изобразяването, отпечатването и изтеглянето на данни от карта с изтекъл срок.

12) Всички функции, изброени в 2.2, трябва да работят при всички режими на работа, с изключение на:

— функцията за калибриране, която е достъпна само в режима на калибриране,

— функцията за пътна проверка на калибрирането, която е достъпна само в контролния режим,

— функцията за управление на блокиранията, наложени от превозвача, която е достъпна само в режим „превозвач“,

— функцията за следене на контролните дейности, която работи само в контролния режим,

— функцията за изтегляне на данни не е достъпна в работен режим (освен в случаите, предвидени в изискване 193) с изключение на изтеглянето на данни от карта на водач, когато в бордовото устройство не е вкарана друга карта.

13) Уредите за регистриране на данните за движението могат да подават всякаква информация към дисплей, печатащо устройство или външни интерфейси, със следните изключения:

— в работен режим, при който всяка идентификация на самоличност (фамилно име и лично(и) име (на)), което не отговаря на вкараната тахографска карта, се маскира, както и всеки номер на карта, който не отговаря на вкараната тахографска карта, се маскира частично (маскира се всеки нечетен символ отляво надясно),

— в режим „превозвач“ данните за водача (изисквания 102, 105 и 108) могат да бъдат извлечени само за периодите, за които отсъства блокиране, или които не са блокирани от друг превозвач (определяно от първите 13 цифри от номера на картата на превозвач),

— когато в уредите за регистриране на данните за движението не е вкарана карта, данните за водача могат да бъдат извличани само за същия ден и за 8-те предшестващи календарни дни,

— лични данни, произхождащи от бордовото устройство, не трябва да бъдат подавани навън посредством интерфейса с ITS на бордовото устройство, освен ако не бъде проверено че има съгласие на водача, за когото се отнасят данните,

— бордовите устройства обикновено са със срок на валидност на действията от 15 години, считано от датата на издаване на сертификатите на бордовото устройство, но те могат да се използват още 3 месеца само за изтегляне на данни.

2.4 **Сигурност**

Сигурността на системата цели да предпазва паметта така, че да възпрепятства неупълномощен достъп до нея или манипулиране на данните и да открива опити за това, да защитава целостта и автентичността на данните, които се обменят между датчика за движение и бордовото устройство, между уредите за регистриране на данните за движението и тахографските карти, а също така между уредите за регистриране на данните за движението и външното устройство за GNSS, да защитава целостта и автентичността на данните, обменяни чрез връзката за ранно откриване от разстояние с контролна цел, както и да проверява целостта и автентичността на тегленитe данни.

14) С цел постигане на сигурност на системата, следните компоненти трябва да отговарят на изискванията за сигурност, специфицирани в техните профили за защита, както се изисква в допълнение 10:

— бордово устройство,

— тахографска карта,

— датчик за движение,

— външно устройство за GNSS (този профил е необходим и приложим само за варианта с външно устройство за GNSS).

3 КОНСТРУКТИВНИ И ФУНКЦИОНАЛНИ ИЗИСКВАНИЯ ЗА УРЕДИТЕ ЗА РЕГИСТРИРАНЕ НА ДАННИТЕ ЗА ДВИЖЕНИЕТО

3.1 **Следене на вкарването и изваждането на картите**

15) Уредите за регистриране на данните за движението трябва да следят интерфейсните устройства за карта, за да откриват вкарванията и на изваждания на карта.

16) При вкарването на карта, уредите за регистриране на данните за движението трябва да разпознават дали вкараната карта е валидна тахографска карта и ако да, да разпознават типа и поколението ѝ.

Ако в уредите за регистриране на данните за движението вече е била вкарана карта със същия номер на карта и с по-голям индекс за подновяване на валидността на картата, картата трябва да бъде обявена за невалидна.

Ако в уредите за регистриране на данните за движението вече е била вкарана карта със същите номер на карта и индекс за подновяване на валидността на картата, но с по-голям индекс за замяна на картата, картата трябва да бъде обявена за невалидна.

17) Тахографските карти от първо поколение трябва да се считат за невалидни от уредите за регистриране на данните за движението, веднъж щом възможността за използване на тахографски карти от първо поколение е премахната от страна на сервиза, в съответствие с допълнение 15 (MIG003)

18) Карти за монтаж и настройка от първо поколение, които се вкарват в уреди за регистриране на данните за движението от второ поколение, трябва да се считат за невалидни.

19) Уредите за регистриране на данните за движението трябва да бъдат така конструирани, че тахографските карти да бъдат застопорявани в правилно положение в интерфейсното устройства за карта.

20) Изваждането на тахографска карта е възможно само когато превозното средство е спряло и след като съответните данни за записани на нея. Изваждането на тахографската карта трябва да изисква целенасочено действие на потребителя.

3.2 **Измерване на скоростта и разстоянието и определяне на местоположението**

21) Датчикът за движение (евентуално вграден в адаптера) е основният източник на сигнал за измерването на скоростта и на изминатото разстояние.

22) Тази функция трябва да мери непрекъснато и да може да подава стойността от километражния брояч, съответстваща на общото разстояние, изминато от превозното средство, чрез използване на импулсите, подавани от датчика за движение.

23) Тази функция трябва да мери непрекъснато и да може да подава скоростта на превозното средство чрез използване на импулсите, подавани от датчика за движение.

24) Функцията за измерване на скоростта на превозното средство трябва също така да подава информацията дали превозното средство е в движение или е спряло. Смята се, че превозното средство е в движение щом функцията засича от датчика за движение повече от 1 имп./s за период не по-малко от 5 секунди, в противен случай се приема, че превозното средство е спряло.

25) Устройствата за показване на скоростта (скоростомер) и общото изминато разстояние (километражен брояч), монтирани на всяко превозно средство, оборудвано с отговарящи на разпоредбите на настоящия регламент уреди за регистриране на данните за движението, трябва да отговарят на изискванията относно максимално допустимите толеранси (виж 3.2.1 и 3.2.2), посочени в настоящото приложение.

26) За откриване на манипулиране на данни за движението, информацията от датчика за движение трябва да бъде потвърдена от информация за движението на превозното средство, извлечена от приемника на сигнали от GNSS, и като незадължителен вариант, от друг(и) източник(ци), независими от датчика за движение.

27) Тази функция трябва да определя местоположението на превозното средство, за да се даде възможност за автоматично записване на:

— места, където водачът и/или вторият водач започва своя дневен работен период;

— места, където времето на непрекъснато управление на МПС на водача да достига стойност, кратна на три часа;

— места, където водачът и/или вторият водач завършва своя дневен работен период.

3.2.1 *Измерване на изминатото разстояние*

28) Изминатото разстояние може да бъде измервано така че:

— или да се интегрира и движението напред, и движението на заден ход,

— или да де включва само движението напред.

29) Уредите за регистриране на данните за движението трябва да измерват разстояние от 0 до 9 999 999,9 km.

30) Измерваното разстояние трябва да бъде със следния толеранс (разстояния от най-малко 1 000 m):

— ± 1 % преди монтирането,

— ± 2 % по време на монтирането и на периодичните технически прегледи,

— ± 4 % по време на работа.

31) Разделителната способност при измерване на разстоянието трябва да бъде по-висока или равна на 0,1 km.

3.2.2 *Измерване на скоростта*

32) Уредите за регистриране на данните за движението трябва да измерват скорост от 0 до 220 km/h.

33) С цел да гарантира максимален толеранс ± 6 km/h за показваната скорост по време на работа и като се взема предвид:

— толеранс ± 2 km/h за различия в постъпващите данни (различия в гумите и т.н.),

— толеранс ± 1 km/h за измерванията, извършвани по време на монтирането и на периодичните технически прегледи,

при скорости между 20 и 180 km/h и при характеристични коефициенти на превозното средство между 4 000 и 25 000 имп./km, уредите за регистриране на данните за движението трябва да могат да измерват скоростта с толеранс ± 1 km/h (при постоянна скорост).

Забележка: Разделителната способност на записа на данните въвежда допълнителен толеранс от ± 0,5 km/h за скоростта, записвана в уредите за регистриране на данните за движението.

34) Скоростта трябва да бъде измервана правилно, в рамките на нормалния толеранс, в рамките на две секунди след промяна на скоростта, когато се е изменяла с темп 2 m/s^2.

35) Разделителната способност при измерване на скоростта трябва да бъде по-висока или равна на 1 km/h.

3.2.3 *Определяне на местоположението*

36) Уредите за регистриране на данните за движението трябва да определят абсолютното местоположение на превозното средство чрез използване на приемника на сигнали от GNSS.

37) Абсолютното местоположение се определя с географски координати за географска ширина и географска дължина в градуси и минути с разделителна способност 1/10 от минутата.

3.3 **Измерване на времето**

38) Функцията за измерване на времето трябва да осигурява непрекъснато измерване и изобразяването в цифров вид на датата и часа по координираното универсално време.

39) Датата и координираното универсално време се използват за определяне на дата за данните в уредите за регистриране на данните за движението (записи, обмен на данни) и за всички разпечатки, посочени в допълнение 4 „Разпечатки“.

40) С цел показване на местното време, трябва да може да се коригира изместването на времето на стъпки от по половин час. Не се позволяват никакви други изместания освен отрицателни или положителни кратни на половин час стойности.

41) Неточността на времето трябва да е в рамките на ± 2 секунди на ден при условията за одобряване на типа, в отсъствието на всякакво сверяване.

42) Разделителната способност при измерване на времето трябва да бъде по-висока или равна на 1 секунда.

43) Измерването на времето не трябва да се влияе от прекъсване на външното електрическо захранване, с продължителност, по-малка от 12 месеца при условията за одобряване на типа.

3.4 **Следене на дейностите на водача**

44) Тази функция трябва да осигурява постоянно и отделно следене на дейностите, извършвани от един водач и един втори водач.

45) Дейността, извършвана от водача, трябва да бъде управление на МПС, РАБОТА, НА РАЗПОЛОЖЕНИЕ или ПРЕКЪСВАНЕ/ПОЧИВКА.

46) Водачът и/или вторият водач трябва да може да избира ръчно дейността РАБОТА, НА РАЗПОЛОЖЕНИЕ или ПРЕКЪСВАНЕ/ПОЧИВКА.

47) Когато превозното средство е в движение, дейността управление на МПС трябва да бъде автоматично избрана за водача, а дейността НА РАЗПОЛОЖЕНИЕ трябва да бъде автоматично избрана за втория водач.

48) Когато превозното средство спре, за водача трябва да бъде избрана автоматично дейността РАБОТА.

49) Първата промяна на дейността към „ПОЧИВКА“ или към „НА РАЗПОЛОЖЕНИЕ“, настъпила през 120-те секунди след автоматичната промяна към „РАБОТА“ поради спирането на превозното средство, се приема за настъпила в момента на спиране на превозното средство (и следователно евентуално е анулирала преминаването към „РАБОТА“).

50) Тази функция трябва да предава промените в дейността към функциите, осигуряващи записването на информацията, с разделителна способност от една минута.

51) За определена календарна минута, ако е регистрирана дейност „управление на МПС“ за непосредствено предхождащата я минута и за непосредствено следващата я минута, за цялата минута се счита, че се извършва дейността „управление на МПС“.

52) За определена календарна минута, за която не се счита, че се извършва дейността „управление на МПС“ съгласно изискване 051, за цялата минута се счита, че е извършвана дейността, която съвпада с най-дългата непрекъсната дейност, извършвана в рамките на минутата (или с най-скорошната дейност, при наличие на няколко дейности с еднаква продължителност).

53) Тази функция трябва също така да позволява постоянно следене на непрекъснатото работно време и на общото време на прекъсване на водача.

3.5 **Следене на състоянието при управление на МПС**

54) Тази функция трябва да осигурява постоянно и автоматично наблюдение на състоянието при управление на МПС.

55) Състоянието при управление на МПС „ЕКИПАЖ“ трябва да бъде избрано, когато в уреда са вкарани две валидни карти на водач, а при всички останали случаи трябва да бъде избрано състоянието при управление на МПС „САМ“.

3.6 **Въвеждане на данни от водачите**

3.6.1 *Въвеждане на мястото, където дневните периоди на работа започват и/или завършват*

56) Тази функция трябва да позволява въвеждането на местата, където, според водача и/или втория водач, техните дневни периоди на работа започват и/или завършват.

57) Под „места“ се разбира страната и, освен това където е приложимо, регионът, въведен или потвърден ръчно.

58) При изваждането на карта на водач, уредът за регистриране на данните за движението трябва да прикани водача/втория водач да въведе „място, където дневният период на работа завършва“.

59) Тогава водачът трябва да въведе текущото място на превозното средство, което трябва да се счита за временно въвеждане.

60) Трябва да е възможно въвеждането на местата, където дневният период на работа започва/завършва, чрез команди от менюто. Ако в рамките на една календарна минута се направят повече от едно такива въвеждания, трябва да се съхранят само последните извършени задания за начално място и крайно място.

3.6.2 *Ръчно въвеждане на дейностите, извършвани от водача, и на съгласието на водача за интерфейса с ITS*

61) При вкарването на карта на водач (или на карта за монтаж и настройка) и само в този момент, уредът за регистриране на данните за движението трябва да позволява ръчно въвеждане на дейността. Ръчното въвеждане на дейността се извършва, като се използват стойностите за местното време и дата за съответната часова зона (изместване спрямо координираното универсално време), която е текущо зададена за бордовото устройство.

При вкарването на карта на водач или на карта за монтаж и настройка, на титуляря на картата се напомня за:

— датата и часа на последния път, когато е извадил картата;

— незадължително: текущо зададеното за бордовото устройство изместване на местното време спрямо UTC.

При първото вкарване на дадена карта на водач или на карта за монтаж и настройка, към момента неизвестна за бордовото устройство, титулярят на картата трябва да бъде приканен да изрази своето съгласие за подаване на лични данни, свързани с тахографирането, посредством незадължителния интерфейс с ITS.

Във всеки един момент, съгласието на водача (съответно на сервиза) може да бъде активирано или дезактивирано чрез команди от менюто, при условие, че е вкарана карта на водач (съответно карта за монтаж и настройка).

Трябва да е възможно да се зададе дейност със следните ограничения:

— видът на дейността трябва да бъде „РАБОТА“, „НА РАЗПОЛОЖЕНИЕ“ или ПРЕКЪСВАНЕ/ПОЧИВКА;

— Началото и краят на всяка дейност трябва да са в рамките на периода между последното изваждане на картата и нейното настоящо вкарване.

— Не се позволява взаимно припокриване на дейности във времето.

Ако е необходимо, при първото вкарване на неизползвана преди карта на водач (или карта за монтаж и настройки) трябва да е възможно ръчно въвеждане.

Процедурата за ръчно въвеждане на дейности трябва да включва толкова последователни стъпки, колкото е необходимо за задаване на вида и момента, като час и минути, на започване и завършване на всяка една дейност. За титуляря на картата трябва да има избираем вариант да не посочва дейност за която и да е част от периода от време между последното изваждане на картата и нейното настоящо вкарване.

По време на ръчното въвеждане, съответстващо на вкарването на картата и, ако е необходимо, титулярят на картата трябва да има възможност да зададе:

— място, където е завършил предишен дневен период на работа, заедно със съответното време (като по този начин се замества въведеното при последното изваждане на картата),

— място, където започва настоящият дневен период на работа, заедно със съответното време.

Ако титулярят на картата не въведе място, където започва или е завършил периодът на работа, по време на ръчните въвеждания във връзка с вкарването на картата, това се счита за декларация, че периодът му на работа не се е променил от последното изваждане на картата. Следващото въвеждане на място, където е завършил предишен дневен период на работа, трябва да замести временното въвеждане, извършено при последното изваждане на картата.

Ако е въведено място, то трябва да се запише в съответната тахографска карта.

Ръчното въвеждане трябва да бъде прекъснато ако:

— картата бъде извадена или

— превозното средство се движи и картата е в процепа за карта на водач.

Позволени са допълнителни прекъсвания — напр. след изтичане на определен период от време, през който потребителят не е бил активен. Ако ръчното въвеждане бъде прекъснато, уредите за регистриране на данните за движението трябва да валидират вече въведените пълни записи за място и дейност (които съдържат или еднозначно посочени място и време, или вид, време на започване и време на завършване на дейността).

Ако бъде поставена втора карта на водач или карта за монтаж и настройки докато е в ход ръчното въвеждане на дейности за вкарана преди това карта, трябва да е позволено завършване на ръчното въвеждане за тази предишна карта преди да започне ръчното въвеждане за втората карта.

Титулярят на картата трябва да разполага с избираем вариант за ръчно въвеждане по следната минимална процедура:

— Ръчно задаване на дейности в хронологична последователност за периода от последното изваждане на картата до нейното настоящо вкарване.

— Като време на започване на първата дейност трябва да се зададе моментът на изваждане на картата. За всяко следващо въвеждане времето на започване автоматично трябва да се задава така, че непосредствено да следва времето на завършване за предишното въвеждане. За всяка дейност се избира и задава нейният вид и времето на завършване.

Процедурата приключва, когато времето на завършване на ръчно зададена дейност съвпадне с времето на вкарване на картата. Тогава уредите за регистриране на данните за движението може, като избираем вариант, да позволят на титуляря на картата да промени всяка една ръчно въведена дейност до нейното валидиране чрез избор на конкретна команда. След това трябва да е забранено каквато и да е изменение.

3.6.3 *Въвеждане на специфични условия*

62) Уредите за регистриране на данните за движението трябва да позволяват на водача да въвежда в реално време следните две специфични условия:

— „ИЗВЪН ОБХВАТ“ (начало, край)

— „ПЪТУВАНЕ С ФЕРИБОТ/ВЛАК“ (начало, край).

Не може да се задава „ПЪТУВАНЕ С ФЕРИБОТ/ВЛАК“, когато е зададено условието „ИЗВЪН ОБХВАТ“.

Отвореното условие „ИЗВЪН ОБХВАТ“ трябва задължително да бъде затворено автоматично от уреда за регистриране на данните за движението в случай на изваждане или вкарване на карта на водач.

Ако е отворено условие „ИЗВЪН ОБСЕГ“, това води до забрана на следните събития и предупреждения:

— управление на МПС без съответната карта,

— Предупреждения, свързани с времето на непрекъснато управление на МПС.

Началният флаг ПЪТУВАНЕ С ФЕРИБОТ/ВЛАК трябва да се зададе преди спирането на двигателя върху ферибота/влака.

Отворено ПЪТУВАНЕ С ФЕРИБОТ/ВЛАК трябва да приключи, когато се появи някой от следните избираеми варианти:

— Водачът приключва ръчно ПЪТУВАНЕТО С ФЕРИБОТ/ВЛАК

— Водачът изважда картата си

Едно отворено ПЪТУВАНЕ С ФЕРИБОТ/ВЛАК трябва да завърши когато вече не е валидно въз основа на правилата, формулирани в Регламент (ЕО) № 561/2006.

3.7 **Управление на блокиранията, наложени от превозвача**

63) Тази функция трябва да позволява управлението на блокировките, поставени от даден превозвач с цел да ограничи и запази единствено за себе си достъпа до данните в режим „превозвач“.

64) Блокировките, наложени от превозвача, се състоят в дата и час на начало (блокиране) и дата и час на край (разблокиране), свързани с идентификацията на превозвача чрез номера на картата на превозвач (по време на блокирането).

65) Блокирането и разблокирането са възможни само в реално време.

66) Разблокирането трябва да може да се извърши само от превозвача, който е извършил блокирането (така, както то се идентифицира с първите 13 цифри на номера на картата на превозвач), или,

67) Разблокирането трябва да става автоматично, когато друг превозвач извърши блокиране.

68) В случай че даден превозвач извърши блокиране и ако предишното блокиране е било извършено от същия превозвач, се приема, че предишното блокиране не е разблокирано и че то все още е в сила.

3.8 **Следене на контролните дейности**

69) Тази функция трябва да следи дейностите по ИЗОБРАЗЯВАНЕ, ОТПЕЧАТВАНЕ, ИЗТЕГЛЯНЕ НА ДАННИ от БУ и картата, както и пътна ПРОВЕРКА НА КАЛИБРИРАНЕТО, провеждани в контролен режим.

70) Тази функция трябва да осигурява също така следене на дейностите по КОНТРОЛ ЗА ПРЕВИШЕНА СКОРОСТ в контролен режим. Приема се, че е извършен контрол за превишена скорост, когато в контролен режим се изпраща съобщение „превишена скорост“ към печатащото устройство или дисплея или когато данни за „събития или неизправности“ са изтеглени от паметта на бордовото устройство.

3.9 **Откриване на събития и/или неизправности**

71) Тази функция открива следните събития и/или неизправности:

3.9.1 *Събитие „вкарване на невалидна карта“*

72) Това събитие се предизвиква от вкарването на невалидна карта, при вкарване на вече заменена карта на водач, и/или когато валидността на вкарана карта изтича.

3.9.2 *Събитие „конфликт, предизвикан от картата“*

73) Това събитие се предизвиква от всяка от отбелязаните с хикс комбинации от карти в долната таблица:

Конфликт, предизвикан от карта		Процеп за карта на водач				
		Няма карта	Карта на водач	Контролна карта	Карта за монтаж и настройки	Карта на превозвач
Процеп за карта на втория водач	Няма карта					
	Карта на водач				X	
	Контролна карта			X	X	X
	Карта за монтаж и настройки		X	X	X	X
	Карта на превозвач			X	X	X

3.9.3 *Събитие „припокриване във времето“*

74) Това събитие се предизвиква когато датата/часът на последното изваждане на дадена карта на водач, прочетени от картата, са по-късни от текущите дата/час на уреда за регистриране на данните за движението, в който картата е вкарана.

3.9.4 *Събитие „управление на МПС без съответната карта“*

75) Това събитие се предизвиква от всяка от отбелязаните с хикс комбинации от тахографски карти в долната таблица, когато дейността на водача става управление на МПС, или в случай на промяна на режима на работа, когато дейността на водача е управление на МПС:

управление на МПС без съответната карта		Процеп за карта на водач				
		Няма (или невалидна) карта	Карта на водач	Контролна карта	Карта за монтаж и настройки	Карта на превозвач
Процеп за карта на втория водач	Няма (или невалидна) карта	X		X		X
	Карта на водач	X		X	X	X
	Контролна карта	X	X	X	X	X
	Карта за монтаж и настройки	X	X	X		X
	Карта на превозвач	X	X	X	X	X

3.9.5 *Събитие „вкарване на карта по време на управление на МПС“*

76) Това събитие се предизвиква от вкарването на тахографска карта в който и да е процеп, когато дейността на водача е управление на МПС.

3.9.6 *Събитие „неправилно приключена последна картова сесия“*

77) Това събитие се предизвиква, когато уредите за регистриране на данните за движението открият при вкарването на карта, че въпреки разпоредбите на точка 3.1, предишната картова сесия не е била приключена правилно (картата е била извадена преди всички необходими данни да са били записани на картата). Това събитие трябва да се предизвиква само от карта на водач или карта за монтаж и настройки.

3.9.7 *Събитие „превишаване на скоростта“*

78) Това събитие се предизвиква при всяко превишаване на допустимата скорост.

3.9.8 *Събитие „прекъсване на електрическото захранване“*

79) Това събитие се предизвиква в режим, различен от режима на калибриране или от контролния режим, при прекъсване за повече от 200 милисекунди на електрическото захранване на датчика за движение и/или на бордовото устройство. Прагът на прекъсване се определя от производителя. Прекъсването на електрическото захранване, дължащо се на пускането на двигателя на превозното средство, не трябва да предизвиква появата на това събитие.

3.9.9 *Събитие „Грешка в комуникацията с устройството за връзка от разстояние“*

80) Това събитие трябва да се предизвиква, **извън режима на калибриране**, когато устройството за връзка от разстояние не потвърждава успешното приемане на данни при комуникацията от разстояние, изпратени от бордовото устройство, при повече от три опита.

3.9.10 *Събитие „Липса на информация за местоположението от приемник на сигнали от GNSS“*

81) Това събитие трябва да се предизвиква **извън режима на калибриране**, в случай на липса на информация за местоположението, постъпваща от приемник на сигнали от GNSS (вътрешен или външен) за повече от три часа натрупано, време на управление на МПС.

3.9.11 *Събитие „Грешка в комуникацията с външното устройство за GNSS“*

82) Това събитие трябва да се предизвиква **извън режима на калибриране**, в случай на прекъсване на комуникацията между външното устройство за GNSS и бордовото устройство за повече от 20 последователни минути, когато превозното средство е в движение.

3.9.12 *Събитие „Грешка в данните за движението“*

83) Това събитие трябва да се предизвиква, **извън режима на калибриране**, при прекъсване на нормалния поток от данни между датчика за движение и бордовото устройство и/или в случай на грешка, свързана с целостта на данните или с удостоверяването им по време на техния обмен между датчика за движение и бордовото устройство.

3.9.13 *Събитие „Противоречие в данните за движението на превозното средство“*

84) Това събитие трябва да се предизвиква **извън режима на калибриране**, в случай че информацията за движение, изчислена от датчика за движение, противоречи на информацията за движение, изчислена от вътрешния приемник на сигнали от GNSS или от външно устройство за GNSS и евентуално от други независими източници, както е специфицирано в допълнение 12. Това събитие не трябва да се предизвиква по време на пътуване с ферибот/влак, условие „ИЗВЪН ОБСЕГ“, или когато информацията за местоположението не е на разположение от приемника на сигнали от GNSS.

3.9.14 *Събитие „Опит за нарушаване на сигурността“*

85) Извън режима за калибриране това събитие трябва да се предизвиква при настъпване на всяко друго събитие, засягащо сигурността на датчика за движение и/или на бордовото устройство и/или външното устройство за GNSS, така както се изисква в допълнение 10.

3.9.15 *Събитие „времеви конфликт“*

86) Това събитие се предизвиква, **извън режима на калибриране**, когато Бордовото устройство открие несъответствие от над 1 минута между времето на функцията за измерване на времето на бордовото устройство, и времето, постъпващо от приемника на сигнали от GNSS. Това събитие се записва заедно със стойността на вътрешния часовник на бордовото устройство и се придружава от автоматично сверяване на часовника. След предизвикване на събитие на времеви конфликт, през следващите 12 часа бордовото устройство не генерира други събития на времеви конфликт. Това събитие не трябва да се предизвиква в случай, че от приемника на сигнали от GNSS не е могъл да бъде открит валиден сигнал от GNSS в рамките на последните 30 дни. Когато обаче информацията за местоположението от приемника на сигнали от GNSS отново стане достъпна, трябва да бъде извършено автоматично сверяване на часовника.

3.9.16 *Неизправност „Карта“*

87) Тази неизправност се предизвиква при неизправност в тахографската карта по време на нейното функциониране.

3.9.17 *Неизправност „Уред за регистриране на данните за движението“*

88) Тази неизправност се предизвиква при следните неизправности, при режимите, различни от режима за калибриране:

— Неизправност вътре в бордовото устройство

— Неизправност в печатащото устройство

— Неизправност в дисплея

— Грешка при изтегляне на данни

— Неизправност на датчика

— Неизправност в приемника на сигнали от GNSS или външното устройство за GNSS

— Неизправност в устройството за връзка от разстояние

3.10 **Вградени функции за изпробване и самоизпробване**

89) Уредът за регистриране на данните за движението трябва да открива неизправности чрез функции за изпробване и самоизпробване в съответствие с долната таблица:

Елемент за изпробване	Самоизпробване	Вградена функции за изпробване
Софтуер		Работоспособност
Памет за данни	Достъп	Достъп, цялост на данните
Интерфейсни устройства за карта	Достъп	Достъп
Клавиатура		Ръчна проверка
Печатащо устройство	(по избор на производителя)	Разпечатка
Дисплей		Визуална проверка
Изтегляне на данни (извършвано само по време на изтеглянето)	Правилно функциониране	
Датчик	Правилно функциониране	Правилно функциониране
Устройство за връзка от разстояние	Правилно функциониране	Правилно функциониране
Устройство за GNSS	Правилно функциониране	Правилно функциониране

3.11 **Четене от паметта за данни**

90) Уредът за регистриране на данните за движението трябва да може да чете всякакви данни, записани в паметта му.

3.12 **Регистриране и запис в паметта за данни**

За целите на настоящата точка,

— под „365 дни“ се разбира 365 календарни дена на средна дейност на водачите в дадено превозно средство. Средната дейност на ден в едно превозно средство се определя като най-малко 6 водачи или втори водачи, 6 цикъла на вкарване/изваждане на карта и 256 смени на дейностите. Следователно „365 дни“ включват най-малко 2 190 водачи/втори водачи и 93 440 смени на дейностите,

— средният брой на местоположенията на ден се определя като най-малко 6 местоположения, в които започва дневният период на работа, 6 местоположения, в които времето на непрекъснато управление на МПС на водача достига време, кратно на три часа, и 6 местоположения, в които завършва дневният период на работа, така че „365 дни“ включват най-малко 6 570 местоположения,

— часовете се регистрират с точност от една минута, освен ако не е предвидено друго,

— стойностите от километражния брояч се регистрират с разделителна способност един километър,

— скоростите се регистрират с разделителна способност един km/h,

— местоположенията (ширини и дължини) се регистрират в градуси и минути, с разделителна способност 1/10 от минутата, със съответните точност и време за снемане на данни на GNSS.

91) Данните, записани в паметта, не трябва да се влияят от прекъсване на външното електрическо захранване с продължителност, по-малка от 12 месеца, при условията за одобряване на типа. Освен това данните, записани във външното устройство за връзка от разстояние, както е определено в допълнение 14, не трябва да се влияят от прекъсване на електрическото захранване по-краткотрайно от 28 дни.

92) Уредите за регистриране на данните за движението трябва да могат да регистрират и записват по подразбиране или при задаване следните данни в своята памет:

3.12.1 *Данни за идентификация на уредите*

3.12.1.1 Данни за идентификация на бордовото устройство

93) Уредът за регистриране на данните за движението трябва да може да записва в своята памет следните данни за идентификацията на бордовото устройство:

— наименование на производителя,

— адрес на производителя,

— номер на частта,

— сериен номер,

— поколение на БУ,

— способност за използване на тахографски карти от първо поколение

— номер на версията на софтуера,

— дата на инсталиране на версията на софтуера,

— година на производство на уреда,

— номер на одобрение,

94) Данните за идентификацията на бордовото устройство се регистрират и записват еднократно от производителя на бордовото устройство, освен данните за софтуера и номера на одобрението (които могат да бъдат променени при обновяване на софтуера), както и способността за използване на тахографски карти от първо поколение.

3.12.1.2 Данни за идентификация на датчика за движение

95) Датчикът за движение трябва да може да записва в паметта си следните данни за идентификация:

— наименование на производителя,

— сериен номер,

— номер на одобрение,

— идентификатор на вградения компонент за сигурност (напр. сериен номер на вътрешната интегрална схема/процесор),

— идентификатор на операционната система (напр. номер на версията на софтуера).

96) Данните за идентификация на датчика за движение се регистрират и записват еднократно в датчика от неговия производител.

97) Бордовото устройство трябва да може да регистрира и записва в паметта си следните данни, свързани с последните 20 сдвоявания на датчици за движение (ако в рамките на един календарен ден се случат няколко свързвания, в паметта се записват само първото и последното за деня):

За всяко от тези свързвания се регистрират следните данни:

— данни за идентификация на датчика за движение:

— сериен номер

— номер на одобрение

— данни за сдвояването на датчик за движение:

— дата на сдвояването.

3.12.1.3 Данни за идентификация на Глобална навигационна спътникова система

98) Външното устройство за GNSS трябва да може да записва в паметта си следните данни за идентификация:

— наименование на производителя,

— сериен номер,

— номер на одобрение,

— идентификатор на вградения компонент за сигурност (напр. сериен номер на вътрешната интегрална схема/процесор),

— идентификатор на операционната система (напр. номер на версията на софтуера).

99) Данните за идентификация се регистрират и записват еднократно във външното устройство за GNSS от неговия производител.

100) Бордовото устройство трябва да може да регистрира и записва в паметта си следните данни, свързани с последните 20 свързвания на външни устройства за GNSS (ако в рамките на един календарен ден се случат няколко свързвания, в паметта се записват само първото и последното за деня).

За всяко от тези свързвания се регистрират следните данни:

— данни за идентификация на външно устройство за GNSS:

— пореден номер,

— номер на одобрение,

— данни за свързаното външно устройство за GNSS:

— дата на свързването

3.12.2 *Ключове и сертификати*

101) Уредите за регистриране на данните за движението трябва да могат да записват определен брой криптографски ключове и сертификати, както е посочено в допълнение 11, част А и част Б.

3.12.3 *Данни за вкарването и изваждането на картата на водач или картата за монтаж и настройки*

102) За всеки цикъл на вкарване-изваждане на дадена карта на водач или карта за монтаж и настройки в уреда за регистриране на данните за движението, последното трябва да регистрира и записва в своята памет:

— името и презимето на титуляря на картата така, както те са записани в картата,

— номера на картата, държавата членка, която я е издала, и срокът на валидност, така както са записани на картата,

— поколението на картата,

— датата и часа на вкарването,

— стойността от километражния брояч на превозното средство в момента на вкарването на картата,

— процепа, в който се вкарва картата,

— датата и часа на изваждането ѝ,

— стойността от километражния брояч на превозното средство в момента на изваждането на картата,

— следната информация относно последното превозно средство, използвано от водача така, както е записана в картата:

— регистрационния номер на превозното средство (VRN) и държавата членка на регистрация,

— поколението на БУ (когато е налично),

— дата и час на изваждането на картата,

— флаг, указващ дали при вкарването на картата титулярят на картата е въвел ръчно дейностите или не.

103) Паметта трябва да може да запазва тези данни в продължение на най-малко 365 дни.

104) Когато капацитетът за съхраняване на информация е изчерпан, новите данни заместват най-старите данни.

3.12.4 *Данни за дейностите на водача*

105) Уредът за регистриране на данните за движението трябва да регистрира и записва в паметта си всяка промяна на дейността на водача и/или на втория водач, и/или всяка промяна на състоянието при управление на МПС, и/или всяко вкарване или изваждане на карта на водач или карта за монтаж и настройки:

— състояние при управление на МПС (ЕКИПАЖ, САМ),

— процеп (ВОДАЧ, ВТОРИ ВОДАЧ),

— положение на картата в процепа (ВКАРАНА/НЕВКАРАНА),

— дейност (управление на МПС, НА РАЗПОЛОЖЕНИЕ, РАБОТА, ПРЕКЪСВАНЕ/ПОЧИВКА),

— дата и час на промяната.

ВКАРАНА означава, че в процепа е вкарана валидна карта на водач или карта за монтаж и настройки. НЕВКАРАНА означава обратното, тоест че в процепа няма валидна карта на водач или карта за монтаж и настройки (напр. вкарана е карта на превозвач или не е вкарана карта)

Въвежданите ръчно от водача данни за дейността не се записват в паметта.

106) Паметта трябва да може да запазва данните за дейността на водача в продължение на най-малко 365 дни.

107) Когато капацитетът за съхраняване на информация е изчерпан, новите данни заместват най-старите данни.

3.12.5 *Места и местоположения, където започват и завършват дневните периоди на работа, и/или където времето на непрекъснато управление на МПС достига 3 часа.*

108) Уредът за регистриране на данните за движението трябва да регистрира и записва и в своята памет за данни:

— места и местоположения, където водачът и/или вторият водач започва своя дневен работен период;

— места, където времето на непрекъснато управление на МПС на водача да достига стойност, кратна на три часа;

— места и местоположения, където водачът и/или вторият водач приключва своя дневен работен период.

109) Когато в тези моменти местоположението на превозното средство не е на разположение от приемника на сигнали от GNSS, уредът за регистриране на данните за движението трябва да използва последното налично местоположение и съответните дата и час.

110) Заедно с всяко място или местоположение, уредът за регистриране на данните за движението трябва да регистрира и записва и в своята памет за данни:

— номера на картата на водача/втория водач и държавата членка, която е издала картата,

— поколението на картата,

— дата и час на въвеждането,

— вид на въвеждането (начало, край или 3 часа непрекъснато време на управление на МПС),

— съответната точност на GNSS, дата и час, ако е приложимо;

— стойността от километражния брояч на превозното средство.

111) Паметта за данни трябва да позволява съхраняването места и и местоположения, където започват и завършват дневните периоди на работа, и/или където времето на непрекъснато управление на МПС достига 3 часа, в продължение на най-малко 365 дни.

112) Когато капацитетът за съхраняване на информация е изчерпан, новите данни заместват най-старите данни.

3.12.6 *Данни от километражния брояч*

113) Уредът за регистриране на данните за движението трябва да записва в своята памет стойността от километражния брояч на превозното средство и съответната дата в полунощ всеки календарен ден.

114) Паметта за данни трябва да позволява съхраняването ежедневните записи в полунощ от километражния брояч в продължение на най-малко 365 календарни дни.

115) Когато капацитетът за съхраняване на информация е изчерпан, новите данни трябва да заместват най-старите данни.

3.12.7 *Подробни данни за скоростта*

116) Уредът за регистриране на данните за движението трябва да записва в своята памет моментната скорост на превозното средство и датата и часа през всяка секунда от, като минимум, последните 24 часа, по време на които превозното средство е било в движение.

3.12.8 *Данни за събитията*

За целите на настоящата подточка времето се записва с точност една секунда.

117) Уредът за регистриране на данните за движението трябва да записва в своята памет следните данни за всяко засечено събитие, съгласно следните правила за запис:

Събитие	Правила за запис в паметта	Данни, които се регистрират при всяко събитие
Вкарване на невалидна карта	— 10-те най-скорошни събития.	— дата и час на събитие, — тип на картата(ите), номер, държава членка, издала картата, и поколение на картата, предизвикваща събитието. — брой сходни събития, възникнали същия ден
Конфликт, предизвикан от карта	— 10-те най-скорошни събития.	— дата и час на начало на събитието, — дата и час на край на събитието, — тип и номер на картата(ите), държава членка, издала картата(ите), и поколение на двете карти, предизвикващи събитието.
управление на МПС без съответната карта	— най-продължителното събитие за всеки от десетте последни дена на възникване на това събитие, — 5-те най-продължителни събития през последните 365 дни.	— дата и час на начало на събитието, — дата и час на край на събитието, — тип и номер на картата(ите), държава членка, издала картата(ите), както и поколение на всяка карта, вкарана в началото и/или в края на събитието, — брой сходни събития, възникнали същия ден.

Събитие	Правила за запис в паметта	Данни, които се регистрират при всяко събитие
Вкарване на карта по време на управление на МПС	— последното събитие за всеки от десетте последни дена на възникване на това събитие,	— дата и час на събитието, — тип и номер на картата(ите), държава членка, издала картата(ите), поколение, — брой сходни събития, възникнали същия ден
Неправилно приключване на последната картова сесия	— 10-те най-скорошни събития.	— дата и час на вкарване на картата, — тип и номер на картата(ите), държава членка, издала картата(ите), поколение, — данни относно последната сесия така, както са прочетени от картата: — дата и час на вкарване на картата, — VRN, държава членка на регистрация и поколение на бордовото устройство.
Превишаване на скоростта (1)	— най-сериозното събитие (тоест събитието, при което е достигната най-висока средна скорост) през десетте последни дена на възникване на това събитие, — 5-те най-сериозни събития през последните 365 дни. — първото събитие, възникнало след последното калибриране	— дата и час на начало на събитието, — дата и час на край на събитието, — максимална скорост, измерена по време на събитието, — средноаритметична скорост, измерена по време на събитието, — тип и номер на картата, държава членка, издала картата, и поколение на картата на водач (ако е приложимо), — брой сходни събития, възникнали същия ден.
Прекъсване на електрическото захранване (2)	— най-продължителното събитие за всеки от десетте последни дена на възникване на това събитие, — 5-те най-продължителни събития през последните 365 дни.	— дата и час на начало на събитието, — дата и час на край на събитието, — тип и номер на картата(ите), държава членка, издала картата(ите), както и поколение на всяка карта, вкарана в началото и/или в края на събитието, — брой сходни събития, възникнали същия ден.
Грешка в комуникацията с устройството за връзка от разстояние	— най-продължителното събитие за всеки от десетте последни дена на възникване на това събитие, — 5-те най-продължителни събития през последните 365 дни.	— дата и час на началото на събитие, — дата и час на края на събитие, — тип и номер на картата(ите), държава членка, издала картата(ите), както и поколение на всяка карта, вкарана в началото и/или в края на събитието, — брой сходни събития, възникнали същия ден.
Липса на информация за местоположението от приемник на сигнали от GNSS	— най-продължителното събитие за всеки от десетте последни дена на възникване на това събитие, — 5-те най-продължителни събития през последните 365 дни.	— дата и час на началото на събитие, — дата и час на край на събитието, — тип и номер на картата(ите), държава членка, издала картата(ите), както и поколение на всяка карта, вкарана в началото и/или в края на събитието, — брой сходни събития, възникнали същия ден.

Събитие	Правила за запис в паметта	Данни, които се регистрират при всяко събитие
Грешка в данните за движението	— най-продължителното събитие за всеки от десетте последни дена на възникване на това събитие, — 5-те най-продължителни събития през последните 365 дни.	— дата и час на начало на събитието, — дата и час на край на събитието, — тип и номер на картата(ите), държава членка, издала картата(ите), както и поколение на всяка карта, вкарана в началото и/или в края на събитието, — брой сходни събития, възникнали същия ден.
Противоречие в данните за движението на превозното средство	— най-продължителното събитие за всеки от десетте последни дена на възникване на това събитие, — 5-те най-продължителни събития през последните 365 дни.	— дата и час на начало на събитието, — дата и час на край на събитието, — тип и номер на картата(ите), държава членка, издала картата(ите), както и поколение на всяка карта, вкарана в началото и/или в края на събитието, — брой сходни събития, възникнали същия ден.
Опит за нарушаване на сигурността	— 10-те най-скорошни събития за всеки тип събитие.	— дата и час на начало на събитието, — дата и час на края на събитие (ако е от значение), — тип и номер на картата(ите), държава членка, издала картата(ите), както и поколение на всяка карта, вкарана в началото и/или в края на събитието, — тип събитие.
Времеви конфликт	— най-продължителното събитие за всеки от десетте последни дена на възникване на това събитие, — 5-те най-продължителни събития през последните 365 дни.	— уред за регистриране на дата и час — дата и час по GNSS, — тип и номер на картата(ите), държава членка, издала картата(ите), както и поколение на всяка карта, вкарана в началото и/или в края на събитието, — брой сходни събития, възникнали същия ден.

1) Уредът за регистриране на данните за движението трябва да регистрира и записва също и в своята памет за данни:

— датата и часа на последния КОНТРОЛ ЗА ПРЕВИШЕНА СКОРОСТ,

— датата и часа на първото превишаване на скоростта, констатирано след този КОНТРОЛ ЗА ПРЕВИШЕНА СКОРОСТ.

— броя на събитията „превишаване на скоростта след последния КОНТРОЛ ЗА ПРЕВИШЕНА СКОРОСТ“.

2) Тези данни могат да бъдат регистрирани само при повторно включване на електрическото захранване, времената могат да бъдат известни с точност до минута.

3.12.9 *Данни за неизправностите*

За целите на настоящата подточка времето се регистрира с разделителна способност 1 секунда.

118) Уредите за регистриране на данните за движението трябва да се опитват да регистрират и записват в своята памет следните данни относно всяка открита неизправност, съгласно следните правила за запис:

Неизправност	Правила за запис в паметта	Данни, които се регистрират при всяка неизправност
Неизправност на картата	— 10-те последни неизправности на картата на водач.	— дата и час на началото на неизправност, — дата и час на края на неизправност, — тип и номер на картата(ите), държава членка, издала картата(ите), поколение.
неизправности в уредите за регистриране на данните за движението	— 10-те последни неизправности за всеки тип неизправност, — първата неизправност след последното калибриране.	— дата и час на началото на неизправност, — дата и час на края на неизправност, — тип на неизправността, — тип и номер на картата(ите), държава членка, издала картата(ите), както и поколение на всяка карта, вкарана в началото и/или в края на неизправността,

3.12.10 *Данни за калибриране*

119) Уредът за регистриране на данните за движението записва и съхранява данни в своята памет, имащи отношение към:

— параметрите на калибрирането, известни в момента на пускането,

— своето най-първо калибриране след пускането си,

— първото си калибриране в превозното средство, на което се намира в момента (идентифицирано от неговия VIN),

— 20-те последни калибрирания (ако няколко калибрирания се извършват в рамките на един календарен ден, са записват само първото и последното за деня).

120) За всяко от тези калибрирания се регистрират следните данни:

— цел на калибрирането (пускане, първо монтиране, монтиране, периодични технически прегледи),

— наименование и адрес на сервиза,

— номер на картата за монтаж и настройки, държава членка, която я е издала, и срок на валидност на картата,

— идентификация на превозното средство,

— актуализирани или потвърдени параметри: w, k, l, размер на гумите, регулировка на ограничителя на скоростта, брояч на километрите (стара и нова стойност), дата и час (стара и нова стойност),

— типовете и идентификаторите на всички поставени пломби.

121) Освен това уредите за регистриране на данните за движението регистрират и записват в паметта си за данни способността си да използват тахографски карти от първо поколение (все още активирани или не).

122) Датчикът за движение трябва да регистрира и записва в паметта си следните данни относно монтирането му:

— първо сдвояване към бордово устройство (дата, час, номер на одобрение на устройството, сериен номер на устройството),

— последно сдвояване с устройство, монтиран на превозното средство (дата, час, сертификационен номер на устройството, сериен номер на устройството).

123) външното устройство за GNSS трябва да регистрира и записва в паметта си следните данни относно монтирането му:

— първо свързване към бордово устройство (дата, час, номер на одобрение на устройството, сериен номер на устройството),

— последно свързване към бордово устройство (дата, час, номер на одобрение на устройството, сериен номер на устройството).

3.12.11 *Данни за сверяване на часовника*

124) Уредът за регистриране на данните за движението трябва да регистрира и записва данни в своята памет, имащи отношение към: сверяванията на часовника, извършени в режим на калибриране извън рамките на периодичното калибриране (опр. буква е)):

— последното сверяване на часовника,

— 5-те най-значителни сверявания на часовника,

125) За всяко от сверяванията на часовника се записват следните данни:

— дата и час, старата стойност,

— дата и час, новата стойност,

— наименование и адрес на сервиза,

— номер на картата за монтаж и настройки, държава членка, която я е издала, поколение на картата и срок на валидност на картата.

3.12.12 *Данни за контролните дейности*

126) Уредите за регистриране на данните за движението записват и съхраняват в своята памет следните данни, имащи отношение към последните 20 контролни дейности:

— дата и час на извършения контрол,

— номер на контролната карта, държава членка, която я е издала, и поколение на картата,

— тип на контрола (изобразяване на данните и/или отпечатване върху хартия и/или изтегляне на данни от бордовото устройство и/или изтегляне на данни от картата и/или пътна проверка на калибрирането).

127) При извършване на изтегляне на данни се регистрират също така датите на най-отдалечения и на най-близкия ден във времето, данните за които са изтеглени.

3.12.13 *Данни за блокирания, извършени от превозвач*

128) Уредите за регистриране на данните за движението трябва да регистрират и записват в паметта си следните данни, имащи отношение към последните 255 блокирания, извършени от превозвача:

— дата и час на блокирането,

— дата и час на разблокирането,

— номер на картата на превозвач, държава членка, която я е издала, и поколение на картата,

— име и адрес на превозвач,

Данните, блокирани преди чрез блокиране, което е заличено от паметта поради горепосоченото ограничение, се разглеждат като неблокирани.

3.12.14 *Изтегляне на данни за дейностите*

129) Уредите за регистриране на данните за движението трябва да регистрират и записват в паметта си следните данни, имащи отношение към последното изтегляне на данни от паметта към външни носители в режим „превозвач“ или „калибриране“:

— дата и час на изтеглянето на данните,

— номер на картата на превозвач или на картата за монтаж и настройки, държава членка, която я е издала, и поколение на картата,

— наименование на превозвача или на сервиза.

3.12.15 *Данни за специфични условия*

130) Уредите за регистриране на данните за движението трябва да регистрират и записват в паметта си следните данни, имащи отношение към специфични условия:

— дата и час на въвеждането,

— тип на специфичното условие.

131) Паметта трябва да може да запазва данните за специфични условия в продължение на най-малко 365 дни (като се предполага, че средно се отваря и затваря 1 условие на ден). Когато капацитетът за съхраняване на данни е изчерпан, новите данни трябва да заместват най-старите данни.

3.12.16 *Данни за тахографските карти*

132) Уредите за регистриране на данните за движението трябва да могат да записват следните данни, свързани с различните тахографски карти, в които са били използвани в бордовото устройство:

— номера на тахографската карта и нейния сериен номер,

— производителя на тахографската карта,

— типа на тахографската карта,

— версията на тахографската карта,

133) Уредите за регистриране на данните за движението трябва да могат да запишат най-малко 88 такива записа.

3.13 **Четене на тахографските карти**

134) Уредите за регистриране на данните за движението трябва при необходимост да могат да четат от тахографски карти от първо и второ поколение необходимите данни:

— идентификация на типа на картата, на титуляря на картата, на използваното преди това превозно средство, на датата и часа на последното изваждане на картата и на дейността, която е била избрана в този момент,

— проверка, че последната картова сесия е била приключена правилно,

— изчисляване на времето на непрекъснато управление на МПС на водача, общото време на прекъсване и на общото време на управление на МПС за предишната и настоящата седмица,

— отпечатване на заявките за разпечатка, свързани с данните, записани на карта на водач,

— изтегляне на данни от карта на водач към външен носител.

Това изискване се прилага само за тахографски карти от първо поколение, ако възможността за използването им не е била премахната от сервиз.

135) При грешка в четенето, уредите за регистриране на данните за движението трябва да правят нов опит, максимум до три пъти, и при наличие на повтарящ се неуспех, да обявят картата за дефектна и невалидна.

3.14 **Регистриране и запис върху тахографски карти**

3.14.1 *Регистриране и запис в тахографски карти от първо поколение*

136) При условие че използването на тахографски карти от първо поколение не е било премахнато от сервиз, уредите за регистриране на данните за движението трябва да регистрират и записват данни точно по същия начин както това би било извършвано от уреди от първо поколение за регистриране на данните за движението.

137) Уредите за регистриране на данните за движението трябва да задават „данните за картовата сесия“ върху картата на водач или картата за монтаж и настройки веднага след вкарването на картата.

138) Уредите за регистриране на данните за движението трябва да актуализират данните, записани върху валидна карта на водач, карта за монтаж и настройки, карта на превозвач и/или контролна карта, с всички необходими данни относно периода, през който картата е вкарана, и отнасящи се за титуляря ѝ. Данните, записвани върху тези карти, са специфицирани в глава 4.

139) Уредите за регистриране на данните за движението трябва да актуализират данните за дейността на водача и местоположенията (като е специфицирано в 4.5.3.1.9 и 4.5.3.1.11), записани върху валидни карта на водач и/или карта за монтаж и настройки, при ръчно въведени от титуляря на картата данни за дейността на водача и местоположенията.

140) Всички събития, които не са дефинирани за уреди за регистриране на данните за движението от първо поколение, не трябва да се записват върху картата на водача и картата за монтаж и настройки.

141) Актуализирането на данните, записани на тахографските карти се извършва по такъв начин, че когато това е необходимо, като се има предвид реалният капацитет за съхраняване на данни, най-новите данни да заместват най-старите данни.

142) При грешка в записването, уредите за регистриране на данните за движението трябва да правят нов опит, максимум до три пъти, и при повтарящ се неуспех да обявяват картата за невалидна.

143) Преди изваждането на карта на водач и след като всички съответни данни са записани върху картата, уредите за регистриране на данните за движението трябва да инициализират „данните за картовата сесия“.

3.14.2 *Регистриране и запис в тахографски карти от второ поколение*

144) Тахографските карти от второ поколение трябва да съдържат 2 различни картови приложения, първото от които следва да бъде точно същото като приложението TACHO на тахографските карти от първо поколение, а второто — приложението „TACHO_G2“, както е специфицирано в глава 4 и допълнение 2.

145) Уредите за регистриране на данните за движението трябва да задават „данните за картовата сесия“ върху картата на водач или картата за монтаж и настройки веднага след вкарването на картата.

146) Уредите за регистриране на данните за движението трябва да актуализират данните, записани върху 2-те картови приложения на валидна карта на водач, карта за монтаж и настройки, карта на превозвач и/или контролна карта, с всички необходими данни относно периода, през който картата е вкарана, и отнасящи се за титуляря ѝ. Данните, записвани върху тези карти, са специфицирани в глава 4.

147) Уредите за регистриране на данните за движението трябва да актуализират данните за местата на дейността на водача и местоположенията (както е специфицирано в 4.5.3.1.9, 4.5.3.1.11, 4.5.3.2.9 и 4.5.3.2.11), записани върху валидни карта на водач и/или карта за монтаж и настройки, при ръчно въведени от титуляря на картата данни за дейността на водача и местоположенията.

148) Актуализирането на данните, записани на тахографските карти се извършва по такъв начин, че когато това е необходимо, като се има предвид реалният капацитет за съхраняване на данни, най-новите данни да заместват най-старите данни.

149) При грешка в записването, уредите за регистриране на данните за движението трябва да правят нов опит, максимум до три пъти, и при повтарящ се неуспех да обявяват картата за невалидна.

150) Преди изваждането на карта на водач и след като всички съответни данни са записани върху двете картови приложения на картата, уредите за регистриране на данните за движението трябва да инициализират „данните за картовата сесия“.

3.15 **Извеждане върху дисплея**

151) Дисплеят трябва да бъде с най-малко 20 символа.

152) Размерът на символите трябва да бъде най-малко 5 mm височина и 3,5 mm широчина.

153) Дисплеят трябва да може да показва символите, определени в допълнение 1, глава 4 „Набори от символи“. Дисплеят може да използва опростено представяне на символите (напр. букви с ударения може да бъдат изобразени без ударенията, а малките букви може да се показват като главни букви).

154) Дисплеят трябва да е снабден с подходящо незаслепяващо осветяване.

155) Показанията трябва да се виждат от външната страна на уредите за регистриране на данните за движението.

156) Уредите за регистриране на данните за движението трябва да могат да изобразяват:

— данните по подразбиране,

— данни, свързани с предупрежденията,

— данни относно достъпа до менютата,

— други данни, поискани от потребителя.

Уредите за регистриране на данните за движението може да изобразяват допълнителна информация при положение, че тя е ясно различима от гореизискваните информации.

157) При изобразяването на данните на уредите за регистриране на данните за движението трябва да се използват пиктограмите или комбинациите от пиктограми, изброени в допълнение 3. Могат да се използват допълнителни пиктограми или комбинации от пиктограми при положение, че те ся ясно различими от горепосочените пиктограми или комбинации от пиктограми.

158) Дисплеят трябва да бъде винаги включен, когато превозното средство е в движение.

159) Уредите за регистриране на данните за движението може да имат ръчна или автоматична функция за изключване на дисплея, когато превозното средство не е в движение.

Форматът на изобразяване на данните е специфициран в допълнение 5.

3.15.1 *Изобразяване по подразбиране*

160) Когато не е необходимо да се показва друга информация, уредите за регистриране на данните за движението трябва да показват по подразбиране следното:

— местното време (координирано универсално време (UTC) + поправка, задавана от водача);

— режима на работа,

— текущата дейност на водача и на втория водач,

— информация относно водача:

— ако неговата текуща дейност е „управление на МПС“ — текущото му време на непрекъснато управление на МПС и текущото му общо време на прекъсване,

— ако неговата текуща дейност не е „управление на МПС“ — текущата продължителност на тази дейност (от момента на нейното избиране) и общото време на прекъсване.

161) Изобразяването на данните относно всеки водач трябва да бъде ясно, просто и недвусмислено. Когато информацията за водача и втория водач не може да бъде изобразена едновременно, уредите за регистриране на данните за движението трябва да изобразяват по подразбиране информацията, отнасяща се за водача, и трябва да позволяват на потребителя да изобрази информацията относно втория водач.

162) Когато широчината на изобразяването не е достатъчна за извеждане по подразбиране на режима на работа, уредите за регистриране на данните за движението трябва за кратко да изобразяват новия режим при всяка негова промяна.

163) При вкарване на нова карта уредите за регистриране на данните за движението трябва да изобразяват за кратко време името на титуляря на картата.

164) Когато е отворено условие „ИЗВЪН ОБСЕГ“ или „ПЪТУВАНЕ С ФЕРИБОТ/ВЛАК“, по подразбиране трябва да се изобрази съответната пиктограма, за да се укаже, че това конкретно условие е отворено (текущата активна дейност на водача може да не се изобразява в същото време).

3.15.2 *Изобразяване на предупреждение*

165) Уредите за регистриране на данните за движението трябва да използват при предупрежденията най-вече пиктограмите, фигуриращи в допълнение 3, допълнени при нужда от информация под формата на цифров код. Може също така да се добави съобщение за предупреждение на езика, избран от водача.

3.15.3 *Меню за достъп*

166) Уредите за регистриране на данните за движението трябва да разполагат с необходимите команди чрез подходящо структурирано меню.

3.15.4 *Изобразяване на други данни*

167) При поискване трябва да бъде възможно избирателно показване на:

— датата и часа по координираното универсално време, както и поправката за местното време,

— съдържанието на която и да е от шестте разпечатки, което да бъде в същия формат както самата разпечатка,

— времето на непрекъснато управление на МПС и общото време на прекъсване от водача,

— времето на непрекъснато управление на МПС и общото време на прекъсване от втория водач;

— общото време на управление от водача за предишната и настоящата седмица,

— времето на непрекъснато управление на МПС на втория водач за предишната и настоящата седмица,

незадължително:

— продължителността на текущата дейност на втория водач (от момента на нейното избиране),

— общото време на управление на МПС на водача за настоящата седмица,

— общото време на управление на МПС на втория водач за настоящия дневен работен период,

— общото време на управление на МПС от водача за настоящия дневен работен период.

168) Изобразяването на съдържанието на разпечатката на хартия е последователно, ред по ред. Ако широчината на изобразяването е по-малка от 24 символа, потребителят може да визуализира цялата информация чрез съответен способ (на няколко реда, изобразяване във вид на безконечен списък, …)

При отпечатването върху хартия, редовете предвидени за ръчното изписване на информация, могат да бъдат изпуснати.

3.16 **Отпечатване**

169) Уредите за регистриране на данните за движението трябва да могат да отпечатват информацията, записана в паметта им и/или върху тахографските карти в съответствие със следните разпечатки на хартия:

— ежедневната разпечатка от картата за дейностите на водача,

— ежедневната разпечатка от бордовото устройство за дейностите на водача,

— разпечатката от картата за събитията и неизправностите,

— разпечатката от бордовото устройство за събитията и неизправностите,

— разпечатка за техническите данни,

— разпечатка за превишаванията на скоростта.

— предистория на данните върху тахографската карта за дадено бордово устройство (вж. глава 3.12.16)

Подробностите относно формата и съдържанието на тези разпечатки са специфицирани в допълнение 4.

В края на разпечатките може да фигурират допълнителни данни.

Уредите за регистриране на данните за движението могат също така да вадят и други разпечатки ако те са ясно различими от гореизброените седем разпечатки.

170) „ежедневната разпечатка от картата за дейностите на водача“ и „разпечатката от картата за събитията и неизправностите“ трябва да са достъпни само когато в уредите за регистриране на данните за движението е вкарана карта на водач или карта за монтаж и настройки. Уредите за регистриране на данните за движението актуализират данните, записани на въпросната карта, преди да стартира отпечатването.

171) За да извадят „ежедневната разпечатка от картата за дейностите на водача“ и „разпечатката от картата за събитията и неизправностите“, уредите за регистриране на данните за движението трябва:

— или да избират автоматично картата на водач, или картата за монтаж и настройки, ако е вкарана само една от тези карти,

— или да имат команда, позволяваща избирането на картата-източник на данните, или да избират картата, поставена в процепа за карта на водач, ако са вкарани и двете карти.

172) Печатащото устройство трябва да може да отпечатва 24 символа на ред.

173) Минималният размер на символите трябва да е височина 2,1 mm и широчина 1,5 mm.

174) Печатащото устройство трябва да може да отпечатва символите, специфицирани в допълнение 1, глава 4, „Набори от символи“.

175) Печатащите устройства трябва да са с такава конструкция, че тези разпечатки да са с ниво на разделителна способност достатъчно, за да се избегне всяка двусмисленост при четенето им.

176) Разпечатките трябва да запазват размерите и съдържанието си при нормалните условия на влажност (10-90 %) и температура.

177) Хартията от одобрен тип, използвана от уредите за регистриране на данните за движението, трябва да бъде със съответен знак за одобрен тип и указание за типа/типовете уреди за регистриране на данните за движението, с който/които може да бъде използвана.

178) Разпечатките трябва да остават четливи и разпознаваеми при нормални условия на съхранение, изразени като светлинен интензитет, влажност и температура, в продължение на най-малко две години.

179) Разпечатките трябва да отговарят минимум на спецификациите за изпитване, определени в допълнение 9.

180) Също така трябва да бъде възможно върху тези документи да се добавят бележки, написани на ръка, като например при подпис на водача.

181) При свършване на хартията по време на разпечатване и след ново зареждане с хартия уредите за регистриране на данните за движението трябва да започват разпечатването отначало или продължават от същото място, като осигуряват недвусмислена връзка с предишната разпечатана част.

3.17 **Предупреждения**

182) Уредите за регистриране на данните за движението трябва да предупреждават водача при откриване на някакво събитие и/или неизправност.

183) Предупреждението относно прекъсване на електрическото захранване може да бъде забавено до момента на възстановяване на захранването.

184) Уредите за регистриране на данните за движението трябва да предупреждават водача 15 минути преди и по време на превишаването на максималното позволено време на непрекъснато управление на МПС.

185) Предупрежденията трябва да бъдат визуални. Освен визуалните предупреждения може да се извършват и звукови предупреждения.

186) Визуалните предупреждения трябва да бъдат ясно различими от потребителя, да се появяват в зрителното поле на водача и да бъдат четливи както през деня, така и през нощта.

187) Визуалните предупреждения могат да бъдат вградени в уредите за регистриране на данните за движението, или да бъдат извън тях.

188) В последния случай те трябва да са означени със символ „Т“.

189) Предупрежденията трябва да са с продължителност не по-малка от 30 секунди, освен ако потребителят потвърди приемането им чрез натискане на един или няколко конкретни бутона на уредите за регистриране на данните за движението. Това първо потвърждаване на приемането на предупреждението не трябва да изтрива изобразяването на причината за предупреждението, посочено в следващия параграф.

190) Причината за съобщението трябва да бъде изобразена на уредите за регистриране на данните за движението и да остане видима докато потребителят потвърди приемането ѝ чрез конкретен бутон или команда на уредите за регистриране на данните за движението.

191) Може да има допълнителни предупреждения, при условие че те не объркват водачите по отношение на дефинираните по-горе.

3.18 **Изтегляне на данни към външни носители**

192) Уредите за регистриране на данните за движението трябва да позволяват при поискване да се изтеглят данни, съхранени в паметта им или от карта на водач към външни носители през съединителя за калибриране/изтегляне на данни. Уредите за регистриране на данните за движението трябва да актуализират данните, записани върху съответната карта, преди да започнат изтеглянето.

193) Освен това като незадължителна функция уредите за регистриране на данните за движението може при всички режими на работа да изтеглят данни по друг начин към превозвач, чието разпознаване е потвърдено чрез този канал. В подобен случай така за изтеглените данни важат правата за достъп, приложими в режим „превозвач“.

194) Изтеглянето на данни не трябва нито да променя, нито да изтрива записаните данни.

195) Електрическият интерфейс за съединителя за калибриране/изтегляне на данни е специфициран в допълнение 6.

196) Протоколите за изтегляне на данни са специфицирани в допълнение 7.

3.19 **Връзка от разстояние за извършване на целенасочени пътни проверки**

197) Когато контактният ключ на превозното средство е в положение „ВКЛЮЧЕН“, бордовото устройство трябва да записва на всеки 60 секунди в устройството за връзка от разстояние най-новите данни, необходими за извършване на целенасочени пътни проверки. Тези данни трябва да са кодирани и с подпис, както е специфицирано в допълнение 11 и допълнение 14.

198) Данните, които се проверяват от разстояние, трябва да бъдат на разположение на четците за връзка от разстояние чрез безжична комуникация от разстояние, както е специфицирано в допълнение 14.

199) Данните, необходими за извършване на целенасочени пътни проверки, трябва да се отнасят за:

— последния опит за нарушаване на сигурността,

— най-дълго прекъсване на електрическото захранване,

— неизправност на датчика,

— грешка в данните за движението,

— противоречие в данните за движението на превозното средство,

— управление без валидна карта,

— вкарване на карта по време на управление на МПС,

— данни за сверяването на часовника,

— данни за калибриране, включително датите на последните две записани калибрирания,

— регистрационния номер на превозното средство,

— скоростта, регистрирана от тахографа.

3.20 **Данни, прехвърляни към допълнителни външни устройства**

200) Уредите за регистриране на данните за движението могат да са оборудвани със стандартизирани интерфейси, позволяващи регистрираните или генерираните от тахографите данни да се използват в работен режим от външно устройство.

В допълнение 13 е дефиниран и стандартизиран незадължително интерфейс с ITS. С него могат да съществуват съвместно други подобни интерфейси, при условие че напълно съответстват на изискванията от допълнение 13 по отношение на минималния списък от данни, сигурността и съгласието на водача.

за данните ITS предоставяни чрез този интерфейс важат следните изисквания:

— тези данни представляват набор от избрани съществуващи данни от речника на данните на тахографа (допълнение 1),

— поднабор на тези избрани данни са отбелязани като „лични данни“,

— поднаборът „лични данни“ е достъпен само ако е активирано удостоверимото съгласие на водача, който приема личните му данни да могат да напускат мрежата на превозното средство.

— Във всеки един момент, съгласието на водача може да бъде активирано или дезактивирано чрез команди от менюто, при условие че е вкарана картата на водач.

— наборът и поднаборът от данни се излъчва чрез безжичния протокол Bluetooth с обхват кабината на превозното средство при честота на обновяване 1 минута,

— сдвояването на външното устройство с интерфейса с ITS ще бъде защитено чрез специален за целта и случаен PIN от най-малко 4 числа, записани във и достъпни чрез дисплея на всяко бордово устройство.

— при всички обстоятелства, наличието на интерфейса с ITS не може да наруши или да се отрази на правилната работа и сигурността на бордовото устройство.

Може да има и други изходни данни освен набора от подбрани съществуващи данни, разглеждани като минимален списък, при условие че те не могат да бъдат считани за лични данни.

Уредите за регистриране на данните за движението трябва да уведомяват други външни устройства за съгласието на водача.

Когато контактният ключ на превозното средство е в положение ВКЛЮЧЕН ДВИГАТЕЛ, тези данни могат да бъдат излъчвани постоянно.

201) Серийният интерфейс, както е специфициран в приложение 1Б към Регламент (ЕИО) № 3821/85, последно изменен, може да продължи да бъде наличен в тахографите с цел обратна съвместимост. Независимо от това, в случай че се предават лични данни е необходимо съгласието на водача.

3.21 **Калибриране**

202) Функцията за калибриране трябва да позволява:

— автоматичното сдвояване на датчика за движение с бордовото устройство,

— автоматично свързване на външното устройство за GNSS с бордовото устройство, ако е приложимо,

— цифрово адаптиране на константата (k) на уредите за регистриране на данните за движението към характеристичния коефициент на превозното средство (w),

— коригиране на текущото време в рамките на срока на валидност на вкараната карта за монтаж и настройки,

— коригиране на текущата стойност на километражния брояч,

— актуализиране на данните за идентификация на датчика за движение, записани в паметта за данни,

— ако е приложимо, актуализиране на данните за идентификация на външното устройство за GNSS, записани в паметта за данни,

— актуализиране на типовете и идентификаторите на всички поставени пломби,

— актуализиране или потвърждаване на други параметри, известни на уредите за регистриране на данните за движението: идентификация на превозното средство, w, l, размер на гумите и настройка на ограничителя на скоростта, ако е приложимо.

203) Освен това функцията за калибриране трябва да позволява потискане на използването на тахографски карти от първо поколение в уредите за регистриране на данните за движението, при положение че са изпълнени условията, формулирани в допълнение 15.

204) Сдвояването на датчика за движение с бордовото устройство, трябва да се състои най-малкото във:

— актуализиране на данните за монтирането на датчика за движение, намиращи се в него (при необходимост),

— копиране от паметта за данни на датчика за движение в тази на бордовото устройство на необходимите данни за идентификация на датчика за движение.

205) Свързването на външното устройство за GNSS с бордовото устройство трябва да се състои най-малкото във:

— актуализиране на данните за монтирането на външното устройство за GNSS, намиращи се във външното устройство за GNSS (при необходимост),

— копиране от външното устройство за GNSS към паметта за данни на бордовото устройство на необходимите данни за идентификация на външното устройство за GNSS, включително серийния му номер.

Свързването трябва да бъде последвано от проверка на информацията за местоположението от GNSS.

206) Функцията за калибриране трябва да позволява въвеждането на необходимите данни посредством съединителя за калибриране /изтегляне в съответствие с протокола за калибриране, дефиниран в допълнение 8. Функцията за калибриране може също така да позволява въвеждането на необходимите данни по други начини.

3.22 **Пътна проверка на калибрирането**

207) Функцията за пътна проверка на калибрирането трябва да позволява прочитане на серийния номер на датчика за движение (евентуално намиращ се в адаптера) и серийния номер на външното устройство за GNSS (когато е приложимо), свързани към бордовото устройство към момента на поискването.

208) Това прочитане трябва да бъде възможно поне на дисплея на бордовото устройство чрез команди от менюто.

209) Функцията за пътна проверка на калибрирането трябва да позволява също управление на избора на входно-изходния режим на входно-изходната сигнална линия за калибриране, специфицирана в допълнение 6, посредством интерфейса на линията K. Това се извършва чрез ECUAdjustmentSession, както е специфицирано в допълнение 8, раздел 7 „Управление на изпитвателните импулси — Функционален блок за управление на вход/изход“.

3.23 **Сверяване на часовника**

210) Функцията за сверяване на часовника трябва да позволява автоматичното сверяване на текущото време. За сверяване на часовника, в уредите за регистриране на данните за движението се използват два времеви източника: 1) вътрешният часовник на БУ, 2) приемникът на сигнали от GNSS.

211) Настройката на часа вътрешния часовник на бордовото устройство трябва да се коригира автоматично на интервали от най-много 12 часа. Когато този срок е изтекъл и няма сигнал от GNSS, настройката на часа трябва да се извършва веднага след веднага след като бордовото устройство получи достъп до валидно време от приемника на сигнали от GNSS според условията за запалването на двигателя. Еталонното време за автоматичната настройка на часа на вътрешния часовник на бордовото устройство трябва да се получава от приемника на сигнали от GNSS. Ако текущото време се отклонява с повече от една (1) минута от времевата информация, постъпваща от приемника на сигнали от GNSS, трябва да бъде предизвикано събитие на времеви конфликт.

212) Функцията за сверяване на часовника трябва да позволява също предизвикано сверяване на текущото време в режим на калибриране.

3.24 **Експлоатационни характеристики**

213) Бордовото устройство трябва да е напълно работоспособен в температурен обхват от – 20°C до 70°C, външното устройство за GNSS в температурен обхват от – 20°C до 70°C, а датчикът за движение — в температурен обхват от – 40°C до 135°C. Съдържанието на паметта трябва да се запазва при температури до – 40°C.

214) Тахографът трябва да е напълно работоспособен в обхват за влажността от 10 % до 90 %.

215) Пломбите, използвани в интелигентния тахограф, трябва да издържат на същите условия като тези, приложими за компонентите на тахографа, към които те са закрепени.

216) Уредите за регистриране на данните за движението трябва да са защитени срещу пренапрежения, размяна на полярността на електрическото им захранване и къси съединения.

217) Датчиците за движение трябва или:

— да реагират на магнитно поле, което смущава установяването на движението на превозното средство. При такива обстоятелства бордовото устройство регистрира и записва неизправност в датчика (изискване 88) или

— да има чувствителен елемент, който е защитен срещу магнитни полета или е устойчив на такива.

218) Уредите за регистриране на данните за движението и външното устройство за GNSS трябва да съответстват на международното Правило №10 на ИКЕ на ООН, и трябва да са защитени срещу електростатични разряди и преходни процеси.

3.25 **Материали**

219) Всички елементи, съставящи уредите за регистриране на данните за движението, трябва да бъдат от материали с достатъчна стабилност и механична здравина, и да имат стабилни електрически и магнитни характеристики.

220) Всички вътрешни части на уредите трябва да бъдат защитени от влага и прах при нормалните условия на употреба.

221) Бордовото устройство и външното устройство за GNS, трябва да отговарят на степен на защита IP 40, а датчикът за движение — на степен на защита IP 64 по смисъла на стандарт IEC 2013:1989 включително A1:1999 и A2:2013.

222) Уредите за регистриране на данните за движението трябва да отговарят на техническите спецификации, свързани с ергономичното проектиране.

223) Уредите за регистриране на данните за движението трябва да бъдат защитени от случайни повреждания.

3.26 **Маркировки**

224) Ако уредите за регистриране на данните за движението визуализират скоростта и километража на превозното средство, следните детайли трябва да бъдат изобразени:

— до числото, указващо изминатото разстояние, мерната единица за разстояние, дадена със съкращението „km“,

— до числото, показващо скоростта, указанието „km/h“.

Уредите за регистриране на данните за движението може също така да бъдат превключени да изобразяват скоростта в мили в час, като в този случай мерната единица за скоростта трябва да е указана със съкращението „mph“. Уредите за регистриране на данните за движението може също така да бъдат превключени да изобразяват разстоянието в мили, като в този случай мерната единица за разстоянието трябва да е указана със съкращението „mi“.

225) На всеки компонент, който е отделен от уредите за регистриране на данните за движението, трябва да се постави указателна табелка със следните данни:

— наименование и адрес на производителя,

— фабричен номер от производителя и година на производство на уреда,

— сериен номер на уреда,

— знак за одобрение на уреда.

226) Когато няма физическо място за изобразяване на всички горепосочени данни, указателната табелка трябва да указва най-малко следното: наименованието и логотипа на производителя, както и фабричния номер.

4 КОНСТРУКТИВНИ И ФУНКЦИОНАЛНИ ИЗИСКВАНИЯ ЗА ТАХОГРАФСКИТЕ КАРТИ

4.1 **Видими данни**

Лицевата страна трябва да съдържа:

227) думите „карта на водач“ или „контролна карта“ или „карта за монтаж и настройки“ или „карта на превозвач“, отпечатани с главни букви на официалния(ите) език(езици) на държавата членка, която е издала картата, според типа карта.

228) наименованието на държавата членка, която издала картата (незадължително);

229) отличителния знак на държавата членка, издала картата, отпечатан в бяло на син фон в правоъгълник, ограден от 12 жълти звезди. Отличителните знаци са както следва:

B	Белгия	LV	Латвия
BG	България	L	Люксембург
CZ	Чешка република	LT	Литва
CY	Кипър	M	Малта
DK	Дания	NL	Нидерландия

D EST	Германия Естония	A PL	Австрия Полша
GR	Гърция	P RO SK SLO	Португалия Румъния Словакия Словения
E	Испания	FIN	Финландия
F HR H	Франция Хърватия Унгария	S	Швеция
IRL	Ирландия	UK	Обединено кралство
I	Италия		

230) информация, специфична за издадената карта, номерирана както следва:

	Карта на водач	Контролна карта	Карта на превозвач или карта за монтаж и настройки
1.	фамилно име на водача	наименование на контролния орган	наименование на превозвача или на сервиза
2.	собствено(и) име(на) на водача	фамилно име на контрольора (ако е приложимо)	фамилно име на титуляря на картата (ако е приложимо)
3.	дата на раждане на водача	собствено(и) име(на) на контрольора (ако е приложимо)	собствено(и) име(на) на титуляря на картата (ако е приложимо)
4.а	дата на начало на валидността на картата		
4.б	срок на валидност на картата		
4.в	наименование на органа, който я е издал (може да се отпечата на обратната страна)		
4.г	номер, различен от указания в точка 5, по административни причини (незадължително)		
5.а	Номер на свидетелството за управление на МПС (към датата на издаване на картата на водач)	—	—
5.б	Номер на картата		
6.	Снимка на водача	снимка на контрольора (незадължително)	снимка на монтьора (незадължително)

	Карта на водач	Контролна карта	Карта на превозвач или карта за монтаж и настройки
7.	Подпис на титуляря (незадължително)		
8.	Обичайно място на пребиваване или пощенски адрес на титуляря (незадължително)	Пощенски адрес на контролния орган	Пощенски адрес на превозвача или на сервиза

231) датите трябва да са написани в следния формат „дд/мм/гггг“ или „дд.мм.гггг“ (ден, месец, година).

Обратната страна трябва да съдържа:

232) легенда на номерираните позиции, налични върху лицевата страна на картата;

233) с изрично писмено съгласие на титуляря на картата, може да бъде добавена и информация, която не е свързана с администрирането на картата, при положение че това добавяне не променя с нищо използването на модела като тахографска карта.

234) Преобладаващите цветове на фона при отпечатването на тахографските карти трябва да бъдат както следва:

— карта на водач: бял,

— контролна карта: син,

— карта за монтаж и настройки: червен,

— карта на превозвач: жълт.

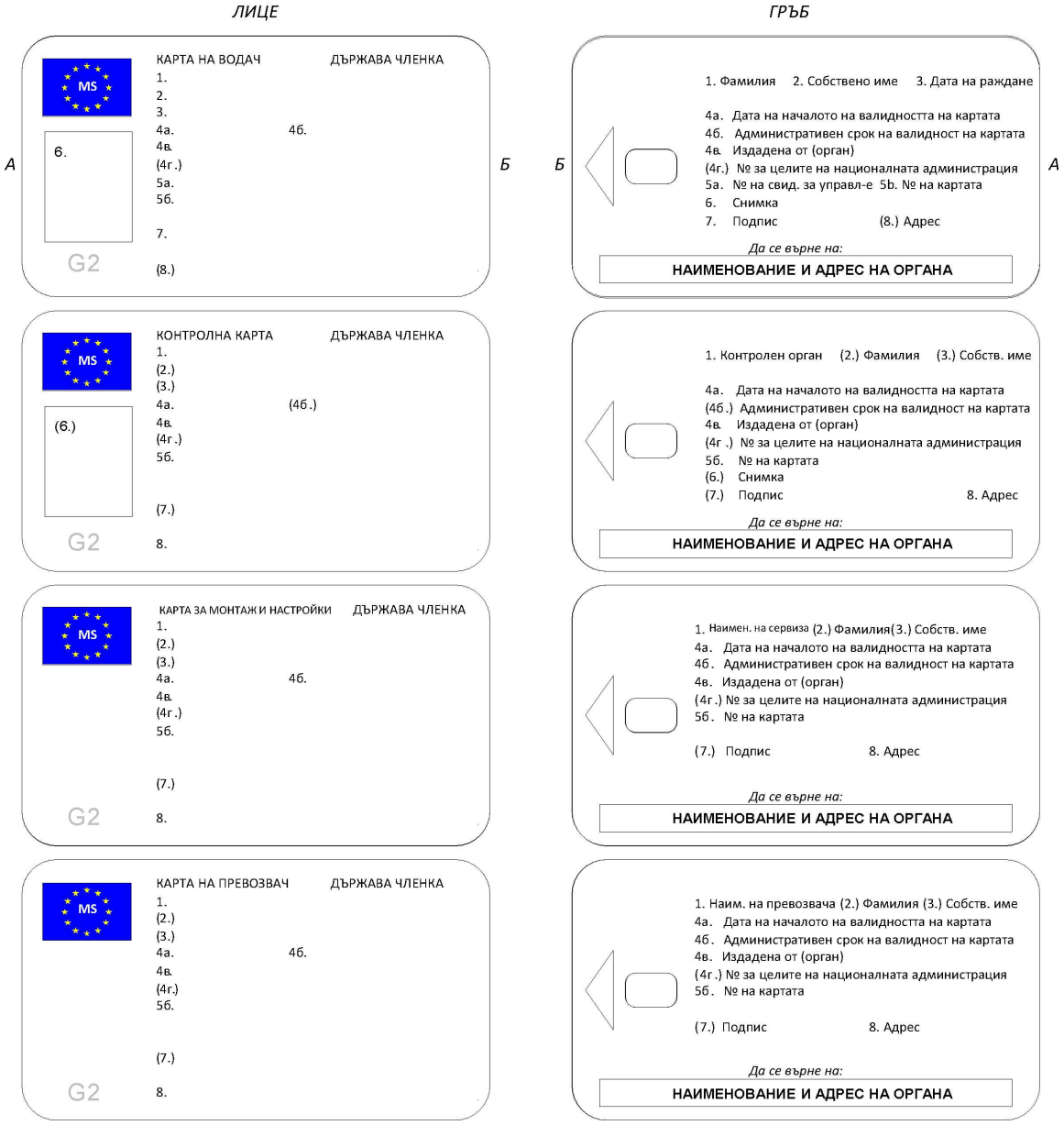
235) Тахографските карти трябва да имат следните елементи на защита на тялото на картата срещу подправяне и фалшифициране:

— фон със защитни характеристики, включващ мотиви с плетеници (гилоши) от тънки линии и ирисов печат,

— припокриване на фоновия защитен печат и на снимката,

— поне една двуцветна линия с микропечат.

ОБРАЗЕЦ НА ОБЩНОСТТА ЗА ТАХОГРАХФСКИ КАРТИ



236) След консултация с Комисията държавите членки могат да добавят цветове или маркировки, като например националните символи и защитни елементи, без това да засяга другите разпоредби на настоящото приложение.

237) Временните карти, посочени в член 26.4 от Регламент (ЕС) №165/2014, трябва да съответстват на разпоредбите на настоящото приложение.

4.2 Сигурност

Сигурността на системата цели да предпази целостта и автентичността на данните, обменяни между картите и уредите за регистриране на данните за движението, както и целостта и автентичността на данните, прехвърляни от карти, като позволява единствено извършването на някои операции по записване на данни върху картите на уредите за регистриране на данните за движението, дешифриране на определени данни като изключва всяка възможност за фалшифициране на данните, съхранени на картата, и като открива всякакъв опит от този вид.

238) С цел постигане на сигурност на системата, тахографските карти трябва да отговарят на изискванията за сигурност, дефинирани в допълнения 10 и 11.

239) Тахографските карти трябва да могат да бъдат четени от други устройства, като например персонални компютри.

4.3 **Стандарти**

240) Тахографските карти трябва да отговарят на следните стандарти:

— ISO/IEC 7810 — Идентификационни карти — физични характеристики,

— ISO/IEC 7816 Идентификационни карти — Карти с интегрална схема:

— Част 1: Физични характеристики,

— Част 2: Размери и разположение на контактите (ISO/IEC 7816-2: 2007),

— Част 3: Електрически интерфейс и протоколи за предаване (ISO/IEC 7816-3:2006),

— Част 4: Организация, сигурност и команди за обмен (ISO/IEC 7816-4:2013 + Cor 1:2014),

— Част 6: Вътрешноотраслови елементи от данни за взаимен обмен (ISO/IEC 7816-6:2004 + Cor 1:2006),

— Част 8: Команди за операции по сигурността (ISO/IEC 7816-8:2004).

— Тахографските карти се изпитват в съответствие със стандарта ISO/IEC 10373-3: 2010 Идентификационни карти — методи за изпитване — Част 3: Карти с интегрална(и) схема(и) с контакти и съответни интерфейсни устройства

4.4 **Спецификации във връзка с околната среда и електрически спецификации**

241) Тахографските карти трябва да могат да функционират правилно при всички климатични условия, които нормално се наблюдават на територията на Общността и в минимален температурен интервал от – 25 °C до + 70 °C, с моментни върхови стойности до + 85 °C, като „моментни“ означава продължителност под 4 часа и не повече от 100 пъти по време на живота на картата.

242) Тахографските карти трябва да могат да функционират правилно при интервал на влажността от 10 % до 90 %.

243) Тахографските карти трябва да могат да функционират правилно през период от пет години, ако се използват в рамките на спецификациите във връзка с околната среда и електрическите спецификации.

244) При функционирането си тахографските карти трябва да са в съответствие с Правило № 10 на ИКЕ на ООН, отнасящо се за електромагнитната съвместимост и да бъдат защитени срещу електростатични разряди.

4.5 **Записване на данни**

За целите на настоящата точка,

— часовете се регистрират с точност от една минута, освен ако не е предвидено друго,

— стойностите от километражния брояч се регистрират с разделителна способност един километър,

— скоростите се регистрират с разделителна способност 1 km/h,

— местоположенията (ширини и дължини) се регистрират в градуси и минути, с разделителна способност 1/10 от минутата.

Функциите, командите и логическите структури на тахографските карти, които отговарят на изискванията относно записването на данните, са указани в допълнение 2.

Ако не е предвидено друго, записването на данни върху тахографските карти трябва да бъде организирано по такъв начин, че новите данни да заместват най-старите записани данни, в случай че предвиденият размер за конкретните записи се изчерпа.

245) В настоящия параграф се специфицира минималният капацитет за съхраняване на данни за различните файлове с данни на приложенията. Тахографските карти трябва да могат да указват на уредите за регистриране на данните за движението реалния капацитет за съхранение на тези файлове с данни.

246) Всякакви допълнителни данни, които могат да бъдат записвани на тахографски карти и свързани с други приложения, евентуално намиращи се в картата, се записват в съответствие с Директива 95/46/ЕО с Директива 2002/58/ЕО и в съответствие с член 7 от Регламент (ЕС) № 165/2014.

247) Всеки главен файл (MF) на която и да било тахографска карта трябва да съдържа до пет елементарни файла (EF) за управление на картата, идентификация на приложенията и на чипа, както и два специализирани файла (DF):

— DF Tachograph, който съдържа приложението, достъпно за бордови устройства от първо поколение, присъстващо и в тахографските карти от първо поколение,

— DF Tachograph_G2, който съдържа приложението, достъпно само за бордови устройства от второ поколение, присъстващо само в тахографските карти от второ поколение.

Пълните подробности за структурата на тахографските карти, са специфицирани в допълнение 2.

4.5.1 *Елементарни файлове за идентификация на управление на картата*

4.5.2 *Идентификация на картите с интегрална(и) схема(и)*

248) Тахографските карти трябва да могат да съхраняват следните данни за идентификация на карти с чип:

— спиране на тактовия генератор,

— сериен номер на картата (включително справочни данни за производството),

— номер на одобрението на картата,

— идентификация на организацията за персонализиране на картата (ID),

— идентификация на интегратора,

— идентификатор на интегралната схема.

4.5.2.1 Идентификация на интегралната схема

249) Тахографските карти трябва да могат да съхраняват следните данни за идентификация на интегралната схема:

— сериен номер на интегралната схема,

— справочни данни за производството на интегралната схема.

4.5.2.2 DIR (има го само в тахографските карти от второ поколение)

250) Тахографските карти трябва да могат да съхраняват обектите от данни за идентификация на приложенията, посочени в допълнение 2.

4.5.2.3 Информация за отговора на инициализиране (ATR) (условна, има я само в тахографските карти от второ поколение).

251) Тахографските карти трябва да могат да съхраняват следния обекта от данни с увеличена дължина:

— в случай че тахографската карта дава възможност за полета с увеличена дължина — обекта от данни с увеличена дължина, специфициран в допълнение 2.

4.5.2.4 Информация за увеличена дължина (условна, има я само в тахографските карти от второ поколение).

252) Тахографските карти трябва да могат да съхраняват следните обекти от данни с увеличена дължина:

— в случай че тахографската карта дава възможност за полета с увеличена дължина — обектите от данни с увеличена дължина, специфициран в допълнение 2.

4.5.3 *Карта на водач*

4.5.3.1 Тахографско приложение (достъпно за бордови устройства от първо и второ поколение)

4.5.3.1.1 Идентификация на приложенията

253) Картата на водач трябва да позволява съхраняването на следните данни за идентификация на приложението:

— идентификация на тахографското приложение,

— идентификация на типа тахографска карта.

4.5.3.1.2 Ключ и сертификати

254) Картата на водач трябва да позволява съхраняването определен брой криптографски ключове и сертификати, както е посочено в допълнение 11, част А.

4.5.3.1.3 Идентификация на картата

255) Картата на водач трябва да позволява съхраняването на следните данни за идентификация на картата:

— номер на картата,

— държава членка, издала картата, наименование на органа, който я е издал, дата на издаване,

— дата на начало на валидността на картата, дата на край на валидността.

4.5.3.1.4 Идентификация на титуляря на картата

256) Картата на водач трябва да позволява съхраняването на следните данни за идентификация на титуляря на картата:

— фамилно име на титуляря,

— собствено(и) име(на) на титуляря,

— дата на раждане,

— предпочитан език.

4.5.3.1.5 Изтегляне на данни от карта

257) Картата на водач трябва да позволява съхраняването на следните данни относно изтеглянето на данни от нея:

— дата и час на последното изтегляне на данни от картата (с цел, различна от извършването на контрол).

258) Картата на водача трябва да позволява съхраняването на един такъв запис.

4.5.3.1.6 Информация за свидетелството за управление

259) Картата на водач трябва да позволява съхраняването на следните данни за свидетелството за управление:

— държава членка, наименование на органа, който го е издал,

— номер на свидетелството за управление (към датата на издаване на картата).

4.5.3.1.7 Данни за събития

За целите на настоящата подточка времето се регистрира с разделителна способност 1 секунда.

260) Картата на водача трябва да позволява съхраняването на данните, свързани със следните събития, засечени от уредите за регистриране на данните за движението по времето, когато картата е вкарана:

— Припокриване във времето (когато дадената карта е причина за събитието),

— Вкарване на карта по време на управление на МПС (когато събитието засяга дадената карта),

— Неправилно приключване на предишна сесия (когато събитието засяга дадената карта),

— Прекъсване на електрическото захранване,

— Грешка в данните за движението,

— Опити за нарушаване на сигурността.

261) Картата на водач трябва да позволява съхраняването на следните данни за тези събития:

— Код на събитието,

— Дата и час на начало на събитието (или на вкарването на картата в случай, че в този момент събитието е било текущо),

— Дата и час на край на събитието (или на изваждането на картата в случай, че в този момент събитието е било текущо),

— VRN и държава членка, извършила регистрацията на превозното средство, в което събитието е настъпило.

Забележка: За събитието „Припокриване във времето“:

— Датата и часът на началото на събитието трябва да съответстват на датата и часа на изваждане на картата от предишното превозно средство,

— Датата и часът на края на събитието трябва да съответстват на датата и на часа на вкарването на картата в настоящото превозно средство,

— Данните за превозното средство трябва да съответстват на настоящото превозно средство, в което събитието се е случило.

Забележка: За събитието „Неправилно приключване на предишната сесия“:

— Датата и часът на началото на събитието трябва да съответстват на датата и на часа на вкарването на картата, съответстващо на неправилно приключената сесия,

— Датата и часът на края на събитието трябва да съответстват на датата и на часа на вкарването на картата за сесията, по време на която събитието е засечено (текуща сесия),

— Данните за превозното средство трябва да съответстват на превозното средство, в което сесията не е била приключена правилно.

262) Картата на водач трябва да позволява съхраняването на данните за шестте последни събития от всеки тип (т.е. 36 събития).

4.5.3.1.8 Данни за неизправностите

За целите на настоящата подточка времето се регистрира с разделителна способност 1 секунда.

263) Картата на водача трябва да позволява съхраняването на данните, свързани със следните неизправности, засечени от уредите за регистриране на данните за движението по времето, когато картата е била вкарана:

— Неизправност на картата (когато събитието засяга дадената карта),

— Неизправност в уредите за регистриране на данните за движението.

264) Картата на водач трябва да позволява съхраняването на следните данни за тези неизправности:

— Код на неизправността,

— Дата и час на начало на неизправността (или на вкарването на картата, в случай че неизправността е била текуща в този момент),

— Дата и час на край на неизправността (или на изваждането на картата, в случай че неизправността е била текуща в този момент),

— VRN и държава членка, извършила регистрацията на превозното средство, в което се е появила неизправността.

265) Картата на водач трябва да позволява съхраняването на данните за дванайсетте последни неизправности от всеки тип (т.е. 24 неизправности).

4.5.3.1.9 Данни за дейностите на водача

266) Картата на водач трябва да позволява съхраняването на следните данни за всеки календарен ден, в който тя се използва, или в който водачът е въвел ръчно дейностите си:

— датата;

— брояч на присъствените дни (който се увеличава с една единица за всеки от тези календарни дни),

— общо разстояние, изминато от водача през този ден,

— статус на водача в 00:00 часа,

— всякакви промени в дейността на водача и/или промени в обстановката при управление на МПС, и/или вкарване или изваждане на картата на водач:

— състояние при управление на МПС (ЕКИПАЖ, САМ),

— процеп (ВОДАЧ, ВТОРИ ВОДАЧ),

— положение на картата (ВКАРАНА, НЕВКАРАНА),

— дейност (управление на МПС, НА РАЗПОЛОЖЕНИЕ, РАБОТА, ПРЕКЪСВАНЕ/ПОЧИВКА),

— час на промяната.

267) Паметта на картата на водач трябва да позволява съхраняването на данните за дейността на водача в продължение на най-малко 28 дни (средната дейност на водач се определя като 93 промени на дейността на ден).

268) Данните, изброени в изисквания 261, 264 и 266 трябва да бъдат съхранени по начин, позволяващ дейностите да бъдат открити по реда на тяхното настъпване, дори в случай на припокриване във времето.

4.5.3.1.10 Данни за използваното превозно средство

269) Картата на водач трябва да позволява съхраняването за всеки календарен ден, в който тя се използва, и за всеки период на използване на определено превозно средство през този ден (периодът на използване включва всички последователни цикли на вкарване/изваждане на картата в превозното средство, като се има предвид самата карта), следните данни:

— дата и час на първото използване на превозното средство (т.е. първото вкарване на картата за този период на употреба на превозното средство, или 00:00 часа, ако периодът на използване е протичал по това време),

— стойност на километражния брояч на превозното средство в този момент,

— дата и час на последното използване на превозното средство (тоест последното изваждане на картата за този период на употреба на превозното средство, или 23:59 часа, ако периодът на използване е протичал по това време),

— стойност на километражния брояч на превозното средство в този момент,

— VRN и държава членка, извършила регистрацията на превозното средство.

270) Картата на водача трябва да позволява съхраняването 84 такива записа.

4.5.3.1.11 Места, където дневните периоди на работа започват и/или завършват

271) Картата на водач трябва да позволява съхраняването на следните данни относно местоположенията, където дневните периоди на работа започват и/или завършват, въведени от водача:

— дата и час на въвеждането (или дата и час, свързани с въвеждането, когато то се извършва по време на процедурата по ръчно въвеждане),

— типа на въвежданата информация (начало или край, условия на въвеждане на информацията),

— въведените страна и област,

— стойността от километражния брояч на превозното средство.

272) Картата на водача трябва да позволява съхраняването най-малко 42 двойки такива записи.

4.5.3.1.12 Данни за картовата сесия

273) Картата на водач трябва да позволява съхраняването на следните данни относно превозното средство, в което е отворена текущата сесия:

— дата и час на отваряне на сесията (тоест на вкарване на картата), с точност до една секунда,

— VRN и държава членка, извършила регистрацията на превозното средство.

4.5.3.1.13 Данни за контролните дейности

274) Картата на водач трябва да позволява съхраняването на следните данни относно контролните дейности:

— дата и час на извършения контрол,

— номер на контролната карта, държава членка, която я е издала,

— вид на проверката (изобразяване на данните и/или отпечатване и/или изтегляне на данни от БУ и/или изтегляне на данни от картата (виж забележката)),

— изтеглен период, в случай на изтегляне,

— VRN и държава членка, извършила регистрацията на превозното средство, в което е извършена проверката.

Забележка: изтеглянето от картата се регистрира само ако се извърши чрез уреди за регистриране на данните за движението.

275) Картата на водач трябва да позволява съхраняването на един такъв запис.

4.5.3.1.14 Данни за специфични условия

276) Картата на водач трябва да позволява съхраняването на следните данни, свързани със специфични условия, въведени докато картата е била вкарана (независимо в кой процеп):

— дата и час на въвеждането,

— тип на специфичното условие.

277) Картата на водач трябва да позволява съхраняването минимум 56 такива записа.

4.5.3.2 Тахографско приложение от поколение 2 (не е достъпно за бордово устройство от първо поколение)

4.5.3.2.1 Идентификация на приложенията

278) Картата на водач трябва да позволява съхраняването на следните данни за идентификация на приложението:

— Идентификация на тахографското приложение,

— Идентификация на типа тахографска карта.

4.5.3.2.2 Ключове и сертификати

279) Картата на водач трябва да позволява съхраняването определен брой криптографски ключове и сертификати, както е посочено в допълнение 11, част Б.

4.5.3.2.3 Идентификация на картата

280) Картата на водач трябва да позволява съхраняването на следните данни за идентификация на картата:

— номер на картата,

— държава членка, издала картата, наименование на органа, който я е издал, дата на издаване,

— дата на начало на валидността на картата, дата на край на валидността.

4.5.3.2.4 Идентификация на титуляря на картата

281) Картата на водач трябва да позволява съхраняването на следните данни за идентификация на титуляря на картата:

— фамилно име на титуляря,

— собствено(и) име(на) на титуляря,

— дата на раждане,

— предпочитан език.

4.5.3.2.5 Изтегляне на данни от карта

282) Картата на водач трябва да позволява съхраняването на следните данни относно изтеглянето на данни от нея:

— дата и час на последното изтегляне на данни от картата (с цел, различна от извършването на контрол).

283) Картата на водач трябва да позволява съхраняването на един такъв запис.

4.5.3.2.6 Информация за свидетелството за управление

284) Картата на водач трябва да позволява съхраняването на следните данни за свидетелството за управление:

— държава членка, наименование на органа, който го е издал,

— номер на свидетелството за управление (към датата на издаване на картата).

4.5.3.2.7 Данни за събития

За целите на настоящата подточка времето се регистрира с разделителна способност 1 секунда.

285) Картата на водач трябва да позволява съхраняване на данните, свързани със следните събития, засечени от уредите за регистриране на данните за движението по времето, когато картата е била вкарана:

— Припокриване във времето (когато дадената карта е причина за събитието),

— Вкарване на карта по време на управление на МПС (когато събитието засяга дадената карта),

— Неправилно приключване на предишна сесия (когато събитието засяга дадената карта),

— Прекъсване на електрическото захранване,

— Грешка в комуникацията с устройството за връзка от разстояние,

— Събитие „Липса на информация за местоположението от приемник на сигнали от GNSS“

— Грешка в комуникацията с външното устройство за GNSS

— Грешка в данните за движението,

— Противоречие в данните за движението на превозното средство

— Опити за нарушаване на сигурността,

— Времеви конфликт.

286) Картата на водач трябва да позволява съхраняването на следните данни за тези събития:

— Код на събитието,

— Дата и час на начало на събитието (или на вкарването на картата в случай, че събитието е било текущо за този момент),

— Дата и час на край на събитието (или на изваждането на картата в случай, че в този момент събитието е било текущо),

— VRN и държава членка, извършила регистрацията на превозното средство, в което събитието е настъпило.

Забележка: За събитието „Припокриване във времето“:

— Датата и часът на началото на събитието трябва да съответстват на датата и часа на изваждане на картата от предишното превозно средство,

— Датата и часът на края на събитието трябва да съответстват на датата и на часа на вкарването на картата в настоящото превозно средство,

— Данните за превозното средство трябва да съответстват на настоящото превозно средство, в което събитието се е случило.

Забележка: За събитието „Неправилно приключване на предишната сесия“:

— Датата и часът на началото на събитието трябва да съответстват на датата и на часа на вкарването на картата, съответстващо на неправилно приключената сесия,

— Датата и часът на края на събитието трябва да съответстват на датата и на часа на вкарването на картата за сесията, по време на която събитието е засечено (текуща сесия),

— Данните за превозното средство трябва да съответстват на превозното средство, в което сесията не е била приключена правилно.

287) Картата на водач трябва да позволява съхраняването на данните за шестте последни събития от всеки тип (т.е. 66 събития).

4.5.3.2.8 Данни за неизправностите

За целите на настоящата подточка времето се регистрира с разделителна способност 1 секунда.

288) Картата на водача трябва да позволява съхраняването на данните, свързани със следните неизправности, засечени от уредите за регистриране на данните за движението по времето, когато картата е била вкарана:

— Неизправност на картата (когато събитието засяга дадената карта),

— Неизправност в уредите за регистриране на данните за движението.

289) Картата на водач трябва да позволява съхраняването на следните данни за тези неизправности:

— Код на неизправността,

— Дата и час на начало на неизправността (или на вкарването на картата, в случай че неизправността е била текуща в този момент),

— Дата и час на край на неизправността (или на изваждането на картата, в случай че неизправността е била текуща в този момент),

— VRN и държава членка, извършила регистрацията на превозното средство, в което се е появила неизправността.

290) Картата на водач трябва да позволява съхраняването на данните за дванайсетте последни неизправности от всеки тип (т.е. 24 неизправности).

4.5.3.2.9 Данни за дейностите на водача

291) Картата на водач трябва да позволява съхраняването на следните данни за всеки календарен ден, в който тя се използва, или в който водачът е въвел ръчно дейностите си:

— датата;

— брояч на присъствените дни (който се увеличава с една единица за всеки от тези календарни дни),

— общо разстояние, изминато от водача през този ден,

— статус на водача в 00:00 часа,

— всякакви промени в дейността на водача и/или промени в обстановката при управление на МПС, и/или вкарване или изваждане на картата на водач:

— състояние при управление на МПС (ЕКИП, САМ),

— процеп (ВОДАЧ, ВТОРИ ВОДАЧ),

— положение на картата (ВКАРАНА, НЕВКАРАНА),

— дейност (управление на МПС, НА РАЗПОЛОЖЕНИЕ, РАБОТА, ПРЕКЪСВАНЕ/ПОЧИВКА).

— час на промяната,

292) Паметта на картата на водач трябва да позволява съхраняването на данните за дейността на водача в продължение на най-малко 28 дни (средната дейност на водач се определя като 93 промени на дейността на ден).

293) Данните, изброени в изисквания 286, 289 и 291 трябва да бъдат съхранени по начин, позволяващ дейностите да бъдат открити по реда на тяхното настъпване, дори в случай на припокриване във времето.

4.5.3.2.10 Данни за използваното превозно средство

294) Картата на водач трябва да позволява съхраняването за всеки календарен ден, в който тя се използва, и за всеки период на използване на определено превозно средство през този ден (периодът на използване включва всички последователни цикли на вкарване/изваждане на картата в превозното средство, като се има предвид самата карта), следните данни:

— дата и час на първото използване на превозното средство (т.е. първото вкарване на картата за този период на употреба на превозното средство, или 00:00 часа, ако периодът на използване е протичал по това време),

— стойност на километражния брояч на превозното средство в този момент на първо използване,

— дата и час на последното използване на превозното средство (тоест последното изваждане на картата за този период на употреба на превозното средство, или 23:59 часа, ако периодът на използване е протичал по това време),

— стойност на километражния брояч на превозното средство в този момент на последно използване,

— VRN и държава членка, извършила регистрацията на превозното средство,

— VIN на превозното средство.

295) Картата на водач трябва да позволява съхраняването минимум 84 такива записа.

4.5.3.2.11 Места и местоположения, където дневните периоди на работа започват и/или завършват

296) Картата на водач трябва да позволява съхраняването на следните данни относно местоположенията, където дневните периоди на работа започват и/или завършват, въведени от водача:

— дата и час на въвеждането (или дата и час, свързани с въвеждането, когато то се извършва по време на процедурата по ръчно въвеждане),

— типа на въвежданата информация (начало или край, условия на въвеждане на информацията),

— въведените страна и област,

— стойността от километражния брояч на превозното средство,

— местоположението на превозното средство,

— точността на ГНСС, датата и времето, когато е била определено местоположението.

297) Картата на водача трябва да позволява съхраняването най-малко 84 двойки такива записи.

4.5.3.2.12 Данни за картовата сесия

298) Картата на водач трябва да позволява съхраняването на следните данни относно превозното средство, в което е отворена текущата сесия:

— дата и час на отваряне на сесията (тоест на вкарване на картата), с точност до една секунда,

— VRN и държава членка, извършила регистрацията на превозното средство.

4.5.3.2.13 Данни за контролните дейности

299) Картата на водач трябва да позволява съхраняването на следните данни относно контролните дейности:

— дата и час на извършения контрол,

— номер на контролната карта, държава членка, която я е издала,

— вид на проверката (изобразяване на данните и/или отпечатване и/или изтегляне на данни от БУ и/или изтегляне на данни от картата (виж забележката)),

— изтеглен период, в случай на изтегляне,

— VRN и държава членка, извършила регистрацията на превозното средство, в което е извършена проверката.

Забележка: Изискванията за сигурност предполагат, че изтеглянето от картата се регистрира само ако се извърши чрез уреди за регистриране на данните за движението.

300) Картата на водач трябва да позволява съхраняването на един такъв запис.

4.5.3.2.14 Данни за специфични условия

301) Картата на водач трябва да позволява съхраняването на следните данни, свързани със специфични условия, въведени докато картата е била вкарана (независимо в кой процеп):

— дата и час на въвеждането,

— тип на специфичното условие.

302) Картата на водач трябва да позволява съхраняването минимум 56 такива записа.

4.5.3.2.15 Данни за използваните бордови устройства

303) Картата на водач трябва да позволява съхраняването на следните данни, свързани с различните бордови устройства, в които е била използвана:

— датата и часа на началото на периода на използване на превозното средство (т.е. първото вкарване на картата в бордовото устройство през периода),

— наименование на производителя на бордовото устройство,

— тип на бордовото устройство,

— номер на версията на софтуера на бордовото устройство.

304) Картата на водач трябва да позволява съхраняването минимум 84 такива записа.

4.5.3.2.16 Данни за местата за три часа управление на МПС

305) Картата на водач трябва да позволява съхраняването на следните данни, свързани с местоположението на превозното средство, когато времето на непрекъснато управление на МПС на водача достигне кратно на три часа:

— дата и час, когато времето на непрекъснато управление на МПС на титуляря на картата достигне кратно на три часа,

— местоположението на превозното средство.

— точността на ГНСС, датата и времето, когато е била определено местоположението.

306) Картата на водач трябва да позволява съхраняването минимум 252 такива записа.

4.5.4 *Карта за монтаж и настройки*

4.5.4.1 Тахографско приложение (достъпно за бордови устройства от първо и второ поколение)

4.5.4.1.1 Идентификация на приложенията

307) Картата за монтаж и настройки трябва да позволява съхраняването на следните данни за идентификация на приложението:

— Идентификация на тахографското приложение,

— Идентификация на типа тахографска карта.

4.5.4.1.2 Ключове и сертификати

308) Картата за монтаж и настройки трябва да позволява съхраняването определен брой криптографски ключове и сертификати, както е посочено в допълнение 11, част А.

309) Картата за монтаж и настройки трябва да позволява съхраняването на персонален идентификационен номер (PIN).

4.5.4.1.3 Идентификация на картата

310) Картата за монтаж и настройки трябва да позволява съхраняването на следните данни относно идентификацията на картата:

— номер на картата,

— държава членка, издала картата, наименование на органа, който я е издал, дата на издаване,

— дата на начало на валидността на картата, дата на край на валидността.

4.5.4.1.4 Идентификация на титуляря на картата

311) Картата за монтаж и настройки трябва да позволява съхраняването на следните данни относно идентификацията на титуляря на картата:

— наименование на сервиза,

— адрес на сервиза,

— фамилно име на титуляря,

— собствено(и) име(на) на титуляря,

— предпочитан език.

4.5.4.1.5 Изтегляне на данни от карта

312) Картата за монтаж и настройки трябва да позволява съхраняването на запис за изтеглянето на данни от картата по същия начин като картата на водач.

4.5.4.1.6 Данни за калибрирането и сверяването на часовника

313) Картата за монтаж и настройки трябва да позволява съхраняването на записи за калибрирания и/или сверявания на часовника, извършени когато картата е била вкарана в уред за регистриране на данните за движението.

314) Всеки запис за калибриране трябва да позволява съхраняване на следните данни:

— Цел на калибрирането (пускане, първо монтиране, монтиране, периодични технически прегледи),

— Идентификация на превозното средство

— Актуализирани или потвърдени параметри (w, k, l, размер на гумите, регулировка на ограничителя на скоростта, километражен брояч (стара и нова стойност), дата и час (стара и нова стойност)).

— Идентификация на уредите за регистриране на данните за движението (фабричен и сериен номер на бордовото устройство, сериен номер на датчика за движение).

315) Картата за монтаж и настройки трябва да позволява съхраняването на най-малко 88 такива записа.

316) Картата за монтаж и настройки трябва да има брояч, указващ общия брой на калибрираният, извършени с картата.

317) Картата за монтаж и настройки трябва да съдържа брояч, указващ общия брой на калибрираният, извършени от последното изтегляне на данни.

4.5.4.1.7 Данни за събития и за неизправности

318) Картата за монтаж и настройки трябва да позволява съхраняването на данни за събитията и неизправностите по същия начин като картата на водач.

319) Картата за монтаж и настройки трябва да позволява съхраняването на трите последни събития от всеки тип (т.е. 18 събития) и на шестте последни неизправности от всеки тип (т.е. 12 неизправности).

4.5.4.1.8 Данни за дейностите на водача

320) Картата за монтаж и настройки трябва да позволява съхраняването на данни за дейността на водача по същия начин като картата на водач.

321) Картата за монтаж и настройки трябва да позволява съхраняването на данни за дейността на водача за най-малко 1 ден средна дейност на водача.

4.5.4.1.9 Данни за използваното превозно средство

322) Картата за монтаж и настройки трябва да позволява съхраняването на записи от данни за използваните превозни средства по същия начин като картата на водач.

323) Картата за монтаж и настройки трябва да позволява съхраняването на най-малко 4 такива записа.

4.5.4.1.10 Данни относно края и/или началото на дневните периоди на работа

324) Картата за монтаж и настройки трябва да позволява съхраняването на данни за началото и/или края на дневните периоди на работа по същия начин като картата на водача.

325) Картата на водача трябва да позволява съхраняването на най-малко 3 двойки такива записи.

4.5.4.1.11 Данни за картовата сесия

326) Картата за монтаж и настройки трябва да позволява съхраняването на запис от данни за картова сесия по същия начин като картата на водач.

4.5.4.1.12 Данни за контролните дейности

327) Картата за монтаж и настройки трябва да позволява съхраняването на запис от данни за контролните дейности по същия начин като картата на водач.

4.5.4.1.13 Данни за специфични условия

328) Картата за монтаж и настройки трябва да позволява съхраняването на данни за специфични условия по същия начин като картата на водач.

329) Картата за монтаж и настройки трябва да позволява съхраняването на най-малко 2 такива записа.

4.5.4.2 Тахографско приложение от поколение 2 (не е достъпно за бордово устройство от първо поколение)

4.5.4.2.1 Идентификация на приложенията

330) Картата за монтаж и настройки трябва да позволява съхраняването на следните данни за идентификация на приложението:

— идентификация на тахографското приложение,

— идентификация на типа тахографска карта.

4.5.4.2.2 Ключове и сертификати

331) Картата за монтаж и настройки трябва да позволява съхраняването определен брой криптографски ключове и сертификати, както е посочено в допълнение 11, част Б.

332) Картата за монтаж и настройки трябва да позволява съхраняването на персонален идентификационен номер (PIN).

4.5.4.2.3 Идентификация на картата

333) Картата за монтаж и настройки трябва да позволява съхраняването на следните данни за идентификацията на картата:

— номер на картата,

— държава членка, издала картата, наименование на органа, който я е издал, дата на издаване,

— дата на начало на валидността на картата, дата на край на валидността.

4.5.4.2.4 Идентификация на титуляря на картата

334) Картата за монтаж и настройки трябва да позволява съхраняването на следните данни относно идентификацията на титуляря на картата:

— наименование на сервиза,

— адрес на сервиза,

— фамилно име на титуляря,

— собствено(и) име(на) на титуляря,

— предпочитан език.

4.5.4.2.5 Изтегляне на данни от карта

335) Картата за монтаж и настройки трябва да позволява съхраняването на запис за изтеглянето на данни от картата по същия начин като картата на водач.

4.5.4.2.6 Данни за калибрирането и сверяването на часовника

336) Картата за монтаж и настройки трябва да позволява съхраняването на записи за калибрирания и/или сверявания на часовника, извършени когато картата е била вкарана в уред за регистриране на данните за движението.

337) Всеки запис за калибриране трябва да позволява съхраняване на следните данни:

— цел на калибрирането (пускане, първо монтиране, монтиране, периодични технически прегледи),

— идентификация на превозното средство,

— актуализирани или потвърдени параметри (w, k, l, размер на гумите, регулировка на ограничителя на скоростта, километражен брояч (стара и нова стойност), дата и час (стара и нова стойност)).

— Идентификация на уредите за регистриране на данните за движението (фабричен и сериен номер на БУ, сериен номер на датчика за движение, сериен номер на устройството за връзка от разстояние, сериен номер на външното устройство за GNSS (ако е приложимо),

— типове и идентификатори на всички поставени пломби,

— способност на бордовото устройство да използва тахографски карти от първо поколение (може или не).

338) Картата за монтаж и настройки трябва да позволява съхраняването на най-малко 88 такива записа.

339) Картата за монтаж и настройки трябва да има брояч, указващ общия брой на калибрированията, извършени с картата.

340) Картата за монтаж и настройки трябва да съдържа брояч, указващ общия брой на калибрированията, извършени от последното изтегляне на данни.

4.5.4.2.7 Данни за събития и за неизправности

341) Картата за монтаж и настройки трябва да позволява съхраняването на данни за събитията и неизправностите по същия начин като картата на водач.

342) Картата за монтаж и настройки трябва да позволява съхраняването на трите последни събития от всеки тип (т.е. 33 събития) и на шестте последни неизправности от всеки тип (т.е. 12 неизправности).

4.5.4.2.8 Данни за дейностите на водача

343) Картата за монтаж и настройки трябва да позволява съхраняването на данни за дейността на водача по същия начин като картата на водач.

344) Картата за монтаж и настройки трябва да позволява съхраняването на данни за дейността на водача за най-малко 1 ден средна дейност на водача.

4.5.4.2.9 Данни за използваното превозно средство

345) Картата за монтаж и настройки трябва да позволява съхраняването на записи от данни за използваните превозни средства по същия начин като картата на водач.

346) Картата за монтаж и настройки трябва да позволява съхраняването на най-малко 4 такива записа.

4.5.4.2.10 Данни за края и/или началото на дневните периоди на работа

347) Картата за монтаж и настройки трябва да позволява съхраняването на данни за началото и/или края на дневните периоди на работа по същия начин като картата на водача.

348) Картата на водача трябва да позволява съхраняването на най-малко 3 двойки такива записи.

4.5.4.2.11 Данни за картовата сесия

349) Картата за монтаж и настройки трябва да позволява съхраняването на запис от данни за картова сесия по същия начин като картата на водач.

4.5.4.2.12 Данни за контролните дейности

350) Картата за монтаж и настройки трябва да позволява съхраняването на запис от данни за контролните дейности по същия начин като картата на водач.

4.5.4.2.13 Данни за използваните бордови устройства

351) Картата за монтаж и настройки трябва да позволява съхраняването на следните данни, свързани с различните бордови устройства, в които е била използвана:

— датата и часа на началото на периода на използване на превозното средство (т.е. първото вкарване на картата в бордовото устройство през периода),

— наименование на производителя на бордовото устройство,

— тип на бордовото устройство,

— номер на версията на софтуера на бордовото устройство.

352) Картата за монтаж и настройки трябва да позволява съхраняването на най-малко 4 такива записа.

4.5.4.2.14 Данни за местата за три часа управление на МПС

353) Картата за монтаж и настройки трябва да позволява съхраняването на следните данни, свързани с местоположението на превозното средство, когато времето на непрекъснато управление на МПС на водача достигне кратно на три часа:

— дата и час, когато времето на непрекъснато управление на МПС на титуляря на картата достигне кратно на три часа,

— местоположението на превозното средство,

— точността на ГНСС, датата и времето, когато е била определено местоположението.

354) Картата за монтаж и настройки трябва да позволява съхраняването на най-малко 18 такива записа.

4.5.4.2.15 Данни за специфични условия

355) Картата за монтаж и настройки трябва да позволява съхраняването на данни за специфични условия по същия начин като картата на водач.

356) Картата за монтаж и настройки трябва да позволява съхраняването на най-малко 2 такива записа.

4.5.5 *Контролна карта*

4.5.5.1 Тахографско приложение (достъпно за бордови устройства от първо и второ поколение)

4.5.5.1.1 Идентификация на приложенията

357) Контролната карта трябва да позволява съхраняването на следните данни за идентификация на приложението:

— идентификация на тахографското приложение,

— идентификация на типа тахографска карта.

4.5.5.1.2 Ключове и сертификати

358) Контролната карта трябва да позволява съхраняването определен брой криптографски ключове и сертификати, както е посочено в допълнение 11, част А.

4.5.5.1.3 Идентификация на картата

359) Контролната карта трябва да позволява съхраняването на следните данни относно идентификацията на картата:

— номер на картата,

— държава членка, издала картата, наименование на органа, който я е издал, дата на издаване,

— дата на начало на валидността на картата, дата на край на валидността (при необходимост).

4.5.5.1.4 Идентификация на титуляря на картата

360) Контролната карта трябва да позволява съхраняването на следните данни за титуляря на картата:

— наименование на контролния орган,

— адрес на контролния орган,

— фамилно име на титуляря,

— собствено(и) име(на) на титуляря,

— предпочитан език.

4.5.5.1.5 Данни за контролните дейности

361) Контролната карта трябва да позволява съхраняването на следните данни за контролните дейности:

— дата и час на извършената проверка,

— вид на проверката (изобразяване на данните и/или отпечатване върху хартия и/или изтегляне на данни от бордовото устройство и/или изтегляне на данни от картата и/или пътна проверка на калибрирането).

— изтеглен период (ако има такъв),

— VRN и орган на държавата членка, регистрирал проверяваното превозно средство,

— номер на проверяваната карта на водач и държава членка, която я е издала.

362) Контролната карта трябва да позволява съхраняването на най-малко 230 такива записи.

4.5.5.2 Тахографско приложение от поколение 2 (не е достъпно за бордово устройство от първо поколение)

4.5.5.2.1 Идентификация на приложенията

363) Контролната карта трябва да позволява съхраняването на следните данни за идентификация на приложението:

— идентификация на тахографското приложение,

— идентификация на типа тахографска карта.

4.5.5.2.2 Ключове и сертификати

364) Контролната карта трябва да позволява съхраняването определен брой криптографски ключове и сертификати, както е посочено в допълнение 11, част Б.

4.5.5.2.3 Идентификация на картата

365) Контролната карта трябва да позволява съхраняването на следните данни относно идентифицирането на картата:

— номер на картата,

— държава членка, издала картата, наименование на органа, който я е издал, дата на издаване,

— дата на начало на валидността на картата, дата на край на валидността (ако има).

4.5.5.2.4 Идентифициране на титуляря на картата

366) Контролната карта трябва да позволява съхраняването на следните данни за титуляря на картата:

— наименование на контролния орган,

— адрес на контролния орган,

— фамилно име на титуляря,

— собствено(и) име(на) на титуляря,

— предпочитан език.

4.5.5.2.5 Данни за контролните дейности

367) Контролната карта трябва да позволява съхраняването на следните данни за контролните дейности:

— дата и час на извършената проверка,

— вид на проверката (изобразяване на данните и/или отпечатване върху хартия и/или изтегляне на данни от бордовото устройство и/или изтегляне на данни от картата и/или пътна проверка на калибрирането)

— изтеглен период (ако има такъв),

— VRN и орган на държавата членка, регистрирал проверяваното превозно средство,

— номер на проверяваната карта на водач и държава членка, която я е издала.

368) Контролната карта трябва да позволява съхраняването на най-малко 230 такива записи.

4.5.6 *Карта на превозвач*

4.5.6.1 Тахографско приложение (достъпно за бордови устройства от първо и второ поколение)

4.5.6.1.1 Идентифициране на приложенията

369) Картата на превозвач трябва да позволява съхраняването на следните данни за идентификация на приложението:

— идентификация на тахографското приложение,

— идентификация на типа тахографска карта.

4.5.6.1.2 Ключове и сертификати

370) Картата на превозвач трябва да позволява съхраняването определен брой криптографски ключове и сертификати, както е посочено в допълнение 11, част А.

4.5.6.1.3 Идентифициране на картата

371) Картата на превозвач трябва да позволява съхраняването на следните данни за идентифицирането на картата:

— номер на картата,

— държава членка, издала картата, наименование на органа, който я е издал, дата на издаване,

— дата на начало на валидността на картата, дата на край на валидността (ако има).

4.5.6.1.4 Идентифициране на титуляря на картата

372) Картата на превозвач трябва да позволява съхраняването на следните данни за идентифицирането на титуляря на картата:

— наименование на превозвача,

— адрес на превозвача.

4.5.6.1.5 Данни относно дейността на предприятието

373) Картата на превозвач трябва да позволява съхраняването на следните данни за дейностите на превозвача:

— дата и час на дейността,

— тип на дейността (блокиране и/или разблокиране на бордовото устройство, изтегляне на данни от бордовото устройство и/или от картата)

— изтеглен период (ако има такъв),

— VRN и орган на държавата членка, извършил регистрацията на превозното средство,

— номер на картата и държава членка, която я е издала (при изтегляне на данни от картата).

374) Картата на превозвач трябва да позволява съхраняването на най-малко 230 такива записа.

4.5.6.2 Тахографско приложение от поколение 2 (не е достъпно за бордово устройство от първо поколение)

4.5.6.2.1 Идентифициране на приложенията

375) Картата на превозвач трябва да позволява съхраняването на следните данни за идентификация на приложението:

— идентификация на тахографското приложение,

— идентификация на типа на тахографската карта.

4.5.6.2.2 Ключове и сертификати

376) Картата на превозвач трябва да позволява съхраняването определен брой криптографски ключове и сертификати, както е посочено в допълнение 11, част Б.

4.5.6.2.3 Идентифициране на картата

377) Картата на превозвач трябва да позволява съхраняването на следните данни за идентифицирането на картата:

— номер на картата,

— държава членка, издала картата, наименование на органа, който я е издал, дата на издаване,

— дата на начало на валидността на картата, дата на край на валидността (ако има).

4.5.6.2.4 Идентифициране на титуляря на картата

378) Картата на превозвач трябва да позволява съхраняването на следните данни за идентифицирането на титуляря на картата:

— наименование на превозвача,

— адрес на превозвача.

4.5.6.2.5 Данни за дейността на предприятието

379) Картата на превозвач трябва да позволява съхраняването на следните данни за дейностите на превозвача:

— дата и час на дейността,

— тип на дейността (блокиране и/или разблокиране на бордовото устройство, изтегляне на данни от бордовото устройство и/или от картата)

— изтеглен период (ако има такъв),

— VRN и орган на държавата членка, извършил регистрацията на превозното средство,

— номер на картата и държава членка, която я е издала (при изтегляне на данни от картата).

380) Картата на превозвач трябва да позволява съхраняването на най-малко 230 такива записа.

5 МОНТИРАНЕ НА УРЕДИ ЗА РЕГИСТРИРАНЕ НА ДАННИТЕ ЗА ДВИЖЕНИЕТО

5.1 **Монтиране**

381) Новите уреди за регистриране на данните за движението се доставят неактивирани на монтьорите или на производителите на превозното средство, заедно с всички параметри на калибрирането, фигуриращи в списъка на глава 3.21, настроени на подходящи и валидни стойности по подразбиране. Когато не е подходяща никаква определена стойност, за буквените параметри се задават низове от „?“, а за числените параметри се задава „0“). Доставянето на важни за сигурността части на уредите за регистриране на данните за движението може да бъде ограничено ако това е необходимо по време на сертифицирането за сигурност.

382) Преди своето активиране уредите за регистриране на данните за движението трябва да дадат достъп до функцията за калибриране, дори и да не са в режим на калибриране.

383) Преди своето активиране уредите за регистриране на данните за движението не трябва нито да регистрират, нито да записват данни, посочени в точки 3.12.3, 3.12.9 и 3.12.12 до 3.12.15 включително.

384) По време на монтирането производителите на превозното средство трябва да настроят предварително всички известни параметри.

385) Производителите на превозното средство или монтьорите трябва да активират монтираните уреди за регистриране на данните за движението най-късно преди да започне използването на превозното средство в обхвата на Регламент (ЕО) № 561/2006.

386) Активирането на уредите за регистриране на данните за движението трябва да се задейства автоматично при първото вкарване на карта за монтаж и настройки в кое да е от интерфейсните устройства за карта.

387) Специфичните действия по свързването на датчика за движение с бордовото устройство, ако има такива, трябва да се извършват автоматично преди или по време на активирането.

388) По подобен начин специфични действия по свързването на външното устройство за GNSS с бордовото устройство, ако има такива, трябва да се извършват автоматично преди или по време на активирането.

389) След активирането си уредите за регистриране на данните за движението трябва да приложат в пълна степен контрол върху достъпа до функциите и данните.

390) След активирането си уредите за регистриране на данните за движението трябва да съобщят на устройството за връзка от разстояние защитените данни, необходими за целите на целенасочените пътни проверки.

391) Регистриращите и записващите функции на уредите за регистриране на данните за движението трябва да бъдат напълно действащи след активирането.

392) Монтирането трябва да бъде последвано от калибриране. Не е задължително първоначалното калибриране да включва въвеждане на регистрационния номер на превозното средство, когато той не е известен на одобрения сервиз, който трябва да извърши това калибриране. При такива обстоятелства и само по това време собственикът на превозното средство трябва да може да въведе регистрационния номер на превозното средство (VRN), като използва своята карта на превозвач, преди да започне използването на превозното средство в обхвата на Регламент (ЕО) № 561/2006 (напр. чрез използване на команди посредством подходяща структура от менюта в интерфейса „човек — машина“ на бордовото устройство) ([1]). Актуализирането или потвърждаването на това въвеждане трябва да е възможно само с използване на карта за монтаж и настройки.

393) За монтирането на външно устройство за GNSS е необходимо свързване с бордовото устройство и последваща проверка на информацията за местоположението от GNSS.

394) Уредите за регистриране на данните за движението трябва да бъдат разположени така в превозното средство, че водачът да има достъп до необходимите функции от седалката си.

([1]) ОВ L 102, 11.4.2006 г., стр. 1.

5.2 **Монтажна табелка**

395) След като монтираните уреди за регистриране на данните за движението бъдат проверени, е необходимо върху уредите да се прикрепи монтажна табелка (гравирана или отпечатана неизтриваемо), която да е добре видима и лесно достъпна. В случаи, когато това не е възможно, табелката трябва да се прикрепи към средната колона на автомобилната каросерия, така че да е добре видима. За превозни средства, които нямат средна колона на каросерията, монтажната табелка следва да бъде прикрепена към рамката на вратата от страната на водача на превозното средство и във всички случаи да бъде добре видима.

След всяко инспектиране от страна на лицензиран монтьор или сервиз, на мястото на старата табелка се поставя нова такава.

396) Табелката трябва да съдържа най-малко следните данни:

— име и адрес или търговско наименование на одобрения монтьор или сервиз,

— характеристичен коефициент на превозното средство, във вида „w = … импулса/km“,

— константа на уредите за регистриране на данните за движението, във вида „k = … импулса/km“,

— действителна обиколка на колелата с гумите, във вида „l = … mm“,

— размер на гумите,

— датата, на която са измерени характеристичният коефициент на превозното средство и действителната обиколка на колелата с гумите,

— идентификационния номер на превозното средство,

— Наличието (или не) на външно устройство за GNSS,

— серийния номер на външното устройство за GNSS,

— серийния номер на устройството за връзка от разстояние,

— серийния номер на всички поставени пломби,

— частта на превозното средство, на която е монтиран адаптерът, ако има такъв,

— частта на превозното средство, на която е монтиран датчикът за движение, ако не е свързан с предавателната кутия или не се използва адаптер,

— описание на цвета на кабела между адаптера и тази част на превозното средство, която изработва входящите за адаптера импулси,

— серийния номер на вградения в адаптера датчик за движение.

397) Само за превозни средства от категории M1 и N1, които са оборудвани с адаптер в съответствие с Регламент (ЕО) № 68/2009 на Комисията ([1]) с последните му изменения, и когато не е възможно да се включи цялата необходима информация, както е описано в изискване 396, може да се използва втора, допълнителна табелка. В такива случаи тази допълнителна табелка трябва да съдържа поне информацията съгласно последните четири тирета от изискване 396.

Ако се използва втора, допълнителна табелка, тя трябва да бъде поставена близо до първата основна табелка, описана в изискване 396, и трябва да е със същото ниво на защита. Освен това допълнителната табелка трябва да съдържа името, адреса или търговската марка на лицензирания монтьор или сервиз, извършил монтирането, и датата на монтиране.

([1]) Регламент (ЕО) № 68/2009 на Комисията от 23 януари 2009 година за адаптиране за девети път към техническия прогрес на Регламент (ЕИО) № 3821/85 на Съвета относно контролните уреди за регистриране на данните за движението при автомобилен транспорт (ОВ L 21, 24.1.2009 г., стр. 3).

5.3 **Пломбиране**

398) Трябва да бъдат пломбирани следните части:

— Всяка връзка, която ако бъде прекъсната, би предизвикала неоткриваеми промени или неоткриваема загуба на данни (това може да важи например за монтирането на датчика за движение към предавателната кутия, адаптера за превозни средства от категории M1/N1, връзката с външното устройство за ГНСС или бордовото устройство);

— Монтажната табелка, освен ако е прикрепена по такъв начин, че не може да бъде отделена без да се разрушат маркировките върху нея.

399) Предвидените пломби може да бъдат премахнати:

— В случаите на извънредни обстоятелства,

— С цел монтиране, регулиране или поправяне на ограничител на скоростта или на всяко друго устройство, което има отношение към пътната безопасност, при положение че уредите за регистриране на данните за движението продължават да функционират правилно и сигурно и при положение, че той се пломбира отново от лицензиран монтьор или сервиз (съгласно глава 6) веднага след монтирането на ограничителя на скоростта или на всяко друго устройство, което има отношение към пътната безопасност, или в течение на следващите 7 дена в другите случаи.

400) При всяко счупване на тези пломби се съставя писмена декларация, указваща причините за това действие, и тя се предоставя на компетентния орган.

401) Пломбите трябва да бъдат с идентификационен номер, зададен от производителя. Този номер трябва да е уникален и да е различен от всеки друг номер на пломба, зададен от друг производител на пломби.

Този уникален идентификационен номер се определя като: MMNNNNNN чрез неизтриваема маркировка, като MM е уникална идентификация на производителя (регистрирането в базата данни се управлява от ЕК), а NNNNNN е буквено-цифров номер на пломбата, който е уникален в областта на производителя.

402) Пломбите трябва да имат свободно място, където одобрените монтьори, сервизи или производители на превозни средства да могат да добавят специална маркировка в съответствие с член 22, параграф 3 от Регламент (ЕС) № 165/2014.

Тази маркировка не трябва да закрива идентификационния номер на пломбата.

403) Производителите на пломби трябва да бъдат регистрирани в специална база данни и да направят своите идентификационни номера на пломби публични чрез процедура, която ще се определи от Европейската комисия.

404) Одобрени сервизи и производители на превозни средства, в рамките на Регламент (ЕС) № 165/2014, използват само пломби от тези на производители, включени в гореспоменатата база данни.

405) Производителите на пломби и техните разпространители трябва да водят пълна ведомост за проследяемост на пломбите, продавани, за да бъдат използвани в рамките на Регламент (ЕС) № 165/2014, и трябва да са подготвени да ги представят винаги когато е необходимо на компетентните национални органи.

406) Уникалните идентификационни номера на пломби трябва да се виждат върху монтажната табелка.

6 ПРОВЕРКИ, ИНСПЕКТИРАНЕ И ПОПРАВКИ

Изискванията относно обстоятелствата, при които пломбите могат да бъдат премахнати, както е указано в член 22, параграф 5 на Регламент (ЕС) № 165/2014, са определени в глава 5.3 от настоящото приложение.

6.1 **Одобряване на монтьори, сервизи и производители на превозни средства**

Държавите членки одобряват, контролират редовно и сертифицират органите, натоварени със следните задачи:

— монтирания,

— проверки,

— инспекции,

— поправки.

Картите за монтаж и настройки се издават само на монтьорите и/или сервизите, които са одобрени да извършват активирането и/или калибрирането на уредите за регистриране на данните за движението в съответствие с настоящото приложение и които, освен при надлежно мотивиран случай:

— не отговарят на условията за получаване на карта на превозвач;

— при които останалите професионални дейности не са от вид, който да попречи на общата сигурност на системата както се изисква в допълнение 10.

6.2 **Проверка на новите или поправените измервателни уреди**

407) Всяко отделно устройство, било то ново или поправено, трябва да бъде проверено дали функционира правилно и дали е с точни показания и записи, в границите, определени в глава 3.2.1, 3.2.2, 3.2.3 и 3.3, чрез пломбиране в съответствие с глава 5.3 и калибриране.

6.3 **Проверка на монтирането**

408) При монтирането в превозното средство, всички монтирани компоненти (включително уредите за регистриране на данните за движението) трябва да отговарят на разпоредбите относно максималните толеранси, определени в глави 3.2.2, 3.2.3 и 3.3.

6.4 **Периодични технически прегледи**

409) Извършват се периодични технически прегледи на уредите, монтирани на превозните средства, след всяка поправка или след всяка промяна на характеристичния коефициент на превозното средство или на действителната обиколка на търкаляне на гумите, или когато часовникът, показващ координираното универсално време, е неточен с повече от 20 минути, или когато е променен регистрационният номер, или най-малко един път на всеки две години (24 месеца).

410) Тези прегледи трябва да включват следните проверки:

— за правилно функциониране на уредите за регистриране на данните за движението, включително функцията за записване на данни в тахографските карти и комуникацията с четците за връзка с цел ранно откриване от разстояние.

— че е осигурено съответствие с разпоредбите на глава 3.2.1 и III.2.2 относно максималните толеранси при монтиране,

— че е осигурено съответствие с разпоредбите на глава 3.2.3 и 3.3,

— че уредите за регистриране на данните за движението имат знак за одобрение на типа,

— че монтажната табелка, както е определено с изискване 396, и указателната табелка, както е определено с изискване 225, са поставени,

— на размера на гумите и действителната обиколка на гумите,

— за отсъствие на устройства за манипулиране, прикрепени към уредите,

— че пломбите са правилно поставени, в добро състояние, техните идентификационни номера са валидни (производител на пломбите с позоваване на базата данни на ЕК) и че техните идентификационни номера съответстват на маркировките върху монтажната табела (вж. изискване 401).

411) Ако за едно от събитията, изброени в глава 3.9 („Откриване на събития и/или неизправности“), е установено, че се е случило след последното инспектиране, и то се счита от производителите на тахографи и/или от националните органи за потенциално излагащо на риск сигурността на уредите, сервизът трябва:

a. да извърши съпоставка на данните за идентификация на датчика за движение от свързания към предавателната кутия датчик за движение, с тези от сдвоения датчик за движение, регистриран в бордовото устройство.

б. да провери дали информацията, записана върху монтажната табелка, съответства на информацията, съдържаща се в записа от бордовото устройство;

в. да провери дали серийният номер на датчика за движение и номерът на одобрението му, ако са отпечатани върху корпуса на датчика за движение, съответстват на информацията, записана в паметта за данни на бордовото устройство;

г. да сравни идентификационните данни, отбелязани върху указателната табелка на външното устройство за GNSS, ако има такова, с тези, записани в паметта за данни на бордовото устройство;

412) Сервизите трябва да записват в своите протоколи от проверки всички констатации относно счупени пломби или за устройства за манипулиране. Тези протоколи трябва да се съхраняват от сервизите поне две години и да се предоставят на компетентния орган при всяко поискване.

413) Тези проверки трябва да включват калибриране и превантивна замяна на пломбите, за чието монтиране са отговорни сервизите..

6.5 **Измерване на грешките**

414) Измерването на грешките при монтирането и по време на използването трябва да се осъществява при следните условия, които се разглеждат като стандартни условия на изпитване:

— превозно средство без товар, в готовност за движение,

— налягане в гумите в съответствие с указанията на производителя,

— износване на гумите в границите, разрешени от националното законодателство,

— движение на превозното средство:

— превозното средство трябва да се движи напред под действие на собствения си двигател, по права линия и върху равна повърхност със скорост 50 ± 5 km/h. Измереното разстояние трябва да бъде най-малко 1 000 m.

— при положение са със сходна точност, за това изпитание могат също така да бъдат използвани други методи, като например подходящ изпитвателен стенд.

6.6 **Поправки**

415) Сервизите трябва да могат да изтеглят данни от уредите за регистриране на данните за движението, за да ги върнат на съответното транспортно предприятие (превозвач).

416) Одобрените сервизи трябва да издават на транспортните предприятия сертификат, удостоверяващ че данните не могат да бъдат изтеглени, когато повреда в уредите за регистриране на данните за движението не позволява записаните данни да бъдат изтеглени, дори след поправка в самия сервиз. Сервизите запазват копие от всеки издаден сертификат в продължение на най-малко две години.

7 ИЗДАВАНЕ НА КАРТИ

Процедурите, прилагани от държавите членки при издаване на картите, трябва да отговарят на следните изисквания:

417) Номерът на картата при първото издаване на тахографска карта трябва да съдържа пореден номер (ако е приложимо), индекс за замяна и индекс за подновяване на валидността, зададен като „0“.

418) Номерата на картата на всички тахографски карти, които не са поименни и са издадени от един контролен орган или от един сервиз или едно транспортно предприятие, трябва да са със същите първи 13 цифри да са с различен пореден номер.

419) Тахографска карта, издадена за замяна на друга съществуваща тахографска карта, трябва да е със същия номер на картата, като този на заменената карта, с изключение на индекса за замяна, който трябва да се увеличи с 1 (в реда 0, …, 9, A, …, Z).

420) Тахографска карта, издадена за замяна на друга съществуваща тахографска карта, трябва да е със същата дата на край на валидността като картата, която заменя.

421) Тахографска карта, издадена за подновяване на съществуваща тахографска карта, трябва да е със същия номер на картата като номера на картата, чиято валидност подновява, с изключение на индекса за подновяване, който трябва да се увеличи с 1 (в реда 0, …, 9, A, …, Z).

422) Замяната на съществуваща тахографска карта, с цел промяна на административните данни, трябва да следва правилата, прилагани при подновяване, ако тя се извършва в рамките на една и съща държава членка, или правилата, прилагани при първото издаване, ако се извършва в друга държава членка.

423) „Фамилното име на титуляря на картата“ в случая на контролна карта или карта за монтаж и настройки, която не е поименна, трябва да бъде попълнено с наименованието на сервиза или на контролния орган или с името на монтьора или на контролиращия служител, ако така бъде решено от държавите членки.

424) Държавите членки трябва да обменят данни по електронен път, за да гарантират уникалността на картите на водач, които издават, в съответствие с член 31 от Регламент (ЕС) № 165/2014.

8 ОДОБРЕНИЕ НА ТИПА НА УРЕДИТЕ ЗА РЕГИСТРИРАНЕ НА ДАННИТЕ ЗА ДВИЖЕНИЕТО И НА ТАХОГРАФСКИТЕ КАРТИ

8.1 **Общи положения**

За целите на настоящата глава под „Уреди за регистриране на данните за движението“ се имат предвид уредите за регистриране на данните за движението или техните компоненти. Не се изисква одобрение на типа на кабела(ите), свързващ(и) датчика за движение с бордовото устройство, външното устройство за GNSS с бордовото устройство или устройството за връзка от разстояние с бордовото устройство. Хартията, използвана в уредите за регистриране на данните за движението, се приема като компонент на уредите за регистриране на данните за движението.

Всеки производител може да поиска одобрение на типа на своя компонент с всякакъв тип датчик за движение, външно устройство за GNSS и обратно, при условие че всеки компонент отговаря на изискванията от настоящото приложение. Като алтернатива, производителите могат да поискат и одобряване на типа на уредите за регистриране на данните за движението.

425) Уредите за регистриране на данните за движението трябва да се представят за одобряване заедно с всички свои компоненти, както и с всички допълнителни устройство, вградени в тях.

426) Одобрението на типа на уреди за регистриране на данните за движението и на тахографски карти трябва да включва изпитвания, свързани със сигурността, изпитвания на функционирането и изпитвания за оперативна съвместимост. Положителните резултати от всяко от тези изпитвания се удостоверяват чрез съответен сертификат.

427) Органите по одобряването на типа на държавите членки не предоставят сертификат за одобряване на типа при положение, че при тях няма:

— сертификат за сигурност,

— сертификат за функциониране,

— както и сертификат за оперативна съвместимост,

за уредите за регистриране на данните за движението или тахографската карта, предмет на искането за одобряване на типа.

428) Всяка промяна на софтуера или хардуера, или на материалите, използвани при производството, трябва да бъде съобщена предварително на органа, който е издал одобрение на типа на уредите. Този орган трябва да потвърди на производителя разширяването на одобрението на типа или може да поиска актуализиране или потвърждаване на сертификатите за функционирането, сигурността и/или оперативната съвместимост.

429) Процедурите по обновяване на място на софтуера на уредите за регистриране на данните за движението трябва да бъдат одобрени от органа, който е издал одобрение на типа на въпросните уреди. Обновяването на софтуера не трябва да променя или да изтрива никаква информация относно дейността на водача, записана в уредите за регистриране на данните за движението. Софтуерът може да бъде обновяван само на отговорност на производителя на уредите за регистриране на данните за движението.

430) Одобряването на типа на софтуерни изменения, насочени към обновяване на одобрен преди тип уреди за регистриране на данните за движението не може да бъде отказвано, ако такива изменения важат само за функции, които не са специфицирани в настоящото приложение. Обновяването на софтуера на уредите за регистриране на данните за движението може да се изключва въвеждането на нови набори от символи, ако това не е технически осъществимо.

8.2 **Сертификат за сигурност**

431) Сертификатът за сигурност се издава съгласно разпоредбите на допълнение 10 към настоящото приложение. Компонентите на уредите за регистриране на данните за движението, които се сертифицират, са бордово устройство, датчик за движение, външно устройство за GNSS и тахографските карти.

432) При извънредното обстоятелство на отказ на органите за сертифициране за сигурност да сертифицират ново оборудване въз основа на излизане от употреба на механизмите за сигурност, издаването на одобрения на типа трябва да продължи само при това специфично и извънредно обстоятелство, когато не съществува алтернативно решение, съответстващо на регламента.

433) При това обстоятелство въпросната държава членка следва незабавно да информира Европейската комисия, която в рамките на двадесет календарни месеца от издаването на одобрението на типа трябва да започне процедура за гарантиране, че равнището на сигурност е възстановено в неговото първоначално състояние.

8.3 **Сертификат за функциониране**

434) Всеки кандидат за одобрение на типа трябва да предостави на органа, извършващ типовото одобрение в съответната държава членка, цялата материална част и документацията, които този орган смята за необходими.

435) Производителите предоставят съответните образци от продукти, за чието одобрение на типа се кандидатства, и свързаната с тях документация, изисквана от лабораториите, определени да извършват изпитвания на функционирането, в срок от един месец от подаването на искането. Разходите, възникнали в резултат на това искане, се поемат от страната, която го е направила. Лабораториите разглеждат като поверителна цялата търговска информация с чувствителен характер.

436) На производителя се издава сертификат за функциониране само ако всички изпитвания за функциониране, специфицирани в допълнение 9, са били преминати успешно.

437) Сертификатът за функциониране се издава от органа по одобряването на типа. Освен името на притежателя си и наименованието на модела, този сертификат трябва да съдържа подробен списък на извършените изпитвания и на получените резултати.

438) В сертификата за функциониране на всеки компонент на уредите за регистриране на данните за движението трябва да се посочват и номерата на одобренията на типа на всички други одобрени съвместими компоненти на уредите за регистриране на данните за движението, изпитани за сертифицирането.

439) В сертификата за функциониране на всеки компонент на уредите за регистриране на данните за движението също така трябва да се посочва стандарт ISO или CEN, по който е сертифициран функционалният интерфейс.

8.4 **Сертификат за оперативна съвместимост**

440) Изпитванията за оперативна съвместимост се извършват само от една лаборатория под контрола и отговорността на Европейската комисия.

441) Лабораторията записва исканията за провеждане на изпитвания за оперативна съвместимост, подадени от производителите, по реда на тяхното постъпване.

442) Исканията се записват официално само ако лабораторията разполага със:

— цялата материална част и необходимите документи за провеждане на изпитванията за оперативна съвместимост,

— съответния сертификат за сигурност,

— съответния сертификат за функциониране,

Датата на вписване на искането се съобщава на производителя.

443) Лабораторията не извършва изпитвания за оперативна съвместимост на уреди за регистриране на данните за движението или на тахографски карти, за които не е издаден сертификат за сигурност и сертификат за функциониране освен при извънредното обстоятелство, описано в изискване 432.

444) Всеки производител, поискал провеждането на изпитвания за оперативна съвместимост, трябва да се ангажира да остави на лабораторията, натоварена с изпитванията, цялата материална част и документацията, необходими за целите на изпитванията.

445) Изпитванията за оперативна съвместимост се провеждат в съответствие с разпоредбите на допълнение 9 към настоящото приложение, съответни с всички типове уреди за регистриране на данните за движението или тахографски карти:

— валидността на одобрението на типа на които не е изтекла или

— чието одобрение на типа се извършва в момента и за които съществува валиден сертификат за оперативна съвместимост.

446) Изпитванията за оперативна съвместимост трябва да обхващат всички поколения уреди за регистриране на данните за движението или тахографски карти, които все още са в употреба.

447) Сертификатът за оперативна съвместимост трябва да бъде издаден на производителя от лабораторията, само след като са преминати успешно всички изпитвания за оперативна съвместимост.

448) Ако изпитванията за оперативна съвместимост не са преминати успешно от един или от няколко уреда за регистриране на данните за движението или от тахографска(и) карта(и), сертификат за оперативна съвместимост не се издава, докато заявилият производител не направи необходимите промени и не премине изпитванията за оперативна съвместимост. Лабораторията трябва да установи причината за проблема с помощта на съответния производител и се опитва да му помогне при търсенето на техническо решение. В случай че производителят е променил продукта си, той трябва да се увери, като се обърне към компетентните органи, че сертификатът за сигурност и на сертификатът за функциониране са все още валидни.

449) Сертификатът за възможността за взаимна работа важи 6 месеца. Той изтича в края на този период, ако производителят не е получил съответния сертификат за типово одобрение. Той се предава от производителя на органа, извършващ типовото одобрение в държавата членка, която е издала сертификата за функциониране.

450) Всеки елемент, който би могъл да предизвика неизправност свързана с оперативната съвместимост, не трябва да се използва за извличане на печалба или за придобиване на доминиращо положение на пазара.

8.5 Сертификат за одобрение на типа

451) Органът, извършващ одобряването на типа в държавата членка, може да издаде сертификат за одобряване на типа, при положение че при него са налице трите изисквани сертификата.

452) В сертификата за одобряване на типа на всеки компонент на уредите за регистриране на данните за движението трябва да се посочват и номерата на одобрението на типа на другите одобрени съвместими компоненти на уреди за регистриране на данните за движението.

453) Копие от сертификата за одобряване на типа трябва да бъде предадено от органа по одобряването на типа на лабораторията, натоварена с изпитванията за оперативна съвместимост, в момента на издаването на този документ на производителя.

454) Лабораторията, отговаряща за изпитванията за оперативна съвместимост, трябва да има публична интернет страница, на която да се актуализира списъкът на моделите на уредите за регистриране на данните за движението или на тахографски карти:

— за които е било регистрирано искане за провеждане на изпитвания за оперативна съвместимост,

— които са получили сертификат за оперативна съвместимост (дори и временен),

— които са получили сертификат за одобряване на типа.

8.6 **Извънредна процедура: първи сертификати за оперативна съвместимост за уреди за регистриране на данните за движението и тахографски карти от 2-ро поколение**

455) За период от 4 месеца след като една първа двойка от уреди за регистриране на данните за движението от 2-ро поколение и тахографски карти от 2-ро поколение (карта на водач, карта за монтаж и настройки, контролна карта и карта на превозвач) е била призната за оперативно съвместима, всеки издаден сертификат за оперативна съвместимост (включително първия), имащ отношение към заявките, получени през този период, се счита за временен.

456) След изтичане на този период, ако всички въпросни продукти са оперативно съвместими, всички съответни сертификати за оперативна съвместимост стават окончателни.

457) Ако по време на този период се появят неизправности, свързани с оперативната съвместимост, лабораторията, натоварена с провеждането на изпитванията за оперативна съвместимост, трябва да определи причините за проблемите с помощта на всички участващи производители и да прикани последните да направят необходимите промени.

458) Ако в края на този период проблемите, свързани с оперативната съвместимост, все още са налице, лабораторията, натоварена с провеждането на изпитванията, в сътрудничество със заинтересованите производители и с органите по одобряването на типа, определя причините за неизправностите, свързани с оперативната съвместимост, и определя промените, които всеки заинтересован производител трябва да направи. Търсенето на технически решения може да продължи най-много два месеца, след което Комисията, при липса на общо решение и след консултация с лабораторията, натоварена с извършването на изпитванията за оперативна съвместимост, решава на кой(кои) уред(и) и карти ще се издаде окончателен сертификат за оперативна съвместимост, като уточнява причините за своя избор.

459) Всяко искане за извършване на изпитвания за оперативна съвместимост, заведено от лабораторията във времето от края на периода от четири месеца след издаване на първия временен сертификат за оперативна съвместимост до датата на вземане на решение от Комисията, посочена в изискване 455, се отлага до решаване на първоначалните проблеми, свързани с оперативната съвместимост. Тези искания след това се обработват в реда на тяхното завеждане.

Допълнение 1

РЕЧНИК НА ДАННИТЕ

СЪДЪРЖАНИЕ

1. ВЪВЕДЕНИЕ

В настоящото допълнение са посочени форматите, елементите и структурата на данните, използвани от уредите за регистриране на данните за движението и тахографските карти.

1.1. **Подход към определенията на типовете данни**

В настоящото допълнение се използва абстрактно означаване на синтаксиса на информационна единица (ASN.1) за определяне на различните типове данни. Тази система позволява дефинирането на прости и структурирани данни, без да има нужда от използване на специфичен синтаксис за трансфер (правила за кодиране), които да зависят от съответното приложение и среда.

Правилата за наименуване от тип ASN.1 се изготвят съгласно стандарт ISO/IEC 8824-1. От това следва, че:

— в рамките на възможното значението на определен тип данни става ясно от избраните имена,

— ако определен тип данни се състои от други типове данни, името на този тип се представя винаги под формата на една-единствена последователност от буквени символи, започваща с главна буква, въпреки че главните букви се използват в името, за да предадат съответното значение,

— по принцип имената на типовете данни са свързани с името на типовете данни, от които са съставени, с оборудването, в което данните се съхраняват, и с функцията, която е асоциирана към съответните данни.

Ако тип ASN.1 вече е дефиниран като част от друг стандарт и ако е от значение за използването в уредите за регистриране на данните за движението, тогава този тип ASN.1 се дефинира в настоящото допълнение.

За да е възможно прилагането на няколко типа правила за кодиране, някои типове ASN.1, упоменати в настоящото допълнение, са ограничени от идентификаторите на диапазона от стойности. Тези идентификатори са определени в параграф 3 и допълнение 2.

1.2. **Справочни материали**

В настоящото допълнение се използват следните справочни материали:

ISO 639	Код за представяне на наименованията на езиците. Първо издание: 1988 г.
ISO 3166	Кодове за представяне на наименованията на държавите и техните подразделения. Част 1: Кодове на държавите, 2013 г.
ISO 3779	Пътни превозни средства. Номер за идентифициране на превозните средства (VIN). Съдържание и структура. 2009 г.
ISO/IEC 7816-5	Идентификационни карти. Карти с интегрална(и) схема(и) с контакти. Част 5: Система за номериране и процедури по регистрация на идентификаторите на приложенията. Второ издание: 2004 г.
ISO/IEC 7816-6	Идентификационни карти. Карти с интегрални схеми. Част 6: Вътрешно-отраслови елементи от данни за взаимен обмен, 2004 г. + техническа поправка 1: 2006 г.
ISO/IEC 8824-1	Информационни технологии. Абстрактно означаване на синтаксиса на информационна единица (ASN.1). Спецификация на основната нотация 2008 г. + Техническа поправка 1: 2012 г. + Техническа поправка 2: 2014 г.
ISO/IEC 8825-2	Информационни технологии. Правила за кодиране на ASN.1. Спецификация на правилата за пакетно кодиране. 2008 г.
ISO/IEC 8859-1	Информационни технологии — Набори от графични символи, кодирани в байтове — Част 1: Латинска азбука № 1. Първо издание: 1998 г.
ISO/IEC 8859-7	Информационни технологии — Набори от графични символи, кодирани в байтове — Част 7: Латинска/гръцка азбука. 2003 г.

ISO 16844-3	Пътни превозни средства — Тахографски системи — Интерфейси на датчиците за движение. 2004 г. + Техническа поправка 1: 2006 г.
TR-03110-3	BSI / ANSSI Технически насоки TR-03110-3, усъвършенствани механизми за сигурност за машинночетими документи за пътуване и маркер eIDAS. Част 3: Общи спецификации, версия 2.20, 3. Февруари 2015 г.

2. ОПРЕДЕЛЕНИЯ НА ТИПОВЕТЕ ДАННИ

За всеки от следващите типове данни стойността по подразбиране за съдържание „неизвестно“ или „неприложимо“ води до запълване на елемента от данни с байтове „FF“.

Всички типове данни се използват за приложенията от поколение 1 и 2, освен ако е посочено нещо друго.

2.1. **ActivityChangeInfo**

Този тип данни позволява кодирането във вид на дума от два байта на статуса на процепа в 00.00 часа и/или на състоянието при управление в 00.00 часа и/или на промените на дейността, и/или на промените на състоянието при управление, и/или на промените на статуса на картата на водач или втория водач. Този тип данни е свързан с изисквания 105, 266, 291, 320, 321, 343 и 344 от приложение 1B.

```
ActivityChangeInfo ::= OCTET STRING (SIZE(2))
```

Присвояване на стойност — синхронизиран октет: ‘scpaatttttttttt’B (16 бита)

За записването на паметта за данни (или статус на процепа):

‘s’B	Процеп:
	‘0’B: ВОДАЧ,
	‘1’B: ВТОРИ ВОДАЧ,
‘c’B	Състояние при:
	‘0’B: САМ,
	‘1’B: ЕКИПАЖ,
‘p’B	Статус на картата на водач (или картата за монтаж и настройки) в съответния процеп:
	‘0’B: ВКАРАНА, картата е вкарана,
	‘1’B: НЕ Е ВКАРАНА, не е вкарана карта (или картата е извадена),
‘aa’B	Дейност:
	‘00’B: ПРЕКЪСВАНЕ/ПОЧИВКА,
	‘01’B: НА РАЗПОЛОЖЕНИЕ,
	‘10’B: РАБОТА,
	‘11’B: УПРАВЛЕНИЕ,
‘ttttttttttt’B	Време на промяната: брой минути, изтекли след 00.00 часа на съответния ден.

Относно записите на картата на водач (или картата за монтаж и настройки) (и състоянието при управление):

‘s’B	Процеп (не е от значение, ако ‘p’=1 освен забележката по-долу):
	‘0’B: ВОДАЧ,
	‘1’B: ВТОРИ ВОДАЧ,
‘c’B	Състояние при управление (‘p’=0) или
	след статус на дейността (‘p’=1):
	‘0’B: САМ,
	‘0’B: НЕИЗВЕСТНА ДЕЙНОСТ
	‘1’B: ЕКИПАЖ,
	‘1’B: ИЗВЕСТНА ДЕЙНОСТ (=ръчно въведена)
‘p’B	Статус на картата:
	‘0’B: ВКАРАНА, картата е вкарана в уред за регистриране на данните за движението,
	‘1’B: НЕ Е ВКАРАНА, не е вкарана картата (или картата е извадена),
‘aa’B	Дейност (не е от значение, когато ‘p’=1 и ‘c’=0 освен забележката по-долу):
	‘00’B: ПРЕКЪСВАНЕ/ПОЧИВКА,
	‘01’B: НА РАЗПОЛОЖЕНИЕ,
	‘10’B: РАБОТА,
	‘11’B: УПРАВЛЕНИЕ,
‘ttttttttttt’B	Време на промяната: брой минути, изтекли след 00.00 часа на съответния ден.

Забележка в случай на „Изваждане на картата“:

Когато картата е извадена:

— ‘s’ се прилага и указва процепа, откъдето е извадена картата,

— за ‘c’ трябва да се зададе 0,

— за ‘p’ трябва да се зададе 1,

— ‘aa’ трябва да кодира текущата дейност, избрана в същия момент.

Вследствие на ръчното въвеждане битовете ‘c’ и ‘aa’ на думата (съхранена на карта) могат да бъдат изтрити с цел отразяване на постъпването на съответните данни.

2.2. Address

Адрес.

```
Address ::= SEQUENCE {
   codePage                              INTEGER (0..255),
   address                               OCTET STRING (SIZE(35))
}
```

codePage указва набор от символи, определен в глава 4.

address е адрес, кодиран с използването на указания набор от символи.

2.3. **AESKey**

Поколение 2:

Ключ AES с дължина 128, 192 или 256 бита.

```
AESKey ::= CHOICE {
   aes128Key                          AES128Key,
   aes192Key                          AES192Key,
   aes256Key                          AES256Key
}
```

Присвояване на стойност: липса на допълнителна информация.

2.4. **AES128Key**

Поколение 2:

Ключ AES128.

```
AES128Key ::= SEQUENCE {
   length                             INTEGER(0..255),
   aes128Key                          OCTET STRING (SIZE(16))
}
```

length указва дължината на ключа AES128 в октети.

aes128Key е ключ AES с дължина от 128 бита.

Присвояване на стойност:

Дължината трябва да е със стойност 16.

2.5. **AES192Key**

Поколение 2:

Ключ AES192.

```
AES192Key ::= SEQUENCE {
   length                             INTEGER(0..255),
   aes192Key                          OCTET STRING (SIZE(24))
}
```

length указва дължината на ключа AES192 в октети.

aes192Key е ключ AES с дължина от 192 бита.

Присвояване на стойност:

Дължината трябва да е със стойност 24.

2.6. **AES256Key**

Поколение 2:

Ключ AES256.

```
AES256Key ::= SEQUENCE {
   length                                  INTEGER(0..255),
   aes256Key                               OCTET STRING (SIZE(32))
}
```

length указва дължината на ключа AES256 в октети.

aes156Key е ключ AES с дължина от 256 бита.

Присвояване на стойност:

Дължината трябва да е със стойност 32.

2.7. **BCDString**

BCDString се прилага при представяне в двоичен код на данни, представени в десетичен вид (DCB). Този тип данни се използва за представяне на десетично число чрез един полуоктет (4 бита). BCDString се основава на ISO/IEC 8824-1 „CharacterStringType“.

```
BCDString ::= CHARACTER STRING (WITH COMPONENTS {
   identification ( WITH COMPONENTS {
   fixed PRESENT }) })
```

BCDString използва нотацията „hstring“. Най-лявото шестнадесетично число трябва да е най-старши полуоктет на първия октет. За да се получи кратно число на октетите, е необходимо според нуждите да се вмъкне съответният брой младши нулеви полуоктети от най-лявата позиция на полуоктета на първия октет.

Допустими цифри: 0, 1, .. 9.

2.8. **CalibrationPurpose**

Код, указващ причината за записване на набор от параметри за калибриране. Този тип данни е свързан с изисквания 097 и 098 от приложение 1Б и изискване 119 от приложение 1В.

```
CalibrationPurpose ::= OCTET STRING (SIZE(1))
```

Присвояване на стойност:

Поколение 1:

‘00’H	запазена стойност,
‘01’H	активиране: записване на параметрите за калибриране, известни в момента на активиране на бордовото устройство,
‘02’H	първо монтиране: първо калибриране на бордовото устройство след активирането му,
‘03’H	монтиране: първо калибриране на бордовото устройство в съответното превозно средство,
‘04’H	периодичен технически преглед.

Поколение 2:

В допълнение към поколение 1 се използват следните стойности:

‘05’H въвеждане на VRN от превозвача,

‘06’H сверяване на часовника без калибриране,

‘07’H до ‘7F’H RFU,

‘80’H до ‘FF’H Фабрични характеристики.

2.9. CardActivityDailyRecord

Информация, съхранена на карта и отнасяща се до дейностите на водача в определен календарен ден. Този тип данни е свързан с изисквания 266, 291, 320 и 343 от приложение 1B.

```
CardActivityDailyRecord ::= SEQUENCE {
   activityPreviousRecordLength         INTEGER(0..CardActivityLengthRange),
   activityRecordLength                 INTEGER(0..CardActivityLengthRange),
   activityRecordDate                   TimeReal,
   activityDailyPresenceCounter         DailyPresenceCounter,
   activityDayDistance                  Distance,
   activityChangeInfo                   SET SIZE(1..1440) OF ActivityChangeInfo
}
```

activityPreviousRecordLength е общата дължина на предишния дневен запис, изразена в байтове. Максималната стойност съответства на дължината на OCTET STRING, съдържащ тези записи (вж. CardActivity-LengthRange, допълнение 2, параграф 4). Когато този запис е най-старият дневен запис, за стойността на activity-PreviousRecordLength трябва да се зададе 0.

activityRecordLength е общата дължина на този запис, изразена в байтове. Максималната стойност съответства на дължината на OCTET STRING, съдържащ тези записи.

activityRecordDate е датата на записа.

activityDailyPresenceCounter е състоянието за съответния ден на брояча на присъствените дни за картата.

activityDayDistance е общото изминато разстояние през съответния ден.

activityChangeInfo указва за съответния ден набора от данни ActivityChangeInfo, който се отнася за водача. Той не може да съдържа повече от 1440 стойности (една промяна на дейност в минута). Този набор съдържа винаги ActivityChangeInfo, който кодира състоянието при управление в 00:00 часа.

2.10. CardActivityLengthRange

Брой на байтовете в карта на водач или карта за монтаж и настройки, които са налични за съхранение на записите за дейностите на водача.

```
CardActivityLengthRange ::= INTEGER(0..2^16-1)
```

Присвояване на стойност: вж. допълнение 2.

2.11. CardApprovalNumber

Номер на одобрение на типа на картата.

```
CardApprovalNumber ::= IA5String(SIZE(8))
```

Присвояване на стойност:

Номерът на одобрение е този, който е публикуван на съответната интернет страница на Европейската комисия, т.е. например, като се включват тиренца, ако има. Номерът на одобрение се подравнява отляво.

2.12. CardCertificate

Поколение 1:

Сертификат на публичния ключ на карта.

```
CardCertificate ::= Certificate
```

2.13. CardChipIdentification

Информация, съхранена на карта и отнасяща се до идентификация на интегралната схема (ИС) на картата (изискване 249 от приложение 1B). icSerialNumber и icManufacturingReferences идентифицират уникално чипа на картата. Самостоятелно icSerialNumber не идентифицира уникално чипа на картата.

```
CardChipIdentification ::= SEQUENCE {
   icSerialNumber                    OCTET STRING (SIZE(4)),
   icManufacturingReferences         OCTET STRING (SIZE(4))
}
```

icSerialNumber е серийният номер на ИС.

icManufacturingReferences е специфичният идентификатор на производителя на ИС.

2.14. CardConsecutiveIndex

Индекс за пореден номер на картата (определение з).

```
CardConsecutiveIndex ::= IA5String(SIZE(1))
```

Присвояване на стойност: (вж. приложение 1B, глава 7)

Възходящ ред: '0, …, 9, A, …, Z, a, …, z'

2.15. CardControlActivityDataRecord

Информация, съхранена на карта на водач или карта за монтаж и настройки и отнасяща се до последната проверка на водача (изисквания 274, 299, 327 и 350 от приложение 1B).

```
CardControlActivityDataRecord ::= SEQUENCE {
   controlType                       ControlType,
   controlTime                       TimeReal,
   controlCardNumber                 FullCardNumber,
   controlVehicleRegistration        VehicleRegistrationIdentification,
   controlDownloadPeriodBegin        TimeReal,
   controlDownloadPeriodEnd          TimeReal
}
```

controlType е типът проверка.

controlTime е датата и часът на проверката.

controlCardNumber е FullCardNumber на служителя на контролен орган, който е извършил проверката.

controlVehicleRegistration посочва VRN и регистриращата превозното средство държава членка, където е извършена проверката.

controlDownloadPeriodBegin и **controlDownloadPeriodEnd** са периодът, за който са изтеглени данни, при наличие на такова изтегляне на данни.

2.16. CardCurrentUse

Информация относно актуалната употреба на картата (изискване 273, 298, 326 и 349 от приложение 1B).

```
CardCurrentUse ::= SEQUENCE {
   sessionOpenTime                    TimeReal,
   sessionOpenVehicle                 VehicleRegistrationIdentification
}
```

sessionOpenTime е моментът на вкарване на картата за актуалната употреба. Този елемент се нулира при изваждане на картата.

sessionOpenVehicle е идентификацията на понастоящем използваното превозно средство след вкарване на картата. Този елемент се нулира при изваждане на картата.

2.17. CardDriverActivity

Информация, съхранена на карта на водач или карта за монтаж и настройки и отнасяща се до дейностите на водача (изисквания 267, 268, 292, 293, 321 и 344 от приложение 1B).

```
CardDriverActivity ::= SEQUENCE {
   activityPointerOldestDayRecord     INTEGER(0.. CardActivityLengthRange-1),
   activityPointerNewestRecord        INTEGER(0.. CardActivityLengthRange-1),
   activityDailyRecords               OCTET STRING
                                      (SIZE(CardActivityLengthRange))
}
```

activityPointerOldestDayRecord е спецификацията на началото на мястото на съхранение (брой на байтовете от началото на низа) на най-стария пълен дневен запис в низа activityDailyRecords. Максималната стойност съответства на дължината на низа.

activityPointerNewestRecord е спецификацията на началото на мястото на съхранение (брой на байтовете от началото на низа) на най-скорошния дневен запис в низа activityDailyRecords. Максималната стойност съответства на дължината на низа.

activityDailyRecords е мястото, което е налично за съхранение на данните относно дейностите на водача (структура на данни: CardActivityDailyRecord) за всеки календарен ден, през който картата е била използвана.

Присвояване на стойност: този низ от октети се попълва циклично със записи от CardActivityDailyRecord. При първото използване съхранението започва на първия байт на низа. Следващите записи се запаметяват в края на предишния. Когато низът се запълни, съхранението продължава от първия байт на низа, независимо от прекъсването вътре в елемент от данни. Преди да се въведат нови данни за дейността в низа (като се разшири текущият activityDailyRecord или като се въведе нов activityDailyRecord), които заместват по-старите данни за дейността, е необходимо да се актуализира activityPointerOldestDayRecord, за да се отрази новото местоположение на най-стария пълен дневен запис, и трябва да се нулира activityPreviousRecordLength на този (нов) най-стар пълен дневен запис.

2.18. CardDrivingLicenceInformation

Информация, съхранена на карта на водач и отнасяща се до свидетелството за управление на титуляря на картата (изисквания 259 и 284 от приложение 1B).

```
CardDrivingLicenceInformation ::= SEQUENCE {
   drivingLicenceIssuingAuthority       Name,
   drivingLicenceIssuingNation          NationNumeric,
   drivingLicenceNumber                 IA5String(SIZE(16))
}
```

drivingLicenceIssuingAuthority е компетентният орган за издаване на свидетелството за управление.

drivingLicenceIssuingNation е националността на органа, издал свидетелството за управление.

drivingLicenceNumber е номерът на свидетелството за управление.

2.19. CardEventData

Информация, съхранена на карта на водач или карта за монтаж и настройки и отнасяща се до събитията, свързани с титуляря на картата (изисквания 260, 285, 318 и 341 от приложение 1B).

```
CardEventData ::= SEQUENCE SIZE(6) OF {
   cardEventRecords                     SET SIZE(NoOfEventsPerType) OF
                                        CardEventRecord
}
```

CardEventData е последователност във възходящ ред от EventFaultType и cardEventRecords (с изключение на записите относно опитите за нарушаване на сигурността, които са групирани в последния блок от данни на последователността).

cardEventRecords е набор от записи на събития от определен тип (или категория от събития във връзка с опити за нарушаване на сигурността).

2.20. CardEventRecord

Информация, съхранена на карта на водач или карта за монтаж и настройки и отнасяща се до събитие, свързано с титуляря на картата (изисквания 261, 286, 318 и 341 от приложение 1B).

```
CardEventRecord ::= SEQUENCE {
   eventType                            EventFaultType,
   eventBeginTime                       TimeReal,
   eventEndTime                         TimeReal,
   eventVehicleRegistration             VehicleRegistrationIdentification
}
```

eventType е типът на събитието.

eventBeginTime е датата и часът на начало на събитието.

eventEndTime е датата и часът на край на събитието.

eventVehicleRegistration посочва VRN и регистриращата превозното средство държава членка, в която се е случило събитието.

2.21. CardFaultData

Информация, съхранена на карта на водач или карта за монтаж и настройки и отнасяща се до неизправности, свързани с титуляря на картата (изисквания 263, 288, 318 и 341 от приложение 1B).

```
CardFaultData ::= SEQUENCE SIZE(2) OF {
   cardFaultRecords                     SET SIZE(NoOfFaultsPerType) OF
                                        CardFaultRecord
}
```

CardFaultData е последователност, съдържаща набор от записи за неизправности, засягащи уредите за регистриране на данните за движението, и последван от набор записи за неизправностите във връзка с картата.

cardFaultRecords е набор от записи за неизправности в определена категория неизправности (уреди за регистриране на данните за движението или карти).

2.22. CardFaultRecord

Информация, съхранена на карта на водач или карта за монтаж и настройки и отнасяща се до неизправност, свързана с титуляря на картата (изисквания 264, 289, 318 и 341 от приложение 1B).

```
CardFaultRecord ::= SEQUENCE {
   faultType                          EventFaultType,
   faultBeginTime                     TimeReal,
   faultEndTime                       TimeReal,
   faultVehicleRegistration           VehicleRegistrationIdentification
}
```

faultType е типът неизправност.

faultBeginTime е датата и часът на начало на неизправността.

faultEndTime е датата и часът на край на неизправността.

faultVehicleRegistration посочва VRN и регистриращата превозното средство държава членка, в която се е случила съответната неизправност.

2.23. CardIccIdentification

Информация, съхранена на карта и отнасяща се до идентификация на картата с интегрална схема (ИС) (изискване 248 от приложение 1B).

```
CardIccIdentification ::= SEQUENCE {
   clockStop                          OCTET STRING (SIZE(1)),
   cardExtendedSerialNumber           ExtendedSerialNumber,
   cardApprovalNumber                 CardApprovalNumber,
   cardPersonaliserID                 ManufacturerCode,
   embedderIcAssemblerId              EmbedderIcAssemblerId,
   icIdentifier                       OCTET STRING (SIZE(2))
}
```

clockStop е режимът clockStop, определен в допълнение 2.

cardExtendedSerialNumber е уникалният сериен номер на ИС на картата, допълнително специфициран от типа данни ExtendedSerialNumber.

cardApprovalNumber е номерът на одобрение на типа на картата.

cardPersonaliserID е идентификатор на организацията, персонализирала картата, изразен чрез ManufacturerCode.

embedderIcAssemblerId осигурява информация за интегратора/монтажника на ИС.

icIdentifier е идентификаторът на ИС на картата и производителя на нейната ИС, определен в стандарт ISO/IEC 7816-6.

2.24. CardIdentification

Информация, съхранена на карта и отнасяща се до идентификация на картата (изисквания 255, 280, 310, 333, 359, 365, 371 и 377 от приложение 1B).

```
CardIdentification ::= SEQUENCE {
   cardIssuingMemberState              NationNumeric,
   cardNumber                          CardNumber,
   cardIssuingAuthorityName            Name,
   cardIssueDate                       TimeReal,
   cardValidityBegin                   TimeReal,
   cardExpiryDate                      TimeReal
}
```

cardIssuingMemberState е кодът на държавата членка, издаваща картата.

cardNumber е номерът на картата.

cardIssuingAuthorityName е наименованието на органа, издал картата.

cardIssueDate е датата на издаване на картата на актуалния ѝ титуляр.

cardValidityBegin е първата дата на валидност на картата.

cardExpiryDate е датата на край на валидност на картата.

2.25. CardMACertificate

Поколение 2:

Сертификат на публичния ключ на картата за общо удостоверяване с бордовото устройство. Структурата на този сертификат е посочена в допълнение 11.

```
CardMACertificate ::= Certificate
```

2.26. CardNumber

Номер на картата съгласно определение ж).

```
CardNumber ::= CHOICE {
   SEQUENCE {
      driverIdentification             IA5String(SIZE(14)),
      cardReplacementIndex             CardReplacementIndex,
      cardRenewalIndex                 CardRenewalIndex
   },
   SEQUENCE {
      ownerIdentification              IA5String(SIZE(13)),
      cardConsecutiveIndex             CardConsecutiveIndex,
      cardReplacementIndex             CardReplacementIndex,
      cardRenewalIndex                 CardRenewalIndex
   }
}
```

driverIdentification е уникалната идентификация на водач в държава членка.

ownerIdentification е уникалната идентификация на превозвач, сервиз или контролен орган в държава членка.

cardConsecutiveIndex е индексът за пореден номер на картата.

cardReplacementIndex е индексът за замяна на картата.

cardRenewalIndex е индексът за подновяване на валидността на картата.

Първата последователност от селекцията позволява да се кодира номерът на картата на водач, втората последователност — номерата на контролната карта, картата за монтаж и настройки и на картата на превозвач.

2.27. CardPlaceDailyWorkPeriod

Информация, съхранена на карта на водач или карта за монтаж и настройки и отнасяща се за местата в началото и/или в края на дневните периоди на работа (изисквания 272, 297, 325 и 348 от приложение 1B).

```
CardPlaceDailyWorkPeriod ::= SEQUENCE {
   placePointerNewestRecord    INTEGER(0 .. NoOfCardPlaceRecords-1),
   placeRecords                SET SIZE(NoOfCardPlaceRecords) OF PlaceRecord
}
```

placePointerNewestRecord е индексът на последния актуализиран запис за местоположението.

Присвояване на стойност: число, съответстващо на номератора на записа за местоположението, като се започва с 0 за първия случай на записи за местоположението в структурата.

placeRecords е наборът от записи, съдържащ данните относно въведените местоположения.

2.28. CardPrivateKey

Поколение 1:

Частен ключ на карта.

```
CardPrivateKey ::= RSAKeyPrivateExponent
```

2.29. CardPublicKey

Публичен ключ на карта.

```
CardPublicKey ::= PublicKey
```

2.30. CardRenewalIndex

Индекс за подновяване на валидността на картата (определение и).

```
CardRenewalIndex ::= IA5String(SIZE(1))
```

Присвояване на стойност: (вж. глава VII от настоящото приложение).

‘0’ Първо издаване.

Възходящ ред: ‘0, …, 9, A, …, Z’

2.31. CardReplacementIndex

Индекс за замяна на картата (определение й).

```
CardReplacementIndex ::= IA5String(SIZE(1))
```

Присвояване на стойност: (вж. глава VII от настоящото приложение).

‘0’ Оригинална карта.

Възходящ ред: ‘0, …, 9, A, …, Z’

2.32. **CardSignCertificate**

Поколение 2:

Сертификат на публичния ключ на картата за подпис. Структурата на този сертификат е посочена в допълнение 11.

```
CardSignCertificate ::= Certificate
```

2.33. **CardSlotNumber**

Код, позволяващ да се разграничат двата процепа на бордово устройство.

```
CardSlotNumber ::= INTEGER {
   driverSlot                          (0),
   co-driverSlot                       (1)
}
```

Присвояване на стойност: липса на допълнителна информация.

2.34. **CardSlotsStatus**

Код, указващ типа на картите, вкарани в двата процепа на бордовото устройство.

```
CardSlotsStatus ::= OCTET STRING (SIZE(1))
```

Присвояване на стойност — синхронизиран октет: 'ccccdddd'B

'cccc'B Идентификация на типа на картата, вкарана в процепа за втория водач,

'dddd'B Идентификация на типа на картата, вкарана в процепа за водача,

с помощта на следните кодове за идентификация:

'0000'B не е вкарана карта,

'0001'B вкарана е карта на водач,

'0010'B вкарана е карта за монтаж и настройки,

'0011'B вкарана е контролна карта,

'0100'B вкарана е карта на превозвач.

2.35. **CardSlotsStatusRecordArray**

Поколение 2:

CardSlotsStatus плюс метаданните, използвани в протокола за изтегляне на данни.

```
CardSlotsStatusRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF CardSlotsStatus
}
```

recordType указва типа на записа (CardSlotsStatus). **Присвояване на стойност**: вж. RecordType.

recordSize е размерът на CardSlotsStatus в байтове.

noOfRecords е броят на записите в набора от записи.

records е наборът от записи на CardSlotsStatus.

2.36. CardStructureVersion

Код, указващ версията на структурата, приложена в определена тахографска карта.

```
CardStructureVersion ::= OCTET STRING (SIZE(2))
```

Присвояване на стойност: 'aabb'H:

'aa'H Индекс за промените на структурата.

'00'H за приложенията от поколение 1

'01'H за приложенията от поколение 2

'bb'H Индекс за промените, отнасящи се до използването на елементи от данни, определени за съответната структурата от високия байт.

'00'H за тази версия на приложенията от поколение 1

'00'H за тази версия на приложенията от поколение 2

2.37. CardVehicleRecord

Информация, съхранена на карта на водач или карта за монтаж и настройки и отнасяща се до период на използване на превозно средство през определен календарен ден (изисквания 269, 294, 322 и 345 от приложение 1B).

Поколение 1:

```
CardVehicleRecord ::= SEQUENCE {
   vehicleOdometerBegin                    OdometerShort,
   vehicleOdometerEnd                      OdometerShort,
   vehicleFirstUse                         TimeReal,
   vehicleLastUse                          TimeReal,
   vehicleRegistration                     VehicleRegistrationIdentification,
   vuDataBlockCounter                      VuDataBlockCounter
}
```

vehicleOdometerBegin е стойността от километражния брояч на превозното средство в началото на периода на използване на превозното средство.

vehicleOdometerEnd е стойността от километражния брояч на превозното средство в края на периода на използване на превозното средство.

vehicleFirstUse е датата и часът на начало на периода на използване на превозното средство.

vehicleLastUse е датата и часът на край на периода на използване на превозното средство.

vehicleRegistration посочва VRN и държавата членка, регистрираща превозното средство.

vuDataBlockCounter е стойността на vuDataBlockCounter при последното извличане на периода на използване на превозното средство.

Поколение 2:

```
CardVehicleRecord ::= SEQUENCE {
   vehicleOdometerBegin                    OdometerShort,
   vehicleOdometerEnd                      OdometerShort,
   vehicleFirstUse                         TimeReal,
   vehicleLastUse                          TimeReal,
   vehicleRegistration                     VehicleRegistrationIdentification,
   vuDataBlockCounter                      VuDataBlockCounter,
   vehicleIdentificationNumber             VehicleIdentificationNumber
}
```

В допълнение към поколение 1 се използва следният елемент от данни:

VehicleIdentificationNumber е идентификационният номер на превозното средство, обозначаващ цялото превозно средство.

2.38. **CardVehiclesUsed**

Информация, съхранена на карта на водач или карта за монтаж и настройки и отнасяща се до превозните средства, използвани от титуляря на картата (изисквания 270, 295, 323 и 346 от приложение 1B).

```
CardVehiclesUsed := SEQUENCE {
   vehiclePointerNewestRecord          INTEGER(0..NoOfCardVehicleRecords-1),
   cardVehicleRecords                  SET SIZE(NoOfCardVehicleRecords) OF
                                       CardVehicleRecord
}
```

vehiclePointerNewestRecord е индексът на последния актуализиран запис на превозното средство.

Присвояване на стойност: число, съответстващо на номератора на записа за превозното средство, като се започва с 0 за първия случай на записи за превозното средство в структурата.

cardVehicleRecords е наборът от записи, съдържащ информация за използваните превозни средства.

2.39. **CardVehicleUnitRecord**

Поколение 2:

Информация, съхранена на карта на водач или карта за монтаж и настройки и отнасяща се до използвано бордово устройство (изисквания 303 и 351 от приложение 1B).

```
CardVehicleUnitRecord ::= SEQUENCE {
   timeStamp                           TimeReal,
   manufacturerCode                    ManufacturerCode,
   deviceID                            INTEGER(0..255),
   vuSoftwareVersion                   VuSoftwareVersion
}
```

timeStamp е началото на периода на използване на бордовото устройство (т.е. първото вкарване на картата в бордовото устройство за периода).

manufacturerCode идентифицира производителя на бордовото устройство.

deviceID идентифицира типа бордово устройство на производител. Стойността е специфична за съответния производител.

vuSoftwareVersion е номерът на версията на софтуера на бордовото устройство.

2.40. **CardVehicleUnitsUsed**

Поколение 2:

Информация, съхранена на карта на водач или карта за монтаж и настройки и отнасяща се до използваните бордови устройства от титуляря на картата (изисквания 306 и 352 от приложение 1B).

```
CardVehicleUnitsUsed := SEQUENCE {
   vehicleUnitPointerNewestRecord       INTEGER(0..NoOfCardVehicleUnitRecords-1),
   cardVehicleUnitRecords               SET SIZE(NoOfCardVehicleUnitRecords) OF
                                        CardVehicleUnitRecord
}
```

vehicleUnitPointerNewestRecord е индексът на последния актуализиран запис на бордовото устройство.

Присвояване на стойност: число, съответстващо на номератора на записа за бордовото устройство, като се започва с 0 за първия случай на записи за бордовото устройство в структурата.

cardVehicleUnitRecords е наборът от записи, съдържащ информация за използваните бордови устройства.

2.41. Certificate

Сертификатът на публичен ключ, издаден от сертификационен орган.

Поколение 1:

```
Certificate ::= OCTET STRING (SIZE(194))
```

Присвояване на стойност: електронен подпис с частично възстановяване на CertificateContent съгласно общите механизми за сигурност от допълнение 11: подпис (128 байта) || Остатък от публичния ключ (58 байта) || Посочване на сертификационния орган (8 байта).

Поколение 2:

```
Certificate ::= OCTET STRING (SIZE(204..341))
```

Присвояване на стойност: вж. допълнение 11.

2.42. CertificateContent

Поколение 1:

Съдържанието (което е достъпно) на сертификат на публичен ключ съгласно общите механизми за сигурност от допълнение 11.

```
CertificateContent ::= SEQUENCE {
   certificateProfileIdentifier         INTEGER(0..255),
   certificationAuthorityReference      KeyIdentifier,
   certificateHolderAuthorisation       CertificateHolderAuthorisation,
   certificateEndOfValidity             TimeReal,
   certificateHolderReference           KeyIdentifier,
   publicKey                            PublicKey
}
```

certificateProfileIdentifier е версията на съответния сертификат.

Присвояване на стойност: '01h' за тази версия.

certificationAuthorityReference идентифицира сертификационния орган, издаващ сертификата. Тази информация указва също така публичния ключ на този сертификационен орган.

certificateHolderAuthorisation идентифицира правата на титуляря на сертификата.

certificateEndOfValidity е датата, когато от административна гледна точка изтича срокът на валидност на сертификата.

certificateHolderReference идентифицира титуляря на сертификата. Тази информация указва също така публичния ключ.

publicKey е публичният ключ, сертифициран с този сертификат.

2.43. **CertificateHolderAuthorisation**

Идентифициране на правата на титуляря на сертификат.

```
CertificateHolderAuthorisation ::= SEQUENCE {
   tachographApplicationID              OCTET STRING(SIZE(6))
   equipmentType                        EquipmentType
}
```

Поколение 1:

tachographApplicationID е идентификаторът на тахографското приложение.

Присвояване на стойност: ‘FFh’ ‘54h’ ‘41h’ ‘43h’ ‘48h’ ‘4Fh’. Този AID е идентификатор на нерегистрирано приложение, което е обект на права на собственост съгласно ISO/IEC 7816-5.

equipmentType е идентификацията на типа оборудване, за което е предназначен сертификатът.

Присвояване на стойност: съгласно типа данни EquipmentType. **0**, ако сертификатът е издаден от някоя от държавите членки.

Поколение 2:

tachographApplicationID указва 6-те най-старши байта на идентификатора на приложението на тахографската карта от поколение 2 (AID). AID за приложението на тахографската карта е посочен в глава 6.2.

Присвояване на стойност: ‘FF 53 4D 52 44 54’.

equipmentType е идентификацията на типа оборудване, както е посочено за поколение 2, за който е предназначен сертификатът.

Присвояване на стойност: съгласно типа данни EquipmentType.

2.44. **CertificateRequestID**

Уникална идентификация на заявка за сертификат. Може също така да се използва за идентификатор на публичния ключ на бордовото устройство, в случай че серийният номер на бордовото устройство, за което е предназначен ключът, е неизвестен към момента на генериране на сертификата.

```
CertificateRequestID ::= SEQUENCE{
   requestSerialNumber                  INTEGER(0..2^32-1),
   requestMonthYear                     BCDString(SIZE(2)),
   crIdentifier                         OCTET STRING(SIZE(1)),
   manufacturerCode                     ManufacturerCode
}
```

requestSerialNumber е сериен номер на заявката за сертификат, който е уникален за производителя и месеца по-долу.

requestMonthYear е идентификацията на месеца и годината на заявката за сертификат.

Присвояване на стойност: кодиране BCD на месеца (две цифри) и годината (последните две цифри).

crIdentifier: идентификатор, позволяващ да се прави разлика между заявка за сертификат и разширен сериен номер.

Присвояване на стойност: ‘FFh’.

manufacturerCode: цифровият код на производителя, подаващ заявката за сертификат.

2.45. **CertificationAuthorityKID**

Идентификатор на публичния ключ на сертификационен орган (държава членка или европейския сертификационен орган).

```
CertificationAuthorityKID ::= SEQUENCE{
   nationNumeric                        NationNumeric,
   nationAlpha                          NationAlpha,
   keySerialNumber                      INTEGER(0..255),
   additionalInfo                       OCTET STRING(SIZE(2)),
   caIdentifier                         OCTET STRING(SIZE(1))
}
```

nationNumeric е националният цифров код на сертификационния орган.

nationAlpha е националният буквено-цифров код на сертификационния орган.

keySerialNumber е сериен номер, позволяващ да се прави разлика между различните ключове на сертификационния орган, ако някои ключове са променени.

additionalInfo е поле от два байта за допълнително кодиране (специфични за сертификационния орган).

caIdentifier е идентификатор, позволяващ да се прави разлика между идентификатор на ключ на сертификационен орган и други идентификатори на ключове.

Присвояване на стойност: '01h'.

2.46. CompanyActivityData

Информация, съхранена на карта на превозвач и отнасяща се до дейности, извършени с картата (изисквания 373 и 379 от приложение 1B).

```
CompanyActivityData ::= SEQUENCE {
   companyPointerNewestRecord         INTEGER(0..NoOfCompanyActivityRecords-1),
   companyActivityRecords             SET SIZE(NoOfCompanyActivityRecords) OF
    companyActivityRecord              SEQUENCE {
     companyActivityType                 CompanyActivityType,
     companyActivityTime                 TimeReal,
     cardNumberInformation               FullCardNumber,
     vehicleRegistrationInformation      VehicleRegistrationIdentification,
     downloadPeriodBegin                 TimeReal,
     downloadPeriodEnd                   TimeReal
    }
}
```

companyPointerNewestRecord е индексът на последния актуализиран companyActivityRecord.

Присвояване на стойност: число, съответстващо на номератора на записа за дейността на превозвача, като се започва с 0 за първия случай на запис за дейността на превозвача в структурата.

companyActivityRecords е наборът от всички записи за дейността на превозвача.

companyActivityRecord е последователността от данни, свързани с определена дейност на превозвача.

companyActivityType е типът дейност на превозвача.

companyActivityTime е датата и часът на дейността на превозвача.

cardNumberInformation е номерът на картата и ако е необходимо — посочване на държавата членка, където е издадена картата, от която са изтеглени данните.

vehicleRegistrationInformation посочва VRN и регистриращата превозното средство държава членка, като тази информация може да е изтеглена, блокирана или разблокирана.

downloadPeriodBegin и **downloadPeriodEnd** са периодът, за който са изтеглени данни от бордовото устройство, ако има такъв.

2.47. **CompanyActivityType**

Код за дейност, провеждана от определен превозвач, използващ своята карта на превозвач.

```
CompanyActivityType ::= INTEGER {
   card downloading                    (1),
   VU downloading                      (2),
   VU lock-in                          (3),
   VU lock-out                         (4)
}
```

2.48. **CompanyCardApplicationIdentification**

Информация, съхранена на карта на превозвач и отнасяща се за идентификация на приложението на картата (изисквания 369 и 375 от приложение 1B).

```
CompanyCardApplicationIdentification ::= SEQUENCE {
   typeOfTachographCardId              EquipmentType,
   cardStructureVersion                CardStructureVersion,
   noOfCompanyActivityRecords          NoOfCompanyActivityRecords
}
```

typeOfTachographCardId обозначава използвания тип карта.

cardStructureVersion указва версията на структурата, приложена в картата.

noOfCompanyActivityRecords е броят на записите за дейността на превозвача, които картата може да съхранява.

2.49. **CompanyCardHolderIdentification**

Информация, съхранена на карта на превозвач и отнасяща се за идентификация на титуляря на картата (изисквания 372 и 378 от приложение 1B).

```
CompanyCardHolderIdentification ::= SEQUENCE {
   companyName                         Name,
   companyAddress                      Address,
   cardHolderPreferredLanguage         Language
}
```

companyName е наименованието на превозвача, който притежава картата.

companyAddress е адресът на превозвача, който притежава картата.

cardHolderPreferredLanguage е предпочитаният език на титуляря на картата.

2.50. **ControlCardApplicationIdentification**

Информация, съхранена на контролна карта и отнасяща се за идентификация на приложението на картата (изисквания 357 и 363 от приложение 1B).

```
ControlCardApplicationIdentification ::= SEQUENCE {
   typeOfTachographCardId              EquipmentType,
   cardStructureVersion                CardStructureVersion,
   noOfControlActivityRecords          NoOfControlActivityRecords
}
```

typeOfTachographCardId обозначава използвания тип карта.

cardStructureVersion указва версията на структурата, приложена в картата.

noOfControlActivityRecords е броят на записите за контролната дейност, които картата може да съхранява.

2.51. **ControlCardControlActivityData**

Информация, съхранена на контролна карта и отнасяща се до определена контролна дейност, извършена с картата (изисквания 361 и 367 от приложение 1B).

```
ControlCardControlActivityData ::= SEQUENCE {
   controlPointerNewestRecord        INTEGER(0.. NoOfControlActivityRecords-1),
   controlActivityRecords            SET SIZE(NoOfControlActivityRecords) OF
    controlActivityRecord             SEQUENCE {
     controlType                       ControlType,
     controlTime                       TimeReal,
     controlledCardNumber              FullCardNumber,
     controlledVehicleRegistration     VehicleRegistrationIdentification,
     controlDownloadPeriodBegin        TimeReal,
     controlDownloadPeriodEnd          TimeReal
    }
}
```

controlPointerNewestRecord е индексът на последния актуализиран запис за контролната дейност.

Присвояване на стойност: число, съответстващо на номератора на записа за контролната дейност, като се започва с 0 за първия случай на запис за контролната дейност в структурата.

controlActivityRecords е наборът от всички записи за контролната дейност.

controlActivityRecord е последователността от информация, свързана с една проверка.

controlType е типът проверка.

controlTime е датата и часът на проверката.

controlledCardNumber посочва номера на картата и държавата членка, издаваща проверената карта.

controlledVehicleRegistration посочва VRN и регистриращата превозното средство държава членка, в която е извършена проверката.

controlDownloadPeriodBegin и **controlDownloadPeriodEnd** са периодът, за който са изтеглени евентуално данни.

2.52. **ControlCardHolderIdentification**

Информация, съхранена на контролна карта и отнасяща се за идентификация на титуляря на картата (изисквания 360 и 366 от приложение 1B).

```
ControlCardHolderIdentification ::= SEQUENCE {
   controlBodyName                   Name,
   controlBodyAddress                Address,
   cardHolderName                    HolderName,
   cardHolderPreferredLanguage       Language
}
```

controlBodyName е наименованието на контролния орган на титуляря на картата.

controlBodyAddress е адресът на контролния орган на титуляря на картата.

cardHolderName е фамилията и името (и презимето) на титуляря на контролната карта.

cardHolderPreferredLanguage е предпочитаният език на титуляря на картата.

2.53. **ControlType**

Код, указващ дейностите, извършени по време на проверка. Този тип данни е свързан с изисквания 126, 274, 299, 327 и 350 от приложение 1B.

```
ControlType ::= OCTET STRING (SIZE(1))
```

Поколение 1:

Присвояване на стойност — синхронизиран октет: ‘cvpdxxxx’B (8 бита)

‘c’B изтегляне на данни от картата:

‘0’B: не са изтеглени данни от картата при тази контролна дейност,

‘1’B: изтеглени са данни от картата при тази контролна дейност

‘v’B изтегляне на данни от бордовото устройство:

‘0’B: не са изтеглени данни от бордовото устройство при тази контролна дейност,

‘1’B: изтеглени са данни от бордовото устройство при тази контролна дейност

‘p’B отпечатване:

‘0’B: няма отпечатване при тази контролна дейност,

‘1’B: има отпечатване при тази контролна дейност

‘d’B изобразяване:

‘0’B: няма изобразяване при тази контролна дейност,

‘1’B: има изобразяване при тази контролна дейност

‘xxxx’B Не се използва.

Поколение 2:

Присвояване на стойност — синхронизиран октет: ‘cvpdexxx’B (8 бита)

‘c’B изтегляне на данни от картата:

‘0’B: не са изтеглени данни от картата при тази контролна дейност,

‘1’B: изтеглени са данни от картата при тази контролна дейност

‘v’B изтегляне на данни от бордовото устройство:

‘0’B: не са изтеглени данни от бордовото устройство при тази контролна дейност,

‘1’B: изтеглени са данни от бордовото устройство при тази контролна дейност

‘p’B отпечатване:

‘0’B: няма отпечатване при тази контролна дейност,

‘1’B: има отпечатване при тази контролна дейност

‘d’B изобразяване:

‘0’B: няма изобразяване при тази контролна дейност,

‘1’B: има изобразяване при тази контролна дейност

‘e’B пътна проверка на калибрирането:

‘0’B: не са проверени параметрите за калибриране при тази контролна дейност,

‘1’B: проверени са параметрите за калибриране при тази контролна дейност

‘xxx’B RFU.

2.54. **CurrentDateTime**

Актуалната дата и час на уредите за регистриране на данните за движението.

```
CurrentDateTime ::= TimeReal
```

Присвояване на стойност: липса на допълнителна информация.

2.55. **CurrentDateTimeRecordArray**

Поколение 2:

Актуалната дата и час плюс метаданните, използвани в протокола за изтегляне на данни.

```
CurrentDateTimeRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF CurrentDateTime
}
```

recordType указва типа на записа (CurrentDateTime). **Присвояване на стойност**: вж. RecordType.

recordSize е размерът на CurrentDateTime в байтове.

noOfRecords е броят на записите в набора от записи.

records е набор от записи на актуалната дата и час.

2.56. **DailyPresenceCounter**

Брояч, съхранен на карта на водач или карта за монтаж и настройки, чиято стойност се увеличава с едно за всеки календарен ден, когато картата е била вкарана в бордово устройство. Този тип данни е свързан с изисквания 266, 299, 320 и 343 от приложение 1B.

```
DailyPresenceCounter ::= BCDString(SIZE(2))
```

Присвояване на стойност: последователен номер с максималната стойност = 9999, като се започва от 0. При първото издаване на картата номерът е 0.

2.57. **Datef**

Дата, изразена в цифров формат, който може да се разпечата веднага.

```
Datef ::= SEQUENCE {
   year        BCDString(SIZE(2)),
   month       BCDString(SIZE(1)),
   day         BCDString(SIZE(1))
}
```

Присвояване на стойност:

yyyy	Година
mm	Месец
dd	Ден
‘00000000’H	Указва изрично липсата на дата.

2.58. **DateOfDayDownloaded**

Поколение 2:

датата и часът на изтеглянето на данни.

```
DateOfDayDownloaded ::= TimeReal
```

Присвояване на стойност: липса на допълнителна информация.

2.59. **DateOfDayDownloadedRecordArray**

Поколение 2:

Датата и часът на изтегляне плюс метаданните, използвани в протокола за изтегляне на данни.

```
DateofDayDownloadedRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       DateOfDayDownloaded
}
```

recordType указва типа на записа (DateOfDayDownloaded). **Присвояване на стойност**: вж. RecordType.

recordSize е размерът на CurrentDateTime в байтове.

noOfRecords е броят на записите в набора от записи.

records е наборът от дати и часове на записите за изтегляне на данни.

2.60. **Distance**

Изминатото разстояние (резултат от изчислението на разликата между две стойности на километражния брояч на превозното средство).

```
Distance ::= INTEGER(0..2^16-1)
```

Присвояване на стойност: двоична без знак. Стойност в km в работния диапазон от 0 до 9 999 km.

2.61. **DriverCardApplicationIdentification**

Информация, съхранена на карта на водач и отнасяща се до идентификация на приложението на картата (изисквания 253 и 278 от приложение 1B).

Поколение 1:

```
DriverCardApplicationIdentification ::= SEQUENCE {
   typeOfTachographCardId              EquipmentType,
   cardStructureVersion                CardStructureVersion,
   noOfEventsPerType                   NoOfEventsPerType,
   noOfFaultsPerType                   NoOfFaultsPerType,
   activityStructureLength             CardActivityLengthRange,
   noOfCardVehicleRecords              NoOfCardVehicleRecords,
   noOfCardPlaceRecords                NoOfCardPlaceRecords
}
```

typeOfTachographCardId обозначава използвания тип карта.

cardStructureVersion указва версията на структурата, приложена в картата.

noOfEventsPerType е броят на събитията от всеки тип, които картата може да запише.

noOfFaultsPerType е броят на неизправностите от всеки тип, които картата може да запише.

activityStructureLength указва броя на байтовете, които могат да се използват за съхранение на записите за дейността.

noOfCardVehicleRecords е броят на записите за превозното средство, които картата може да съдържа.

noOfCardPlaceRecords е броят на местоположенията, които картата може да запише.

Поколение 2:

```
DriverCardApplicationIdentification ::= SEQUENCE {
   typeOfTachographCardId              EquipmentType,
   cardStructureVersion                CardStructureVersion,
   noOfEventsPerType                   NoOfEventsPerType,
   noOfFaultsPerType                   NoOfFaultsPerType,
   activityStructureLength             CardActivityLengthRange,
   noOfCardVehicleRecords              NoOfCardVehicleRecords,
   noOfCardPlaceRecords                NoOfCardPlaceRecords,
   noOfGNSSCDRecords                   NoOfGNSSCDRecords,
   noOfSpecificConditionRecords        NoOfSpecificConditionRecords
}
```

В допълнение към поколение 1 се използват следните елементи от данни:

noOfGNSSCDRecords е броят на записите за непрекъснато управление по GNSS, които картата може да съхранява.

noOfSpecificConditionRecords е броят на записите за специфични условия, които картата може да съхранява.

2.62. DriverCardHolderIdentification

Информация, съхранена на карта на водач и отнасяща се за идентификация на титуляря на картата (изисквания 256 и 281 от приложение 1B).

```
DriverCardHolderIdentification ::= SEQUENCE {
   cardHolderName                      HolderName,
   cardHolderBirthDate                 Datef,
   cardHolderPreferredLanguage         Language
}
```

cardHolderName е фамилията и името (и презимето) на титуляря на картата на водач.

cardHolderBirthDate е рожденатa дата на титуляря на картата на водач.

cardHolderPreferredLanguage е предпочитаният език на титуляря на картата.

2.63. **DSRCSecurityData**

Поколение 2:

За ясната текстова информация и MAC, които трябва да се предадат по DSRC от тахографа на дистанционното запитващо устройство (RI), вж. допълнение 11, част Б, глава 13 за подробна информация.

```
DSRCSecurityData ::= SEQUENCE {
   tagLenthPlainText                    OCTET STRING(SIZE(2)),
   currentDateTime                      CurrentDateTime,
   counter                              INTEGER(0..2^24-1),
   vuSerialNumber                       VuSerialNumber,
   dSRCMKVersionNumber                  INTEGER(SIZE(1)),
   tagLengthMac                         OCTET STRING(SIZE(2)),
   mac                                  MAC
}
```

tagLength е част от кодирането DER-TLV и се фиксира на ‘81 10’ (допълнение 11, част Б, глава 13).

currentDateTime е актуалната дата и час на бордовото устройство.

counter изброява съобщенията RTM.

vuSerialNumber е серийният номер на бордовото устройство.

dSRCMKVersionNumber е номерът на версията на главния ключ DSRC, от който са получени специалните ключове DSRC на бордовото устройство.

tagLengthMac е тагът и дължината на обекта от данни MAC като част от кодирането DER-TLV. Тагът се фиксира на ‘8E’, а дължината кодира дължината на MAC в октети (вж. допълнение 11, част Б, глава 13).

mac е MAC, изчислен от съобщението RTM (вж. допълнение 11, част Б, глава 13).

2.64. **EGFCertificate**

Поколение 2:

Сертификат на публичния ключ на външното устройство за GNSS за общо удостоверяване с бордовото устройство. Структурата на този сертификат е посочена в допълнение 11.

```
EGFCertificate ::= Certificate
```

2.65. **EmbedderIcAssemblerId**

Дава информация за интегратора на ИС.

```
EmbedderIcAssemblerId ::= SEQUENCE{
   countryCode                          IA5String(SIZE(2)),
   moduleEmbedder                       BCDString(SIZE(2)),
   manufacturerInformation              OCTET STRING(SIZE(1))
}
```

countryCode е двубуквеният код на държавата на интегратора на модула съгласно ISO 3166.

moduleEmbedder указва интегратора на модула.

manufacturerInformation за вътрешна употреба на производителя.

2.66. EntryTypeDailyWorkPeriod

Код, позволяващ да се прави разлика между местоположението в началото и в края на един дневен период на работа и условията на въвеждане на тези данни.

Поколение 1

```
EntryTypeDailyWorkPeriod ::= INTEGER {
   Begin,  related time = card insertion time or time of entry          (0),
   End,    related time = card withdrawal time or time of entry        (1),
   Begin,  related time manually entered (start time)                  (2),
   End,    related time manually entered (end of work period)          (3),
   Begin,  related time assumed by VU                                  (4),
   End,    related time assumed by VU                                  (5)
}
```

Присвояване на стойност: съгласно стандарт ISO/IEC 8824-1.

Поколение 2

```
EntryTypeDailyWorkPeriod ::= INTEGER {
   Begin,  related time = card insertion time or time of entry          (0),
   End,    related time = card withdrawal time or time of entry        (1),
   Begin,  related time manually entered (start time)                  (2),
   End,    related time manually entered (end of work period)          (3),
   Begin,  related time assumed by VU                                  (4),
   End,    related time assumed by VU                                  (5),
   Begin,  related time based on GNSS data                             (6),
   End     related time based on GNSS data                             (7)
}
```

Присвояване на стойност: съгласно стандарт ISO/IEC 8824-1.

2.67. EquipmentType

Код, позволяващ да се прави разлика между различните типове оборудване, използвани за тахографското приложение.

```
EquipmentType ::= INTEGER(0..255)
```

Поколение 1:

```
--Reserved                          (0),
--Driver Card                       (1),
--Workshop Card                     (2),
--Control Card                      (3),
--Company Card                      (4),
--Manufacturing Card                (5),
--Vehicle Unit                      (6),
--Motion Sensor                     (7),
--RFU                               (8..255)
```

Присвояване на стойност: съгласно стандарт ISO/IEC 8824-1.

Стойността 0 е запазена за указване на определена държава членка или на Европа в полето CHA на сертификатите.

Поколение 2:

Използват се същите стойности, както при поколение 1, със следните допълнения:

```
--GNSS Facility                          (8),
--Remote Communication Module            (9),
--ITS interface module                   (10),
--Plaque                                 (11), -- may be used in SealRecord
--M1/N1 Adapter                          (12), -- may be used in SealRecord
--European Root CA (ERCA)                (13),
--Member State CA (MSCA)                 (14),
--External GNSS connection               (15), -- may be used in SealRecord
--Unused                                 (16), -- used in SealDataVu
--RFU                                    (17..255)
```

Забележка: стойностите от поколение 2 за пластината, адаптера и връзката с GNSS, както и стойностите за поколение 1 за бордовото устройство и датчика за движение могат да се използват в SealRecord, т.е. ако е приложимо.

2.68. **EuropeanPublicKey**

Поколение 1:

Европейски публичен ключ.

```
EuropeanPublicKey ::= PublicKey
```

2.69. **EventFaultRecordPurpose**

Код, указващ причината за записване на събитие или неизправност.

```
EventFaultRecordPurpose ::= OCTET STRING (SIZE(1))
```

Присвояване на стойност:

'00'H	едно от 10-те най-скорошни (или последни) събития или неизправности
'01'H	най-дългото събитие, настъпило по време на един от 10-те последни дена, в които са отбелязани събития
'02'H	
'03'H	едно от 5-те най-дълги събития, записани по време на 365-те последни дена
'04'H	последното събитие, настъпило по време на един от 10-те последни дена, в които са отбелязани събития
'05'H	
'06'H	най-сериозното събитие, записано по време на един от 10-те последни дена, в които са отбелязани събития
'07'H	
'08'H to '7F'H	едно от 5-те най-сериозни събития, записани по време на 365-те последни дена
'80'H to 'FF'H	първото събитие или неизправност, настъпила след последното калибриране
	активно/текущо събитие или неизправност
	RFU
	зависи от производителя

2.70. **EventFaultType**

Код, характеризиращ събитие или неизправност.

```
EventFaultType ::= OCTET STRING (SIZE(1))
```

Присвояване на стойност:

Поколение 1:

'0x'H	Общи събития,
'00'H	Няма допълнителна информация,
'01'H	Вкарване на невалидна карта,
'02'H	Конфликт, предизвикан от картата,
'03'H	Припокриване във времето,
'04'H	Управление без съответната карта,
'05'H	Вкарване на карта по време на управление,
'06'H	Неправилно приключена последна картова сесия,
'07'H	Превишаване на скоростта,
'08'H	Прекъсване на електрическото захранване,
'09'H	Грешка в данните за движението,
'0A'H	Конфликт относно движението на превозното средство,
'0B' to '0F'H	RFU,

	Опити за нарушаване на сигурността, свързани с бордовото устройство,
‘1x’H	Няма допълнителна информация,
‘10’H	Неуспешна процедурата по удостоверяване на датчика за движение,
‘11’H	Неуспешна процедурата по удостоверяване на тахографската карта,
‘12’H	Неразрешена смяна на датчика за движение,
‘13’H	Грешка във връзка с целостта на входящите данни на картата,
‘14’H	Грешка във връзка с целостта на съхранените данни на потребител,
‘15’H	Грешка при трансфер на вътрешни данни,
‘16’H	Неразрешено отваряне на корпус,
‘17’H	Възпрепятстване на работата на хардуера,
‘18’H	RFU,
‘19’H to ‘1F’H	
‘2x’H	Опити за нарушаване на сигурността, свързани с датчика за движение,
‘20’H	Няма допълнителна информация,
‘21’H	Неуспешно удостоверяване,
‘22’H	Грешка във връзка с целостта на съхранените данни,
‘23’H	Грешка при трансфер на вътрешни данни,
‘24’H	Неразрешено отваряне на корпус,
‘25’H	Възпрепятстване на работата на хардуера,
‘26’H to ‘2F’H	RFU,
‘3x’H	Неизправности във връзка с уреди за регистриране на данните за движението,
‘30’H	Няма допълнителна информация,
‘31’H	Вътрешна неизправност в бордовото устройство,
‘32’H	Неизправност на печатащото устройство,
‘33’H	Неизправност на екрана,
‘34’H	Неизправност при изтегляне на данни,
‘35’H	Неизправност на датчика,
‘36’H to ‘3F’H	RFU,
‘4x’H	Неизправности във връзка с карта,
‘40’H	Няма допълнителна информация,
‘41’H to ‘4F’H	RFU,
‘50’H to ‘7F’H	RFU,
‘80’H to ‘FF’H	Зависи от производителя.

Поколение 2:

Използват се същите стойности, както при поколение 1, със следните допълнения:

‘0B’H	Времеви конфликт (GNSS/вътрешния часовник на бордовото устройство),
‘0C’ to ‘0F’H	RFU,
‘5x’H	Неизправности, свързани с GNSS,
‘50’H	Няма допълнителна информация,
‘51’H	Неизправност на вътрешния приемник на сигнали от GNSS,
‘52’H	Неизправност на външния приемник на сигнали от GNSS,
‘53’H	Неизправност на външна връзка на GNSS,
‘54’H	Няма данни за местоположението от GNSS,
‘55’H	Установяване на вмешателство в GNSS,
‘56’H	Изтекъл сертификат на външно устройство за GNSS,
‘57’H to ‘5F’H	RFU,
‘6x’H	Неизправности, свързани с модула за връзка от разстояние,
‘60’H	Няма допълнителна информация,
‘61’H	Неизправност на модула за връзка от разстояние,
‘62’H	Неизправност във връзката на модула за връзка от разстояние,
‘63’H to ‘6F’H	RFU,
‘7x’H	Неизправности на интерфейса с ITS,
‘70’H	Няма допълнителна информация,
‘71’H to ‘7F’H	RFU.

2.71. **ExtendedSealIdentifier**

Поколение 2:

Разширеният идентификатор на пломбата уникално идентифицира пломбата (изискване 401 от приложение 1B).

```
ExtendedSealIdentifier ::= SEQUENCE{
   manufacturerCode                    OCTET STRING (SIZE(2)),
   sealIdentifier                      OCTET STRING (SIZE(6))
}
```

manufacturerCode е кодът на производителя на пломбата.

sealIdentifier е идентификатор за пломбата, който е уникален за производителя.

2.72. **ExtendedSerialNumber**

Индивидуална идентификация на оборудване. Този номер може също така да се използва за идентификатор на публичния ключ на оборудването.

Поколение 1:

```
ExtendedSerialNumber ::= SEQUENCE{
   serialNumber                        INTEGER(0..2^32-1),
   monthYear                           BCDString(SIZE(2)),
   type                                OCTET STRING(SIZE(1)),
   manufacturerCode                    ManufacturerCode
}
```

serialNumber е сериен номер на оборудване, уникален за производителя, типа на оборудването и месеца и годината по-долу.

monthYear е идентификация на месеца и годината на производството (или на присвояването на сериен номер).

Присвояване на стойност: кодиране BCD на месеца (две цифри) и годината (последните две цифри).

type е идентификатор на типа оборудване.

Присвояване на стойност: зависи от производителя, като стойността ‘FFh’ е запазена.

manufacturerCode: е цифровият код за идентификация на производителя на оборудването от одобрен тип.

Поколение 2:

```
ExtendedSerialNumber ::= SEQUENCE{
   serialNumber                        INTEGER(0..2^32-1),
   monthYear                           BCDString(SIZE(2)),
   type                                EquipmentType,
   manufacturerCode                    ManufacturerCode
}
```

serialNumber вж. поколение 1.

monthYear вж. поколение 1.

type указва типа оборудване.

manufacturerCode: вж. поколение 1.

2.73. **FullCardNumber**

Код, който изцяло идентифицира тахографска карта.

```
FullCardNumber ::= SEQUENCE {
   cardType                              EquipmentType,
   cardIssuingMemberState                NationNumeric,
   cardNumber                            CardNumber
}
```

cardType е типът тахографска карта.

cardIssuingMemberState е кодът на държавата членка, която е издала картата.

cardNumber е номерът на картата.

2.74. **FullCardNumberAndGeneration**

Поколение 2:

Код, който изцяло идентифицира тахографска карта и поколението ѝ.

```
FullCardNumberAndGeneration ::= SEQUENCE {
   fullCardNumber                        FullCardNumber,
   generation                            Generation
}
```

fullcardNumber идентифицира тахографската карта.

generation указва поколението на използваната тахографска карта.

2.75. **Generation**

Поколение 2:

Указва поколението на използвания тахограф.

```
Generation ::= INTEGER(0..255)
```

Присвояване на стойност:

‘00’H	RFU
‘01’H	Поколение 1
‘02’H	Поколение 2
‘03’H .. ‘FF’H	RFU

2.76. **GeoCoordinates**

Поколение 2:

Геокординатите се кодират като цели числа. Те са кратни числа на кодирането ±DDMM.M за ширината и на ±DDDMM.M за дължината. В случая ±DD, съответно ±DDD, указва градусите, а MM.M — минутите.

```
GeoCoordinates ::= SEQUENCE {
   latitude                              INTEGER(-90000..90001),
   longitude                             INTEGER(-180000..180001)
}
```

latitude се кодира като кратно число (коефициент 10) на представянето ±DDMM.M.

longitude се кодира като кратно число (коефициент 10) на представянето ±DDDMM.M.

2.77. **GNSSAccuracy**

Поколение 2:

Точността на данните за местоположението по GNSS (вж. определение ддд). Тази точност се кодира като цяло число и е кратно число (коефициент 10) на стойността X.Y, подадена от изречението GSA NMEA.

```
GNSSAccuracy ::= INTEGER(1..100)
```

2.78. **GNSSContinuousDriving**

Поколение 2:

Информация, съхранена на карта на водач или карта за монтаж и настройки и отнасяща се до местоположението по GNSS на превозното средство, ако времето за непрекъснато управление на водача достигне кратно число на три часа (изисквания 306 и 354 от приложение 1B).

```
GNSSContinuousDriving := SEQUENCE {
   gnssCDPointerNewestRecord            INTEGER(0..NoOfGNSSCDRecords -1),
   gnssContinuousDrivingRecords         SET SIZE(NoOfGNSSCDRecords) OF
                                        GNSSContinuousDrivingRecord
}
```

gnssCDPointerNewestRecord е индексът на последния актуализиран запис за непрекъснато управление по GNSS.

Присвояване на стойност: число, съответстващо на номератора на записа за непрекъснато управление по GNSS, като се започва с 0 за първия случай на запис за непрекъснато управление по GNSS в структурата.

gnssContinuousDrivingRecords е набор от записи, съдържащ датата и часа, когато непрекъснатото управление достигне кратно число на три часа, и информация за местоположението на превозното средство.

2.79. **GNSSContinuousDrivingRecord**

Поколение 2:

Информация, съхранена на карта на водач или карта за монтаж и настройки и отнасяща се до местоположението по GNSS на превозното средство, ако времето за непрекъснато управление на водача достигне кратно число на три часа (изисквания 305 и 353 от приложение 1B).

```
GNSSContinuousDrivingRecord ::= SEQUENCE {
   timeStamp                            TimeReal,
   gnssPlaceRecord                      GNSSPlaceRecord
}
```

timeStamp е датата и часът, когато времето за непрекъснато управление на титуляря на картата достигне кратно число на три часа.

gnssPlaceRecord съдържа информация за местоположението на превозното средство.

2.80. **GNSSPlaceRecord**

Поколение 2:

Информация във връзка с местоположението по GNSS на превозното средство (изисквания 108, 109, 110, 296, 305, 347 и 353 от приложение 1B).

```
GNSSPlaceRecord ::= SEQUENCE {
   timeStamp                            TimeReal,
   gnssAccuracy                         GNSSAccuracy,
   geoCoordinates                       GeoCoordinates
}
```

timeStamp е датата и часът, когато е било определено местоположението по GNSS на превозното средство.

gnssAccuracy е точността на данните за местоположението по GNSS.

geoCoordinates е записаното местоположение, като се използва GNSS.

2.81. **HighResOdometer**

Стойността от километражния брояч на превозното средство: общо разстояние, изминато от превозното средство по време на експлоатацията му.

```
HighResOdometer ::= INTEGER(0..2^32-1)
```

Присвояване на стойност: двоична без знак. Стойност в 1/200 km в работния диапазон от 0 до 21 055 406 km.

2.82. **HighResTripDistance**

Разстояние, изминато по време на цяло пътуване или част от него.

```
HighResTripDistance ::= INTEGER(0..2^32-1)
```

Присвояване на стойност: двоична без знак. Стойност в 1/200 km в работния диапазон от 0 до 21 055 406 km.

2.83. **HolderName**

Фамилия и име (и презиме) на титуляря на карта.

```
HolderName ::= SEQUENCE {
   holderSurname                    Name,
   holderFirstNames                 Name
}
```

holderSurname е фамилията на титуляря, като не се посочва господин, госпожа или госпожица.

Присвояване на стойност: ако картата не е лична, holderSurname съдържа същите данни, като companyName, workshopName или controlBodyName.

holderFirstNames е името (и презимето) и инициалите на титуляря.

2.84. **InternalGNSSReceiver**

Поколение 2:

Информация дали приемникът на сигнали от GNSS е вътрешен или външен за бордовото устройство. Вярно означава, че приемникът на сигнали от GNSS е вътрешен за бордовото устройство. Невярно означава, че приемникът на сигнали от GNSS е външен.

```
InternalGNSSReceiver ::= BOOLEAN
```

2.85. **K-ConstantOfRecordingEquipment**

Константа на уреда за регистриране на данните за движението (определение м).

```
K-ConstantOfRecordingEquipment ::= INTEGER(0..2^16-1)
```

Присвояване на стойност: импулси на километър в работния диапазон от 0 до 64 255 имп./km.

2.86. **KeyIdentifier**

Уникален идентификатор на публичен ключ, използван за посочване и избор на ключа. Този идентификатор идентифицира също така титуляря на ключа.

```
KeyIdentifier ::= CHOICE {
   extendedSerialNumber                ExtendedSerialNumber,
   certificateRequestID                CertificateRequestID,
   certificationAuthorityKID           CertificationAuthorityKID
}
```

Първият избор е подходящ за указване на публичния ключ на бордово устройство или тахографска карта.

Вторият избор е подходящ за указване на публичния ключ на бордово устройство (в случай че серийният номер на бордовото устройство е неизвестен към момента на генериране на сертификата).

Третият избор е подходящ за указване на публичния ключ на държава членка.

2.87. **KMWCKey**

Поколение 2:

Ключ AES и съответната му версия на ключа за сдвояването на бордово устройство — датчик за движение. За подробни данни вж. допълнение 11.

```
KMWCKey ::= SEQUENCE {
   kMWCKey                             AESKey,
   keyVersion                          INTEGER (SIZE(1))
}
```

kMWCKey е дължината на ключа AES, съединен с ключа, използван за сдвояването бордово устройство — датчик за движение.

keyVersion указва версията на ключа AES.

2.88. **Language**

Код, идентифициращ език.

```
Language ::= IA5String(SIZE(2))
```

Присвояване на стойност: код, съставен от две малки букви съгласно стандарт ISO 639.

2.89. **LastCardDownload**

Дата и час, съхранени на карта на водач, на последното изтегляне на данните от картата (за цели, различни от извършването на проверка). Изисквания 257 и 282 от приложение 1B. Тази дата може да се актуализира от бордово устройство или всеки четец на карта.

```
LastCardDownload ::= TimeReal
```

Присвояване на стойност: липса на допълнителна информация.

2.90. **LinkCertificate**

Поколение 2:

Сертификатът за връзка между двойките ключове на основния европейски сертификационен орган.

```
LinkCertificate ::= Certificate
```

2.91. **L-TyreCircumference**

Действителна обиколка на колелата (определение ф).

```
L-TyreCircumference ::= INTEGER(0.. 2^16-1)
```

Присвояване на стойност: двоична без знак, стойност в 1/8 mm и в работния диапазон от 0 до 8 031 mm.

2.92. **MAC**

Поколение 2:

Сума за криптографски контрол с дължина от 8, 12 или 16 байта, съответстваща на криптографските поредици, посочени в допълнение 11.

```
MAC ::= CHOICE {
   mac8                                 OCTET STRING (SIZE(8)),
   mac12                                OCTET STRING (SIZE(12)),
   mac16                                OCTET STRING (SIZE(12))
}
```

2.93. **ManualInputFlag**

Код, позволяващ да се разбере дали титулярят на картата ръчно е въвел дейностите на водача при вкарване на картата (изискване 081 от приложение 1Б и изискване 102 от приложение 1В).

```
ManualInputFlag ::= INTEGER {
   noEntry                              (0)
   manualEntries                        (1)
}
```

Присвояване на стойност: липса на допълнителна информация.

2.94. **ManufacturerCode**

Код за идентификация на производителя на оборудване от одобрен тип.

```
ManufacturerCode ::= INTEGER(0..255)
```

Лабораторията, компетентна за изпитванията за оперативна съвместимост, поддържа и публикува на своя уебсайт списъка с кодове на производителите (изискване 454 от приложение 1В).

Разработчиците на тахографско оборудване получават временно ManufacturerCodes след подадена заявка до лабораторията, компетентна за изпитванията за оперативна съвместимост.

2.95. **ManufacturerSpecificEventFaultData**

Поколение 2:

Кодовете за грешка, специфични за производителя, опростяват анализа на грешките и поддържането на бордовите устройства.

```
ManufacturerSpecificEventFaultData ::= SEQUENCE {
   manufacturerCode                     ManufacturerCode,
   manufacturerSpecificErrorCode        OCTET STRING(SIZE(3))
}
```

manufacturerCode идентифицира производителя на бордовото устройство.

manufacturerSpecificErrorCode е код за грешка, специфичен за производителя.

2.96. **MemberStateCertificate**

Сертификат на публичния ключ на държава членка, издаден от европейския сертификационен орган.

```
MemberStateCertificate ::= Certificate
```

2.97. **MemberStateCertificateRecordArray**

Поколение 2:

Сертификатът на държавата членка плюс метаданните, използвани в протокола за изтегляне на данни.

```
MemberStateCertificateRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       MemberStateCertificate
}
```

recordType указва типа на записа (MemberStateCertificate). **Присвояване на стойност**: вж. RecordType.

recordSize е размерът на MemberStateCertificate в байтове.

noOfRecords е броят на записите в набора от записи. Стойността се определя на 1, тъй като сертификатите могат да имат различна дължина.

records е наборът от сертификати на държава членка.

2.98. **MemberStatePublicKey**

Поколение 1:

Публичен ключ на държава членка.

```
MemberStatePublicKey ::= PublicKey
```

2.99. **Name**

Име.

```
Name ::= SEQUENCE {
   codePage                            INTEGER (0..255),
   name                                OCTET STRING (SIZE(35))
}
```

codePage указва набор от символи, определен в глава 4.

name е име, кодирано, като е използван указаният набор от символи.

2.100. **NationAlpha**

Буквеният код за указване на държавата трябва да бъде в съответствие с отличителните знаци, използвани върху превозни средства при международен трафик (съгласно Виенската конвенция на ООН от 1968 г. за движението по пътищата).

```
NationAlpha ::= IA5String(SIZE(3))
```

Буквените и цифровите кодове за държави трябва да се съдържат в списък, поддържан на уебсайта на лабораторията, определена да извършва изпитванията за оперативна съвместимост, както е посочено в изискване 440 от приложение 1B.

2.101. **NationNumeric**

Цифров код за указване на държавата.

```
NationNumeric ::= INTEGER(0 .. 255)
```

Присвояване на стойност: вж. данните тип 2.100 (NationAlpha).

Изменението или актуализирането на спецификацията NationAlpha или NationNumeric, описана в параграфа по-горе, трябва да се извършва само след като определената лаборатория получи становищата на производителите на бордови устройства на цифрови и интелигентни тахографи от одобрен тип.

2.102. **NoOfCalibrationRecords**

Брой на записите на калибрированията, които картата за монтаж и настройки може да съхранява.

Поколение 1:

```
NoOfCalibrationRecords ::= INTEGER(0..255)
```

Присвояване на стойност: вж. допълнение 2.

Поколение 2:

```
NoOfCalibrationRecords ::= INTEGER(0..2^16-1)
```

Присвояване на стойност: вж. допълнение 2.

2.103. **NoOfCalibrationsSinceDownload**

Брояч, указващ броя на калибрированията, извършени с една карта за монтаж и настройки от последното изтегляне на данни от нея (изисквания 317 и 340 от приложение 1B).

```
NoOfCalibrationsSinceDownload ::= INTEGER(0..2^16-1)
```

Присвояване на стойност: липса на допълнителна информация.

2.104. **NoOfCardPlaceRecords**

Брой на записите на местоположенията, които картата на водач или картата за монтаж и настройки може да съхранява.

Поколение 1:

```
NoOfCardPlaceRecords ::= INTEGER(0..255)
```

Присвояване на стойност: вж. допълнение 2.

Поколение 2:

```
NoOfCardPlaceRecords ::= INTEGER(0..2^16-1)
```

Присвояване на стойност: вж. допълнение 2.

2.105. **NoOfCardVehicleRecords**

Брой на записите на използваните превозни средства, които картата на водач или картата за монтаж и настройки може да съхранява.

```
NoOfCardVehicleRecords ::= INTEGER(0.. 2^16-1)
```

Присвояване на стойност: вж. допълнение 2.

2.106. **NoOfCardVehicleUnitRecords**

Поколение 2:

Брой на записите на използваните бордови устройства, които картата на водач или картата за монтаж и настройки може да съхранява.

```
NoOfCardVehicleUnitRecords ::= INTEGER(0.. 2^16-1)
```

Присвояване на стойност: вж. допълнение 2.

2.107. **NoOfCompanyActivityRecords**

Брой на записите на дейностите на превозвача, които картата на превозвач може да съхранява.

```
NoOfCompanyActivityRecords ::= INTEGER(0.. 2^16-1)
```

Присвояване на стойност: вж. допълнение 2.

2.108. **NoOfControlActivityRecords**

Брой на записите за контролната дейност, които контролната карта може да съхранява.

```
NoOfControlActivityRecords ::= INTEGER(0.. 2^16-1)
```

Присвояване на стойност: вж. допълнение 2.

2.109. **NoOfEventsPerType**

Брой на събитията от всеки тип, които картата може да съхранява.

```
NoOfEventsPerType ::= INTEGER(0..255)
```

Присвояване на стойност: вж. допълнение 2.

2.110. **NoOfFaultsPerType**

Брой на неизправностите от всеки тип, които картата може да съхранява.

```
NoOfFaultsPerType ::= INTEGER(0..255)
```

Присвояване на стойност: вж. допълнение 2.

2.111. **NoOfGNSSCDRecords**

Поколение 2:

Брой на записите за непрекъснато управление по GNSS, които картата може да съхранява.

```
NoOfGNSSCDRecords ::= INTEGER(0..2^16-1)
```

Присвояване на стойност: вж. допълнение 2.

2.112. **NoOfSpecificConditionRecords**

Поколение 2:

Брой на записите за специфични условия, които картата може да съхранява.

```
NoOfSpecificConditionRecords ::= INTEGER(0..2^16-1)
```

Присвояване на стойност: вж. допълнение 2.

2.113. **OdometerShort**

Стойност от километражния брояч на превозното средство в съкратена форма.

```
OdometerShort ::= INTEGER(0..2^24-1)
```

Присвояване на стойност: двоична без знак. Стойност в km в работния диапазон от 0 до 9 999 999 km.

2.114. **OdometerValueMidnight**

Стойността от километражния брояч в полунощ от определено денонощие (изискване 090 от приложение 1Б и изискване 113 от приложение 1В).

```
OdometerValueMidnight ::= OdometerShort
```

Присвояване на стойност: липса на допълнителна информация.

2.115. **OdometerValueMidnightRecordArray**

Поколение 2:

OdometerValueMidnight плюс метаданните, използвани в протокола за изтегляне на данни.

```
OdometerValueMidnightRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       OdometerValueMidnight
}
```

recordType указва типа на записа (OdometerValueMidnight). **Присвояване на стойност**: вж. RecordType.

recordSize е размерът на OdometerValueMidnight в байтове.

noOfRecords е броят на записите в набора от записи.

records е наборът от записи на OdometerValueMidnight.

2.116. **OverspeedNumber**

Брой на събитията „превишаване на скоростта“ след последната проверка за превишаването на скоростта.

```
OverspeedNumber ::= INTEGER(0..255)
```

Присвояване на стойност: 0 означава, че никакво събитие „превишаване на скоростта“ не е настъпило след последната проверка за превишаването на скоростта, 1 означава, че едно събитие от този тип е настъпило след последната проверка за превишаването на скоростта … 255 означава, че броят на събитията „превишаване на скоростта“, настъпили след последната проверка за превишаването на скоростта, е равен на 255 или надвишава тази стойност.

2.117. **PlaceRecord**

Информация относно местоположението в началото или в края на един дневен период на работа (изисквания 108, 271, 296, 324 и 347 от приложение 1В).

Поколение 1:

```
PlaceRecord ::= SEQUENCE {
   entryTime                          TimeReal,
   entryTypeDailyWorkPeriod           EntryTypeDailyWorkPeriod,
   dailyWorkPeriodCountry             NationNumeric,
   dailyWorkPeriodRegion              RegionNumeric,
   vehicleOdometerValue               OdometerShort
}
```

entryTime е датата и часът във връзка с въведените данни.

entryTypeDailyWorkPeriod е типът въведени данни.

dailyWorkPeriodCountry е въведената държава.

dailyWorkPeriodRegion е въведеният регион.

vehicleOdometerValue е стойността от километражния брояч в часа на въвеждане на местоположението.

Поколение 2:

```
PlaceRecord ::= SEQUENCE {
   entryTime                          TimeReal,
   entryTypeDailyWorkPeriod           EntryTypeDailyWorkPeriod,
   dailyWorkPeriodCountry             NationNumeric,
   dailyWorkPeriodRegion              RegionNumeric,
   vehicleOdometerValue               OdometerShort,
   entryGNSSPlaceRecord               GNSSPlaceRecord
}
```

В допълнение към поколение 1 се използва следният компонент:

entryGNSSPlaceRecord е записаното местоположение и час.

2.118. **PreviousVehicleInfo**

Информация за превозното средство, използвано преди това от определен водач по време на вкарване на неговата карта в бордово устройство (изискване 081 от приложение 1Б и изискване 102 от приложение 1В).

Поколение 1:

```
PreviousVehicleInfo ::= SEQUENCE {
   vehicleRegistrationIdentification      VehicleRegistrationIdentification,
   cardWithdrawalTime                     TimeReal
}
```

vehicleRegistrationIdentification посочва VRN и държавата членка, регистрираща превозното средство.

cardWithdrawalTime е датата и часът на изваждане на картата.

Поколение 2:

```
PreviousVehicleInfo ::= SEQUENCE {
   vehicleRegistrationIdentification      VehicleRegistrationIdentification,
   cardWithdrawalTime                     TimeReal,
   vuGeneration                           Generation
}
```

В допълнение към поколение 1 се използва следният елемент от данни:

vuGeneration идентифицира поколението на бордовото устройство.

2.119. **PublicKey**

Поколение 1:

Публичен ключ RSA.

```
PublicKey ::= SEQUENCE {
   rsaKeyModulus                    RSAKeyModulus,
   rsaKeyPublicExponent             RSAKeyPublicExponent
}
```

rsaKeyModulus е модулът на двойката ключове.

rsaKeyPublicExponent е публичният степенен показател на двойката ключове.

2.120. **RecordType**

Поколение 2:

Посочване на типа запис. Този тип данни се използва в RecordArrays.

```
RecordType ::= OCTET STRING(SIZE(1))
```

Присвояване на стойност:

'01'H	ActivityChangeInfo,
'02'H	CardSlotsStatus,
'03'H	CurrentDateTime,
'04'H	MemberStateCertificate,
'05'H	OdometerValueMidnight,
'06'H	DateOfDayDownloaded,
'07'H	SensorPaired,
'08'H	Signature,
'09'H	SpecificConditionRecord,
'0A'H	VehicleIdentificationNumber,
'0B'H	VehicleRegistrationNumber,
'0C'H	VuCalibrationRecord,
'0D'H	VuCardIWRecord,
'0E'H	VuCardRecord,
'0F'H	VuCertificate,
'10'H	VuCompanyLocksRecord,
'11'H	VuControlActivityRecord,
'12'H	VuDetailedSpeedBlock,
'13'H	VuDownloadablePeriod,
'14'H	VuDownloadActivityData,
'15'H	VuEventRecord,
'16'H	VuGNSSCDRecord,
'17'H	VuITSConsentRecord,
'18'H	VuFaultRecord,
'19'H	VuIdentification,
'1A'H	VuOverSpeedingControlData,
'1B'H	VuOverSpeedingEventRecord,
'1C'H	VuPlaceDailyWorkPeriodRecord,
'1D'H	VuTimeAdjustmentGNSSRecord,
'1E'H	VuTimeAdjustmentRecord,
'1F'H	VuPowerSupplyInterruptionRecord,
'20'H	SensorPairedRecord,
'21'H	SensorExternalGNSSCoupledRecord,
'22'H to '7F'H	RFU,
'80'H to 'FF'H	Зависи от производителя.

2.121. **RegionAlpha**

Буквено означение на регион в определена държава.

```
RegionAlpha ::= IA5STRING(SIZE(3))
```

Поколение 1:

Присвояване на стойност:

```
‘   ’         No information available,
Spain:
‘AN ’         Andalucía,
‘AR ’         Aragón,
‘AST’         Asturias,
‘C  ’         Cantabria,
‘CAT’         Cataluña,
‘CL ’         Castilla-León,
‘CM ’         Castilla-La-Mancha,
‘CV’          Valencia,
‘EXT’         Extremadura,
‘G  ’         Galicia,
‘IB ’         Baleares,
‘IC ’         Canarias,
‘LR ’         La Rioja,
‘M  ’         Madrid,
‘MU ’         Murcia,
‘NA ’         Navarra,
‘PV ’         País Vasco
```

Поколение 2:

Кодовете за RegionAlpha трябва да се съдържат в списък, поддържан на уебсайта на лабораторията, определена да извършва изпитванията за оперативна съвместимост.

2.122. **RegionNumeric**

Цифрово означение на регион в определена държава.

```
RegionNumeric ::= OCTET STRING (SIZE(1))
```

Поколение 1:

Присвояване на стойност:

```
‘00’H         No information available,
Spain:
‘01’H         Andalucía,
‘02’H         Aragón,
‘03’H         Asturias,
‘04’H         Cantabria,
‘05’H         Cataluña,
‘06’H         Castilla-León,
‘07’H         Castilla-La-Mancha,
‘08’H         Valencia,
‘09’H         Extremadura,
‘0A’H         Galicia,
‘0B’H         Baleares,
‘0C’H         Canarias,
‘0D’H         La Rioja,
‘0E’H         Madrid,
‘0F’H         Murcia,
‘10’H         Navarra,
‘11’H         País Vasco
```

Поколение 2:

Кодовете за RegionNumeric трябва да се съдържат в списък, поддържан на уебсайта на лабораторията, определена да извършва изпитванията за оперативна съвместимост.

2.123. **RemoteCommunicationModuleSerialNumber**

Поколение 2:

Сериен номер на модула за връзка от разстояние.

```
RemoteCommunicationModuleSerialNumber ::= ExtendedSerialNumber
```

2.124. **RSAKeyModulus**

Поколение 1:

Модули на двойка ключове RSA.

```
RSAKeyModulus ::= OCTET STRING (SIZE(128))
```

Присвояване на стойност: не е указана.

2.125. **RSAKeyPrivateExponent**

Поколение 1:

Частен степенен показател на двойка ключове RSA.

```
RSAKeyPrivateExponent ::= OCTET STRING (SIZE(128))
```

Присвояване на стойност: не е указана.

2.126. **RSAKeyPublicExponent**

Поколение 1:

Публичен степенен показател на двойка ключове RSA.

```
RSAKeyPublicExponent ::= OCTET STRING (SIZE(8))
```

Присвояване на стойност: не е указана.

2.127. **RtmData**

Поколение 2:

за определението на този тип данни вж. допълнение 14.

2.128. **SealDataCard**

Поколение 2:

Този тип данни съхранява информация за пломбите, поставени върху различни компоненти на превозното средство, и е предназначен за съхранение върху карта. Този тип данни е свързан с изискване 337 от приложение 1B.

```
SealDataCard ::= SEQUENCE {
   noOfSealRecords                        INTEGER(1..5),
   sealRecords                            SET SIZE(noOfSealRecords) OF SealRecord
}
```

noOfSealRecords е броят записи в sealRecords.

sealRecords е набор от записи за пломбите.

2.129. **SealDataVu**

Поколение 2:

Този тип данни съхранява информация за пломбите, поставени върху различни компоненти на превозното средство, и е предназначен за съхранение в бордово устройство.

```
SealDataVu ::= SEQUENCE SIZE(5) OF {
   sealRecords                            SealRecord
}
```

sealRecords е набор от записи за пломбите. Ако има по-малко от 5 налични пломби, стойността на EquipmentType във всички неизползвани sealRecords се фиксира на 16, т.е. неизползвани.

2.130. **SealRecord**

Поколение 2:

Този тип данни съхранява информация за пломба, вкарана върху компонент. Този тип данни е свързан с изискване 337 от приложение 1B.

```
SealRecord ::= SEQUENCE {
   equipmentType                          EquipmentType,
   extendedSealIdentifier                 ExtendedSealIdentifier
}
```

equipmentType идентифицира типа оборудване, върху което е вкарана пломбата.

extendedSealIdentifier е идентификатор на пломбата, вкарана върху оборудването.

2.131. **SensorApprovalNumber**

Номер на одобрение на типа датчик.

Поколение 1:

```
SensorApprovalNumber ::= IA5String(SIZE(8))
```

Присвояване на стойност: не е указана.

Поколение 2:

```
SensorApprovalNumber ::= IA5String(SIZE(16))
```

Присвояване на стойност:

Номерът на одобрение е този, който е публикуван на съответната интернет страница на Европейската комисия, т.е. например, като се включват тиренца, ако има. Номерът на одобрение се подравнява отляво.

2.132. **SensorExternalGNSSApprovalNumber**

Поколение 2:

Номер на одобрение на типа външно устройство за GNSS.

```
SensorExternalGNSSApprovalNumber ::= IA5String(SIZE(16))
```

Присвояване на стойност:

Номерът на одобрение е този, който е публикуван на съответната интернет страница на Европейската комисия, т.е. например, като се включват тиренца, ако има. Номерът на одобрение се подравнява отляво.

2.133. **SensorExternalGNSSCoupledRecord**

Поколение 2:

Информация, съхранена в бордовото устройство и отнасяща се до идентификация на външното устройство за GNSS, свързано с бордовото устройство (изискване 100 от приложение 1B).

```
SensorExternalGNSSCoupledRecord ::= SEQUENCE {
   sensorSerialNumber                  SensorGNSSSerialNumber,
   sensorApprovalNumber                SensorExternalGNSSApprovalNumber,
   sensorCouplingDate                  SensorGNSSCouplingDate
}
```

sensorSerialNumber е серийният номер на външното устройство за GNSS, свързано с бордовото устройство.

sensorApprovalNumber е номерът на одобрение на това външно устройство за GNSS.

sensorCouplingDate е дата на свързване на това външно устройство за GNSS с бордовото устройство.

2.134. **SensorExternalGNSSIdentification**

Поколение 2:

Информация, свързана с идентификацията на външното устройство за GNSS (изискване 98 от приложение 1B).

```
SensorExternalGNSSIdentification ::= SEQUENCE {
   sensorSerialNumber                  SensorGNSSSerialNumber,
   sensorApprovalNumber                SensorExternalGNSSApprovalNumber,
   sensorSCIdentifier                  SensorExternalGNSSSCIdentifier,
   sensorOSIdentifier                  SensorExternalGNSSOSIdentifier
}
```

sensorSerialNumber е разширеният сериен номер на външното устройство за GNSS.

sensorApprovalNumber е номерът на одобрение на външното устройство за GNSS.

sensorSCIdentifier е идентификаторът на компонента за сигурност на външното устройство за GNSS.

sensorOSIdentifier е идентификаторът на операционната система на външното устройство за GNSS.

2.135. **SensorExternalGNSSInstallation**

Поколение 2:

Информация, съхранена на външно устройство за GNSS и свързана с монтирането на външния датчик за GNSS (изискване 123 от приложение 1B).

```
SensorExternalGNSSInstallation ::= SEQUENCE {
   sensorCouplingDateFirst              SensorGNSSCouplingDate,
   firstVuApprovalNumber                VuApprovalNumber,
   firstVuSerialNumber                  VuSerialNumber,
   sensorCouplingDateCurrent            SensorGNSSCouplingDate,
   currentVuApprovalNumber              VuApprovalNumber,
   currentVUSerialNumber                VuSerialNumber
}
```

sensorCouplingDateFirst е датата на първото свързване на външно устройство за GNSS с бордово устройство.

firstVuApprovalNumber е номерът на одобрение на първото бордово устройство, свързано с външното устройство за GNSS.

firstVuSerialNumber е серийният номер на първото бордово устройство, свързано с външното устройство за GNSS.

sensorCouplingDateCurrent е датата на свързване към съответния момент на външно устройство за GNSS с бордово устройство.

currentVuApprovalNumber е номерът на одобрение на бордовото устройство, свързано към съответния момент с външното устройство за GNSS.

currentVUSerialNumber е серийният номер на бордовото устройство, свързано към съответния момент с външното устройство за GNSS.

2.136. **SensorExternalGNSSOSIdentifier**

Поколение 2:

Идентификатор на операционната система на външното устройство за GNSS.

```
SensorOSIdentifier ::= IA5String(SIZE(2))
```

Присвояване на стойност: зависи от производителя.

2.137. **SensorExternalGNSSSCIdentifier**

Поколение 2:

Този тип се използва например за идентификация на криптографския модул на външното устройство за GNSS.

Идентификатор на компонента за сигурност на външното устройство за GNSS.

```
SensorExternalGNSSSCIdentifier ::= IA5String(SIZE(8))
```

Присвояване на стойност: зависи от производителя на компонента.

2.138. **SensorGNSSCouplingDate**

Поколение 2:

Дата на свързване на външното устройство за GNSS с бордово устройство.

```
SensorGNSSCouplingDate ::= TimeReal
```

Присвояване на стойност: не е указана.

2.139. **SensorGNSSSerialNumber**

Поколение 2:

Този тип се използва за съхранение на серийния номер на приемника на сигнали от GNSS, когато е във и извън бордовото устройство.

Сериен номер на приемника на сигнали от GNSS.

```
SensorGNSSSerialNumber ::= ExtendedSerialNumber
```

2.140. **SensorIdentification**

Информация, съхранена на датчик за движение и отнасяща се до идентификация на датчика за движение (изискване 077 от приложение 1Б и изискване 95 от приложение 1В).

```
SensorIdentification ::= SEQUENCE {
   sensorSerialNumber                  SensorSerialNumber,
   sensorApprovalNumber                SensorApprovalNumber,
   sensorSCIdentifier                  SensorSCIdentifier,
   sensorOSIdentifier                  SensorOSIdentifier
}
```

sensorSerialNumber е разширеният сериен номер на датчика за движение (включително номер на частта и код на производителя).

sensorApprovalNumber е номерът на одобрение на датчика за движение.

sensorSCIdentifier е идентификаторът на компонента за сигурност на датчика за движение.

sensorOSIdentifier е идентификаторът на операционната система на датчика за движение.

2.141. **SensorInstallation**

Информация, съхранена на датчик за движение и отнасяща се до монтирането на датчика за движение (изискване 099 от приложение 1Б и изискване 122 от приложение 1В).

```
SensorInstallation ::= SEQUENCE {
   sensorPairingDateFirst              SensorPairingDate,
   firstVuApprovalNumber               VuApprovalNumber,
   firstVuSerialNumber                 VuSerialNumber,
   sensorPairingDateCurrent            SensorPairingDate,
   currentVuApprovalNumber             VuApprovalNumber,
   currentVUSerialNumber               VuSerialNumber
}
```

sensorPairingDateFirst е датата на първото сдвояване на датчика за движение с бордово устройство.

firstVuApprovalNumber е номерът на одобрение на първото бордово устройство, свързано с датчика за движение.

firstVuSerialNumber е серийният номер на първото бордово устройство, свързано с датчика за движение.

sensorPairingDateCurrent е датата на сдвояване към съответния момент на датчика за движение с бордовото устройство.

currentVuApprovalNumber е номерът на одобрение на бордовото устройство, свързано към съответния момент с датчика за движение.

currentVUSerialNumber е серийният номер на бордовото устройство, свързано към съответния момент с датчика за движение.

2.142. **SensorInstallationSecData**

Информация, съхранена на карта за монтаж и настройки и отнасяща се за данните относно сигурността, необходими за сдвояване на датчиците за движение с бордовите устройства (изисквания 308 и 331 от приложение 1В).

Поколение 1:

```
SensorInstallationSecData ::= TdesSessionKey
```

Присвояване на стойност: съгласно стандарт ISO 16844-3.

Поколение 2:

Както е описано в допълнение 11, картата за монтаж и настройки съхранява до три ключа за сдвояването на датчик за движение с бордово устройство. Тези ключове трябва да имат различни версии на ключовете.

```
SensorInstallationSecData ::= SEQUENCE {
   kMWCKey1                              KMWCKey,
   kMWCKey2                              KMWCKey OPTIONAL,
   kMWCKey3                              KMWCKey OPTIONAL
}
```

2.143. **SensorOSIdentifier**

Идентификатор на операционната система на датчика за движение.

```
SensorOSIdentifier ::= IA5String(SIZE(2))
```

Присвояване на стойност: зависи от производителя.

2.144. **SensorPaired**

Поколение 1:

Информация, съхранена в бордово устройство и отнасяща се за идентификация на датчика за движение, свързан с бордовото устройство (изискване 079 от приложение 1Б).

```
SensorPaired ::= SEQUENCE {
   sensorSerialNumber                    SensorSerialNumber,
   sensorApprovalNumber                  SensorApprovalNumber,
   sensorPairingDateFirst                SensorPairingDate
}
```

sensorSerialNumber е серийният номер на датчика за движение, свързан към съответния момент с бордовото устройство.

sensorApprovalNumber е номерът на одобрение на датчика за движение, свързан към съответния момент с бордовото устройство.

sensorPairingDateFirst е датата на първото сдвояване с бордово устройство на датчика за движение, свързан към съответния момент с бордовото устройство.

2.145. **SensorPairedRecord**

Поколение 2:

Информация, съхранена в бордово устройство и отнасяща се за идентификация на датчик за движение, свързан с бордовото устройство (изискване 97 от приложение 1B).

```
SensorPairedRecord ::= SEQUENCE {
   sensorSerialNumber                  SensorSerialNumber,
   sensorApprovalNumber                SensorApprovalNumber,
   sensorPairingDate                   SensorPairingDate
}
```

sensorSerialNumber е серийният номер на датчик за движение, свързан с бордовото устройство.

sensorApprovalNumber е номерът на одобрение на този датчик за движение.

sensorPairingDate е датата на сдвояване на този датчик за движение с бордовото устройство.

2.146. **SensorPairingDate**

Дата на сдвояване на датчика за движение с бордово устройство.

```
SensorPairingDate ::= TimeReal
```

Присвояване на стойност: не е указана.

2.147. **SensorSCIdentifier**

Идентификатор на компонента за сигурност на датчика за движение.

```
SensorSCIdentifier ::= IA5String(SIZE(8))
```

Присвояване на стойност: зависи от производителя на компонента.

2.148. **SensorSerialNumber**

Сериен номер на датчика за движение.

```
SensorSerialNumber ::= ExtendedSerialNumber
```

2.149. **Signature**

Електронен подпис.

Поколение 1:

```
Signature ::= OCTET STRING (SIZE(128))
```

Присвояване на стойност: съгласно общите механизми за сигурност от допълнение 11.

Поколение 2:

```
Signature ::= OCTET STRING (SIZE(64..132))
```

Присвояване на стойност: съгласно общите механизми за сигурност от допълнение 11.

2.150. **SignatureRecordArray**

Поколение 2:

Набор от подписи плюс метаданните, използвани в протокола за изтегляне на данни.

```
SignatureRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF Signature
}
```

recordType указва типа запис (Signature). **Присвояване на стойност**: вж. RecordType.

recordSize е размерът на Signature в байтове.

noOfRecords е броят на записите в набора от записи. Стойността се определя на 1, тъй като подписите могат да имат различна дължина.

records е наборът от подписи.

2.151. **SimilarEventsNumber**

Броят на сходните събития от определен ден (изискване 094 от приложение 1Б и изискване 117 от приложение 1В).

```
SimilarEventsNumber ::= INTEGER(0..255)
```

Присвояване на стойност: 0 не се използва, 1 означава, че само едно събитие от този тип е настъпило и е било съхранено през съответния ден, 2 означава, че две събития от този тип са настъпили през съответния ден (само едно от тях е било съхранено), … 255 означава, че през разглеждания ден са настъпили 255 или повече събития от този тип.

2.152. **SpecificConditionRecord**

Информация, съхранена на карта на водач, карта за монтаж и настройки или бордово устройство и отнасяща се до определено специфично условие (изисквания 130, 276, 301, 328 и 355 от приложение 1В).

```
SpecificConditionRecord ::= SEQUENCE {
   entryTime                           TimeReal,
   specificConditionType               SpecificConditionType
}
```

entryTime е датата и часът на въвеждането на тези данни.

specificConditionType е кодът, идентифициращ специфичното условие.

2.153. **SpecificConditions**

Информация, съхранена на карта на водач, карта за монтаж и настройки или бордово устройство и отнасяща се до определено специфично условие (изисквания 131, 277, 302, 329 и 356 от приложение 1В).

Поколение 2:

```
SpecificConditions := SEQUENCE {
   conditionPointerNewestRecord        INTEGER(0..NoOfSpecificConditionRecords-1),
   specificConditionRecords            SET SIZE(NoOfSpecificConditionRecords) OF
                                       SpecificConditionRecord
}
```

conditionPointerNewestRecord е индексът на последния актуализиран запис за специфично условие.

Присвояване на стойност: число, съответстващо на номератора на записа за специфично условие, като се започва с 0 за първия случай на запис за специфично условие в структурата.

specificConditionRecords е наборът от записи, съдържащ информация за записаните специфични условия.

2.154. **SpecificConditionType**

Код, идентифициращ специфично условие (изисквания 050б, 105а, 212а и 230а от приложение 1Б и изискване 62 от приложение 1В).

```
SpecificConditionType ::= INTEGER(0..255)
```

Поколение 1:

Присвояване на стойност:

‘00’H	RFU
‘01’H	Извън обхват — начало
‘02’H	Извън обхват— край
‘03’H	Пътуване с ферибот/влак
‘04’H .. ‘FF’H	RFU

Поколение 2:

Присвояване на стойност:

‘00’H	RFU
‘01’H	Извън обхват — начало
‘02’H	Извън обхват — край
‘03’H	Пътуване с ферибот/влак — начало
‘04’H	Пътуване с ферибот/влак — край
‘05’H .. ‘FF’H	RFU

2.155. **Speed**

Скорост на превозното средство (km/h).

```
Speed ::= INTEGER(0..255)
```

Присвояване на стойност: километри на час в работния диапазон от 0 до 220 km/h.

2.156. **SpeedAuthorised**

Максимална разрешена скорост на превозното средство (определение зз).

```
SpeedAuthorised ::= Speed
```

2.157. **SpeedAverage**

Средна скорост, измерена в рамките на предварително определен период от време (km/h).

```
SpeedAverage ::= Speed
```

2.158. **SpeedMax**

Максимална скорост, измерена в рамките на предварително определен период от време.

```
SpeedMax ::= Speed
```

2.159. **TachographPayload**

Поколение 2:

За определението на този тип данни вж. допълнение 14.

2.160. **TachographPayloadEncrypted**

Поколение 2:

Криптираните полезни данни от тахографа в DER-TLV, т.е. изпратените данни, криптирани в съобщение RTM. За криптирането вж. допълнение 11, част Б, глава 13.

```
TachographPayloadEncrypted ::= SEQUENCE {
   tag                                  OCTET STRING(SIZE(1)),
   length                               OCTET STRING(SIZE(1..2)),
   paddingContentIndicatorByte          OCTET STRING(SIZE(1)),
   encryptedData                        OCTET STRING(SIZE(16..192))
}
```

tag е част от кодирането DER-TLV и за него се задава‘87’ (вж. допълнение 11, част Б, глава 13).

length е част от кодирането DER-TLV и кодира дължината на следните paddingContentIndicatorByte и encryptedData.

за **paddingContentIndicatorByte** се задава ‘00’.

encryptedData е криптираният tachographPayload, както е посочен в допълнение 11, част Б, глава 13. Дължината на тези данни в октети трябва винаги да е число, кратно на 16.

2.161. **TDesSessionKey**

Поколение 1:

Троен ключ на сесия DES.

```
TDesSessionKey ::= SEQUENCE {
   tDesKeyA                             OCTET STRING (SIZE(8)),
   tDesKeyB                             OCTET STRING (SIZE(8))
}
```

Присвояване на стойност: липса на допълнителна информация.

2.162. **TimeReal**

Код за комбинирано поле — дата и час, изразени в секунди, считано от 00ч.00м.00сек. по координираното универсално време на 1 януари 1970 г.

```
TimeReal{INTEGER:TimeRealRange} ::= INTEGER(0..TimeRealRange)
```

Присвояване на стойност — синхронизиран октет: брой секунди от полунощ на 1 януари 1970 г. по координираното универсално време.

Най-далечната бъдеща дата/час е през 2106 г.

2.163. **TyreSize**

Обозначение на размерите на гумите.

```
TyreSize ::= IA5String(SIZE(15))
```

Присвояване на стойност: съгласно Директива 92/23 (ЕИО), ОВ L 129, 31.3.1992 г., стр. 95.

2.164. **VehicleIdentificationNumber**

Идентификационен номер на превозното средство (VIN), отнасящ се за цялото превозно средство, обикновено сериен номер на шаси или номер на рама.

```
VehicleIdentificationNumber ::= IA5String(SIZE(17))
```

Присвояване на стойност: съгласно стандарт ISO 3779.

2.165. **VehicleIdentificationNumberRecordArray**

Поколение 2:

Идентификационният номер на превозното средство плюс метаданните, използвани в протокола за изтегляне на данни.

```
VehicleIdentificationNumberRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       VehicleIdentificationNumber
}
```

recordType указва типа запис (VehicleIdentificationNumber). **Присвояване на стойност**: вж. RecordType.

recordSize е размерът на VehicleIdentificationNumber в байтове.

noOfRecords е броят на записите в набора от записи.

records е наборът от идентификационни номера на превозни средства.

2.166. **VehicleRegistrationIdentification**

Идентификация на превозно средство, която е уникална за Европа (VRN и държава членка).

```
VehicleRegistrationIdentification ::= SEQUENCE {
   vehicleRegistrationNation           NationNumeric,
   vehicleRegistrationNumber           VehicleRegistrationNumber
}
```

vehicleRegistrationNation е държавата, в която е извършена регистрацията на превозното средство.

vehicleRegistrationNumber е регистрационният номер на превозното средство (VRN).

2.167. **VehicleRegistrationNumber**

Регистрационен номер на превозното средство (VRN). Регистрационният номер се определя от компетентния орган за регистрацията на превозните средства.

```
VehicleRegistrationNumber ::= SEQUENCE {
   codePage                            INTEGER (0..255),
   vehicleRegNumber                    OCTET STRING (SIZE(13))
}
```

codePage указва набор от символи, определен в глава 4.

vehicleRegNumber е VRN, кодиран с използването на указания набор от символи.

Присвояване на стойност: зависи от държавата.

2.168. **VehicleRegistrationNumberRecordArray**

Поколение 2:

Регистрационният номер на превозното средство плюс метаданните, използвани в протокола за изтегляне на данни.

```
VehicleRegistrationNumberRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       VehicleRegistrationNumber
}
```

recordType указва типа запис (VehicleRegistrationNumber). **Присвояване на стойност**: вж. RecordType.

recordSize е размерът на VehicleRegistrationNumber в байтове.

noOfRecords е броят на записите в набора от записи.

records е наборът от регистрационни номера на превозни средства.

2.169. **VuAbility**

Поколение 2:

Информация, съхранена в бордово устройство, за възможността му да използва тахографски карти от поколение 1 (изискване 121 от приложение 1B).

```
VuAbility ::= OCTET STRING (SIZE(1))
```

Присвояване на стойност — синхронизиран октет: 'xxxxxxxa'B (8 бита)

За възможността да поддържа тахографски карти от поколение 1:

‘a’B	Възможност да поддържа тахографски карти от поколение 1:
	‘0’ B поддържат се карти от поколение 1,
	‘1’B не се поддържат карти от поколение 1,
‘xxxxxxx’B	RFU

2.170. **VuActivityDailyData**

Поколение 1:

Информация, съхранена в бордово устройство и отнасяща се за промените на дейността и/или промените на състоянието при управление и/или промените на статуса на картата за определен календарен ден (изискване 084 от приложение 1Б и изисквания 105, 106 и 107 от приложение 1В) и за статуса на процепите в 00.00 часа на този ден.

```
VuActivityDailyData ::= SEQUENCE {
   noOfActivityChanges                  INTEGER SIZE(0..1440),
   activityChangeInfos                  SET SIZE(noOfActivityChanges) OF
                                        ActivityChangeInfo
}
```

noOfActivityChanges е броят думи от ActivityChangeInfo в набора activityChangeInfos.

activityChangeInfos е наборът думи от ActivityChangeInfo, съхранени в бордовото устройство за съответния ден. Той съдържа винаги две думи от ActivityChangeInfo, които указват статуса на двата процепа в 00.00 часа на същия ден.

2.171. **VuActivityDailyRecordArray**

Поколение 2:

Информация, съхранена в бордово устройство и отнасяща се за промените на дейността и/или промените на състоянието при управление и/или промените на статуса на картата за определен календарен ден (изисквания 105, 106 и 107 от приложение 1В) и за статуса на процепите в 00.00 часа на този ден.

```
VuActivityDailyRecordArray ::= SEQUENCE {
   recordType                           RecordType,
   recordSize                           INTEGER(1..65535),
   noOfRecords                          INTEGER(0..65535),
   records                              SET SIZE(noOfRecords) OF ActivityChangeInfo
}
```

recordType указва типа запис (ActivityChangeInfo). **Присвояване на стойност**: вж. RecordType.

recordSize е размерът на ActivityChangeInfo в байтове.

noOfRecords е броят на записите в набора от записи.

records е наборът думи от ActivityChangeInfo, съхранени в бордовото устройство за съответния ден. Той съдържа винаги две думи от ActivityChangeInfo, които указват статуса на двата процепа в 00.00 часа на същия ден.

2.172. **VuApprovalNumber**

Номер на одобрение на типа на бордовото устройство.

Поколение 1:

```
VuApprovalNumber ::= IA5String(SIZE(8))
```

Присвояване на стойност: не е указана.

Поколение 2:

```
VuApprovalNumber ::= IA5String(SIZE(16))
```

Присвояване на стойност:

Номерът на одобрение е този, който е публикуван на съответната интернет страница на Европейската комисия, т.е. например, като се включват тиренца, ако има. Номерът на одобрение се подравнява отляво.

2.173. **VuCalibrationData**

Поколение 1:

Информация, съхранена в бордово устройство и отнасяща се за калибрированията на уредите за регистриране на данните за движението (изискване 098 от приложение 1Б).

```
VuCalibrationData ::= SEQUENCE {
   noOfVuCalibrationRecords             INTEGER(0..255),
   vuCalibrationRecords                 SET SIZE(noOfVuCalibrationRecords) OF
                                        VuCalibrationRecord
}
```

noOfVuCalibrationRecords е броят записи, които съдържа наборът vuCalibrationRecords.

vuCalibrationRecords е наборът записи от калибрированията.

2.174. **VuCalibrationRecord**

Информация, съхранена в бордово устройство и отнасяща се за калибриране на уредите за регистриране на данните за движението (изискване 098 от приложение 1Б и изисквания 119 и 120 от приложение 1В).

Поколение 1:

```
VuCalibrationRecord ::= SEQUENCE {
   calibrationPurpose                   CalibrationPurpose,
   workshopName                         Name,
   workshopAddress                      Address,
   workshopCardNumber                   FullCardNumber,
   workshopCardExpiryDate               TimeReal,
   vehicleIdentificationNumber          VehicleIdentificationNumber,
   vehicleRegistrationIdentification    VehicleRegistrationIdentification,
   wVehicleCharacteristicConstant       W-VehicleCharacteristicConstant,
   kConstantOfRecordingEquipment        K-ConstantOfRecordingEquipment,
   lTyreCircumference                   L-TyreCircumference,
   tyreSize                             TyreSize,
   authorisedSpeed                      SpeedAuthorised,
   oldOdometerValue                     OdometerShort,
   newOdometerValue                     OdometerShort,
   oldTimeValue                         TimeReal,
   newTimeValue                         TimeReal,
   nextCalibrationDate                  TimeReal
}
```

calibrationPurpose е целта на калибрирането.

workshopName, workshopAddress са наименованието и адресът на сервиза.

workshopCardNumber идентифицира картата за монтаж и настройки, използвана при калибрирането.

workshopCardExpiryDate е датата на край на валидност на картата.

vehicleIdentificationNumber е VIN.

vehicleRegistrationIdentification съдържа VRN и регистриращата държава членка.

wVehicleCharacteristicConstant е характеристичният коефициент на превозното средство.

kConstantOfRecordingEquipment е константата на уреда за регистриране на данните за движението.

lTyreCircumference е действителната обиколка на колелата.

tyreSize е обозначение на размерите на гумите, монтирани на превозното средство.

authorisedSpeed е разрешената скорост на превозното средство.

oldOdometerValue и newOdometerValue са старата и новата стойност, отчетени от километражния брояч.

oldTimeValue, newTimeValue са старите и новите стойности на датата и часа.

nextCalibrationDate е датата на следващото калибриране на типа в CalibrationPurpose, което оправомощеният инспектиращ орган трябва да извърши.

Поколение 2:

```
VuCalibrationRecord ::= SEQUENCE {
   calibrationPurpose                    CalibrationPurpose,
   workshopName                          Name,
   workshopAddress                       Address,
   workshopCardNumber                    FullCardNumber,
   workshopCardExpiryDate                TimeReal,
   vehicleIdentificationNumber           VehicleIdentificationNumber,
   vehicleRegistrationIdentification     VehicleRegistrationIdentification,
   wVehicleCharacteristicConstant        W-VehicleCharacteristicConstant,
   kConstantOfRecordingEquipment         K-ConstantOfRecordingEquipment,
   lTyreCircumference                    L-TyreCircumference,
   tyreSize                              TyreSize,
   authorisedSpeed                       SpeedAuthorised,
   oldOdometerValue                      OdometerShort,
   newOdometerValue                      OdometerShort,
   oldTimeValue                          TimeReal,
   newTimeValue                          TimeReal,
   nextCalibrationDate                   TimeReal,
   sealDataVu                            SealDataVu
}
```

В допълнение към поколение 1 се използва следният елемент от данни:

sealDataVu дава информация за пломбите, поставени върху различните компоненти на превозното средство.

2.175. **VuCalibrationRecordArray**

Поколение 2:

Информация, съхранена в бордово устройство и отнасяща се за калибрираниятa на уредите за регистриране на данните за движението (изисквания 119 и 120 от приложение 1B).

```
VuCalibrationRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       VuCalibrationRecord
}
```

recordType указва типа запис (VuCalibrationRecord). **Присвояване на стойност**: вж. RecordType.

recordSize е размерът на VuCalibrationRecord в байтове.

noOfRecords е броят на записите в набора от записи.

records е наборът от записи за калибрирането.

2.176. **VuCardIWData**

Поколение 1:

Информация, съхранена в бордово устройство и отнасяща се за циклите на вкарване и изваждане на картите на водач или картите за монтаж и настройки в бордовото устройство (изискване 081 от приложение 1Б и изискване 103 от приложение 1В).

```
VuCardIWData ::= SEQUENCE {
   noOfIWRecords                       INTEGER(0..2^16-1),
   vuCardIWRecords                     SET SIZE(noOfIWRecords) OF VuCardIWRecord
}
```

noOfIWRecords е броят на записите, които съдържа наборът vuCardIWRecords.

vuCardIWRecords е набор от записи относно циклите на вкарване и изваждане на картите.

2.177. **VuCardIWRecord**

Информация, съхранена в бордово устройство и отнасяща се за цикъла на вкарване и изваждане на карта на водач или карта за монтаж и настройки в бордовото устройство (изискване 081 от приложение 1Б и изискване 102 от приложение 1В).

Поколение 1:

```
VuCardIWRecord ::= SEQUENCE {
   cardHolderName                      HolderName,
   fullCardNumber                      FullCardNumber,
   cardExpiryDate                      TimeReal,
   cardInsertionTime                   TimeReal,
   vehicleOdometerValueAtInsertion     OdometerShort,
   cardSlotNumber                      CardSlotNumber,
   cardWithdrawalTime                  TimeReal,
   vehicleOdometerValueAtWithdrawal    OdometerShort,
   previousVehicleInfo                 PreviousVehicleInfo,
   manualInputFlag                     ManualInputFlag
}
```

cardHolderName е фамилията, името и презимето на титуляря на картата на водач или картата за монтаж и настройки, съхранени на картата.

fullCardNumber е типът карта, държавата членка, която я издава, и нейният номер на карта, съхранени на картата.

cardExpiryDate е датата на изтичане на валидността на картата, както е съхранена на нея.

cardInsertionTime е датата и часът на вкарване на картата.

vehicleOdometerValueAtInsertion е стойността, отчетена от километражния брояч при вкарване на картата.

cardSlotNumber е процепът, където се вкарва картата.

cardWithdrawalTime е датата и часът на изваждане на картата.

vehicleOdometerValueAtWithdrawal е стойността, отчетена от километражния брояч при изваждане на картата.

previousVehicleInfo съдържа информация относно предишното превозно средство, използвано от водача, както е съхранена на картата.

manualInputFlag е знак, позволяващ да се разбере дали титулярят на картата е извършил ръчно въвеждане на дейностите на водача при вкарване на картата.

Поколение 2:

```
VuCardIWRecord ::= SEQUENCE {
   cardHolderName                       HolderName,
   fullCardNumberAndGeneration          FullCardNumberAndGeneration,
   cardExpiryDate                       TimeReal,
   cardInsertionTime                    TimeReal,
   vehicleOdometerValueAtInsertion      OdometerShort,
   cardSlotNumber                       CardSlotNumber,
   cardWithdrawalTime                   TimeReal,
   vehicleOdometerValueAtWithdrawal     OdometerShort,
   previousVehicleInfo                  PreviousVehicleInfo,
   manualInputFlag                      ManualInputFlag
}
```

Вместо fullCardNumber структурата на данните от поколение 2 използва следния елемент от данни.

fullCardNumberAndGeneration е типът карта, държавата членка, която я издава, нейният номер на карта и поколението, съхранени на картата.

2.178. **VuCardIWRecordArray**

Поколение 2:

Информация, съхранена в бордово устройство и отнасяща се до циклите на вкарване и изваждане на карти на водач или карти за монтаж и настройки в бордовото устройство (изискване 103 от приложение 1B).

```
VuCardIWRecordArray ::= SEQUENCE {
   recordType                           RecordType,
   recordSize                           INTEGER(1..65535),
   noOfRecords                          INTEGER(0..65535),
   records                              SET SIZE(noOfRecords) OF VuCardIWRecord
}
```

recordType указва типа запис (VuCardIWRecord). **Присвояване на стойност**: вж. RecordType.

recordSize е размерът на VuCardIWRecord в байтове.

noOfRecords е броят на записите в набора от записи.

records е набор от записи относно циклите на вкарване и изваждане на картите.

2.179. **VuCardRecord**

Поколение 2:

Информация, съхранена в бордово устройство, относно използвана тахографска карта (изискване 132 от приложение 1B).

```
VuCardRecord ::= SEQUENCE {
   cardExtendedSerialNumber            ExtendedSerialNumber,
   cardPersonaliserID                  OCTET STRING(SIZE(1)),
   typeofTachographCardID              EquipmentType,
   cardStructureVersion                CardStructureVersion,
   cardNumber                          CardNumber
}
```

cardExtendedSerialNumber е от файла EF_ICC под MF на картата.

cardPersonaliserID е от файла EF_ICC под MF на картата.

typeOfTachographCardId е от файла EF_Application_Identification под DF_Tachograph_G2

cardStructureVersion е от файла EF_Application_Identification под DF_Tachograph_G2.

cardNumber е от файла EF_Identification под DF_Tachograph_G2.

2.180. **VuCardRecordArray**

Поколение 2:

Информация, съхранена в бордово устройство относно използвани тахографски карти с това бордово устройство. Тази информация е предназначена за анализа на бордово устройство — проблеми с картата (изискване 132 от приложение 1B).

```
VuCardRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF VuCardRecord
}
```

recordType указва типа запис (VuCardRecord). **Присвояване на стойност**: вж. RecordType.

recordSize е размерът на VuCardRecord в байтове.

noOfRecords е броят на записите в набора от записи.

records е набор от записи относно използваните тахографски карти с бордовото устройство.

2.181. **VuCertificate**

Сертификат на публичния ключ на бордово устройство.

```
VuCertificate ::= Certificate
```

2.182. **VuCertificateRecordArray**

Поколение 2:

Сертификатът за бордовото устройство плюс метаданните, използвани в протокола за изтегляне на данни.

```
VuCertificateRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF VuCertificate
}
```

recordType указва типа запис (VuCertificate). **Присвояване на стойност**: вж. RecordType.

recordSize е размерът на VuCertificate в байтове.

noOfRecords е броят на записите в набора от записи. Стойността се определя на 1, тъй като сертификатите могат да имат различна дължина.

records е наборът от сертификати за бордови устройства.

2.183. **VuCompanyLocksData**

Поколение 1:

Информация, съхранена в бордово устройство и отнасяща се до блокировките на превозвач (изискване 104 от приложение 1Б).

```
VuCompanyLocksData ::= SEQUENCE {
   noOfLocks                          INTEGER(0..255),
   vuCompanyLocksRecords              SET SIZE(noOfLocks) OF VuCompanyLocksRecord
}
```

noOfLocks е броят на блокировките, посочени в vuCompanyLocksRecords.

vuCompanyLocksRecords е набор от записи за блокировките на превозвач.

2.184. **VuCompanyLocksRecord**

Информация, съхранена в бордово устройство и отнасяща се до блокировка на превозвач (изискване 104 от приложение 1Б и изискване 128 от приложение 1В).

Поколение 1:

```
VuCompanyLocksRecord ::= SEQUENCE {
   lockInTime                         TimeReal,
   lockOutTime                        TimeReal,
   companyName                        Name,
   companyAddress                     Address,
   companyCardNumber                  FullCardNumber
}
```

lockInTime, lockOutTime са датата и часът на блокиране и отблокиране.

companyName, companyAddress са наименованието и адресът на превозвача, свързан с блокирането.

companyCardNumber идентифицира картата, използвана при блокирането.

Поколение 2:

```
VuCompanyLocksRecord ::= SEQUENCE {
   lockInTime                         TimeReal,
   lockOutTime                        TimeReal,
   companyName                        Name,
   companyAddress                     Address,
   companyCardNumberAndGeneration     FullCardNumberAndGeneration
}
```

Вместо companyCardNumber структурата на данните от поколение 2 използва следния елемент от данни.

companyCardNumberAndGeneration идентифицира картата, включително поколението ѝ, използвана при блокирането.

2.185. **VuCompanyLocksRecordArray**

Поколение 2:

Информация, съхранена в бордово устройство и отнасяща се за блокировките на превозвач (изискване 128 от приложение 1В).

```
VuCompanyLocksRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       VuCompanyLocksRecord
}
```

recordType указва типа запис (VuCompanyLocksRecord). **Присвояване на стойност**: вж. RecordType.

recordSize е размерът на VuCompanyLocksRecord в байтове.

noOfRecords е броят на записите в набора от записи. Стойност 0..255.

records е наборът от записи за блокировките на превозвач.

2.186. **VuControlActivityData**

Поколение 1:

Информация, съхранена в бордово устройство и отнасяща се за проверките, извършени с помощта на това устройство (изискване 102 от приложение 1Б).

```
VuControlActivityData ::= SEQUENCE {
   noOfControls                        INTEGER(0..20),
   vuControlActivityRecords            SET SIZE(noOfControls) OF
                                       VuControlActivityRecord
}
```

noOfControls е броят на проверките, посочени в vuControlActivityRecords.

vuControlActivityRecords е наборът от записи за контролната дейност.

2.187. **VuControlActivityRecord**

Информация, съхранена в бордово устройство и отнасяща се за проверка, извършена, като е използвано това устройство (изискване 102 от приложение 1Б и изискване 126 от приложение 1В).

Поколение 1:

```
VuControlActivityRecord ::= SEQUENCE {
   controlType                         ControlType,
   controlTime                         TimeReal,
   controlCardNumber                   FullCardNumber,
   downloadPeriodBeginTime             TimeReal,
   downloadPeriodEndTime               TimeReal
}
```

controlType е типът проверка.

controlTime е датата и часът на проверката.

controlCardNumber идентифицира контролната карта, използвана за проверката.

downloadPeriodBeginTime е началото на периода на изтегляне на данните.

downloadPeriodEndTime е краят на периода на изтегляне на данните.

Поколение 2:

```
VuControlActivityRecord ::= SEQUENCE {
   controlType                          ControlType,
   controlTime                          TimeReal,
   controlCardNumberAndGeneration       FullCardNumberAndGeneration,
   downloadPeriodBeginTime              TimeReal,
   downloadPeriodEndTime                TimeReal
}
```

Вместо controlCardNumber структурата на данните от поколение 2 използва следния елемент от данни.

controlCardNumberAndGeneration идентифицира контролната карта, включително поколението ѝ, използвана за проверката.

2.188. **VuControlActivityRecordArray**

Поколение 2:

Информация, съхранена в бордово устройство и отнасяща се до проверките, извършени с помощта на това устройство (изискване 126 от приложение 1В).

```
VuControlActivityRecordArray ::= SEQUENCE {
   recordType                           RecordType,
   recordSize                           INTEGER(1..65535),
   noOfRecords                          INTEGER(0..65535),
   records                              SET SIZE(noOfRecords) OF
                                        VuControlActivityRecord
}
```

recordType указва типа запис (VuControlActivityRecord). **Присвояване на стойност**: вж. RecordType.

recordSize е размерът на VuControlActivityRecord в байтове.

noOfRecords е броят на записите в набора от записи.

records е наборът от записи за контролната дейност на бордовото устройство.

2.189. **VuDataBlockCounter**

Брояч, записан на карта и идентифициращ последователно циклите на вкарване и изваждане на картата в бордови устройства.

```
VuDataBlockCounter ::= BCDString(SIZE(2))
```

Присвояване на стойност: последователни номера, с максималната стойност от 9999, като се започва от 0.

2.190. **VuDetailedSpeedBlock**

Информация, съхранена в бордово устройство и отнасяща се до подробните данни за скоростта на превозното средство в продължение на една минута, по време на която превозното средство е било в движение (изискване 093 от приложение 1Б и изискване 116 от приложение 1В).

```
VuDetailedSpeedBlock ::= SEQUENCE {
   speedBlockBeginDate    TimeReal,
   speedsPerSecond        SEQUENCE SIZE(60) OF Speed
}
```

speedBlockBeginDate е датата и часът на първата стойност на скоростта в блока.

speedsPerSecond е хронологичната последователност на скоростите, измерени във всички секунди на минутата, започвайки при скоростта от speedBlockBeginDate (включена).

2.191. **VuDetailedSpeedBlockRecordArray**

Поколение 2:

Информация, съхранена в бордово устройство и отнасяща се за подробните данни за скоростта на превозното средство.

```
VuDetailedSpeedBlockRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       VuDetailedSpeedBlock
}
```

recordType указва типа запис (VuDetailedSpeedBlock). **Присвояване на стойност**: вж. RecordType.

recordSize е размерът на VuDetailedSpeedBlock в байтове.

noOfRecords е броят на записите в набора от записи.

records е наборът от блокове с подробни данни за скоростта.

2.192. **VuDetailedSpeedData**

Поколение 1:

Информация, съхранена в бордово устройство и отнасяща се до подробните данни за скоростта на превозното средство.

```
VuDetailedSpeedData ::= SEQUENCE {
   noOfSpeedBlocks                     INTEGER(0..2^16-1),
   vuDetailedSpeedBlocks               SET SIZE(noOfSpeedBlocks) OF
                                       VuDetailedSpeedBlock
}
```

noOfSpeedBlocks е броят на блоковете с данни за скоростта в набора vuDetailedSpeedBlocks.

vuDetailedSpeedBlocks е наборът блокове с подробни данни за скоростта.

2.193. **VuDownloadablePeriod**

Най-старите и най-скорошните дати, за които определено бордово устройство съдържа данни относно дейностите на водачите (изисквания 081, 084 или 087 от приложение 1Б и изисквания 102, 105 и 108 от приложение 1В).

```
VuDownloadablePeriod ::= SEQUENCE {
   minDownloadableTime                 TimeReal
   maxDownloadableTime                 TimeReal
}
```

minDownloadableTime е датата и часът на най-отдалеченото във времето вкарване на карта, промяна на дейността или въвеждане на местоположението, съхранени в бордовото устройство.

maxDownloadableTime е датата и часът на последното вкарване на карта, промяна на дейността или въвеждане на местоположението, съхранени в бордовото устройство.

2.194. **VuDownloadablePeriodRecordArray**

Поколение 2:

VUDownloadablePeriod плюс метаданните, използвани в протокола за изтегляне на данни.

```
VuDownloadablePeriodRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       VuDownloadablePeriod
}
```

recordType указва типа запис (VuDownloadablePeriod). **Присвояване на стойност**: вж. RecordType.

recordSize е размерът на VuDownloadablePeriod в байтове.

noOfRecords е броят на записите в набора от записи.

records е наборът от записи от VuDownloadablePeriod.

2.195. **VuDownloadActivityData**

Информация, съхранена в бордово устройство и отнасяща се за последното ѝ изтегляне (изискване 105 от приложение 1Б и изискване 129 от приложение 1В).

Поколение 1:

```
VuDownloadActivityData ::= SEQUENCE {
   downloadingTime                     TimeReal,
   fullCardNumber                      FullCardNumber,
   companyOrWorkshopName               Name
}
```

downloadingTime е датата и часът на изтегляне на данни.

fullCardNumber идентифицира картата, използвана за разрешаване на изтеглянето на данните.

companyOrWorkshopName е наименованието на превозвача или сервиза.

Поколение 2:

```
VuDownloadActivityData ::= SEQUENCE {
   downloadingTime                     TimeReal,
   fullCardNumberAndGeneration         FullCardNumberAndGeneration,
   companyOrWorkshopName               Name
}
```

Вместо fullCardNumber структурата на данните от поколение 2 използва следния елемент от данни.

fullCardNumberAndGeneration идентифицира картата, включително поколението ѝ, използвана за разрешаване на изтеглянето на данните.

2.196. **VuDownloadActivityDataRecordArray**

Поколение 2:

Информация, свързана с последните изтеглени данни за бордовото устройство (изискване 129 от приложение 1В).

```
VuDownloadActivityDataRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF VuDownloadActivityData
}
```

recordType указва типа запис (VuDownloadActivityData). **Присвояване на стойност**: вж. RecordType.

recordSize е размерът на VuDownloadActivityData в байтове.

noOfRecords е броят на записите в набора от записи.

records е наборът от записи на изтеглени данни за дейността.

2.197. **VuEventData**

Поколение 1:

Информация, съхранена в бордово устройство и отнасяща се за събития (изискване 094 от приложение 1Б с изключение на събитията „превишаване на скоростта“).

```
VuEventData ::= SEQUENCE {
   noOfVuEvents                          INTEGER(0..255),
   vuEventRecords                        SET SIZE(noOfVuEvents) OF VuEventRecord
}
```

noOfVuEvents е броят на събитията, посочени в набора vuEventRecords.

vuEventRecords е набор записи за събития.

2.198. **VuEventRecord**

Информация, съхранена в бордово устройство и отнасяща се за събитие (изискване 094 от приложение 1Б и изискване 117 от приложение 1В с изключение на събитията „превишаване на скоростта“).

Поколение 1:

```
VuEventRecord ::= SEQUENCE {
   eventType                             EventFaultType,
   eventRecordPurpose                    EventFaultRecordPurpose,
   eventBeginTime                        TimeReal,
   eventEndTime                          TimeReal,
   cardNumberDriverSlotBegin             FullCardNumber,
   cardNumberCodriverSlotBegin           FullCardNumber,
   cardNumberDriverSlotEnd               FullCardNumber,
   cardNumberCodriverSlotEnd             FullCardNumber,
   similarEventsNumber                   SimilarEventsNumber
}
```

eventType е типът на събитието.

eventRecordPurpose е целта на записване на събитието.

eventBeginTime е датата и часът на начало на събитието.

eventEndTime е датата и часът на край на събитието.

cardNumberDriverSlotBegin идентифицира картата, вкарана в процепа за водача в началото на събитието.

cardNumberCodriverSlotBegin идентифицира картата, вкарана в процепа за втория водач в началото на събитието.

cardNumberDriverSlotEnd идентифицира картата, вкарана в процепа за водача в края на събитието.

cardNumberCodriverSlotEnd идентифицира картата, вкарана в процепа за втория водач в края на събитието.

similarEventsNumber е броят на сходните събития през същия ден.

Тази последователност може да се използва за всички събития, различни от „превишаване на скоростта“.

Поколение 2:

```
VuEventRecord ::= SEQUENCE {
   eventType                              EventFaultType,
   eventRecordPurpose                     EventFaultRecordPurpose,
   eventBeginTime                         TimeReal,
   eventEndTime                           TimeReal,
   cardNumberAndGenDriverSlotBegin        FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotBegin      FullCardNumberAndGeneration,
   cardNumberAndGenDriverSlotEnd          FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotEnd        FullCardNumberAndGeneration,
   similarEventsNumber                    SimilarEventsNumber,
   manufacturerSpecificEventFaultData   ManufacturerSpecificEventFaultData
}
```

В допълнение към поколение 1 се използват следните елементи от данни:

manufacturerSpecificEventFaultData съдържа допълнителна конкретна информация от производителя за събитието.

Вместо cardNumberDriverSlotBegin, cardNumberCodriverSlotBegin, cardNumberDriverSlotEnd и cardNumberCodriverSlotEnd структурата на данните от поколение 2 използва следните елементи от данни:

cardNumberAndGenDriverSlotBegin идентифицира картата, включително поколението ѝ, вкарана в процепа за водача в началото на събитието.

cardNumberAndGenCodriverSlotBegin идентифицира картата, включително поколението ѝ, вкарана в процепа за втория водач в началото на събитието.

cardNumberAndGenDriverSlotEnd идентифицира картата, включително поколението ѝ, вкарана в процепа за водача в края на събитието.

cardNumberAndGenCodriverSlotEnd идентифицира картата, включително поколението ѝ, вкарана в процепа за втория водач в края на събитието.

Ако събитието е „времеви конфликт“, eventBeginTime и eventEndTime трябва да се тълкуват, както следва:

eventBeginTime е датата и часът на уредите за регистриране на данните за движението.

eventEndTime е датата и часът по GNSS.

2.199. **VuEventRecordArray**

Поколение 2:

Информация, съхранена в бордово устройство и отнасяща се до събития (изискване 117 от приложение 1B с изключение на събитията „превишаване на скоростта“).

```
VuEventRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF VuEventRecord
}
```

recordType указва типа запис (VuEventRecord). **Присвояване на стойност**: вж. RecordType.

recordSize е размерът на VuEventRecord в байтове.

noOfRecords е броят на записите в набора от записи.

records е набор записи за събития.

2.200. **VuFaultData**

Поколение 1:

Информация, съхранена в бордово устройство и отнасяща се за неизправности (изискване 096 от приложение 1Б).

```
VuFaultData ::= SEQUENCE {
   noOfVuFaults                          INTEGER(0..255),
   vuFaultRecords                        SET SIZE(noOfVuFaults) OF VuFaultRecord
}
```

noOfVuFaults е броят на неизправностите, посочени в набора vuFaultRecords.

vuFaultRecords е набор записи на неизправности.

2.201. **VuFaultRecord**

Информация, съхранена в бордово устройство и отнасяща се за неизправност (изискване 096 от приложение 1Б и изискване 118 от приложение 1В).

Поколение 1:

```
VuFaultRecord ::= SEQUENCE {
   faultType                             EventFaultType,
   faultRecordPurpose                    EventFaultRecordPurpose,
   faultBeginTime                        TimeReal,
   faultEndTime                          TimeReal,
   cardNumberDriverSlotBegin             FullCardNumber,
   cardNumberCodriverSlotBegin           FullCardNumber,
   cardNumberDriverSlotEnd               FullCardNumber,
   cardNumberCodriverSlotEnd             FullCardNumber
}
```

faultType е типът на неизправността на уредите за регистриране на данните за движението.

faultRecordPurpose е целта на записване на неизправността.

faultBeginTime е датата и часът на начало на неизправността.

faultEndTime е датата и часът на край на неизправността.

cardNumberDriverSlotBegin идентифицира картата, вкарана в процепа за водача в началото на неизправността.

cardNumberCodriverSlotBegin идентифицира картата, вкарана в процепа за втория водач в началото на неизправността.

cardNumberDriverSlotEnd идентифицира картата, вкарана в процепа за водача в края на неизправността.

cardNumberCodriverSlotEnd идентифицира картата, вкарана в процепа за втория водач в края на неизправността.

Поколение 2:

```
VuFaultRecord ::= SEQUENCE {
   faultType                              EventFaultType,
   faultRecordPurpose                     EventFaultRecordPurpose,
   faultBeginTime                         TimeReal,
   faultEndTime                           TimeReal,
   cardNumberAndGenDriverSlotBegin        FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotBegin      FullCardNumberAndGeneration,
   cardNumberAndGenDriverSlotEnd          FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotEnd        FullCardNumberAndGeneration,
   manufacturerSpecificEventFaultData   ManufacturerSpecificEventFaultData
}
```

В допълнение към поколение 1 се използват следните елементи от данни:

manufacturerSpecificEventFaultData съдържа допълнителна конкретна информация от производителя за неизправността.

Вместо cardNumberDriverSlotBegin, cardNumberCodriverSlotBegin, cardNumberDriverSlotEnd и cardNumberCodriverSlotEnd структурата на данните от поколение 2 използва следните елементи от данни:

cardNumberAndGenDriverSlotBegin идентифицира картата, включително поколението ѝ, вкарана в процепа за водача в началото на неизправността.

cardNumberAndGenCodriverSlotBegin идентифицира картата, включително поколението ѝ, вкарана в процепа за втория водач в началото на неизправността.

cardNumberAndGenDriverSlotEnd идентифицира картата, включително поколението ѝ, вкарана в процепа за водача в края на неизправността.

cardNumberAndGenCodriverSlotEnd идентифицира картата, включително поколението ѝ, вкарана в процепа за втория водач в края на неизправността.

2.202. **VuFaultRecordArray**

Поколение 2:

Информация, съхранена в бордово устройство и отнасяща се за неизправности (изискване 118 от приложение 1B).

```
VuFaultRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF VuFaultRecord
}
```

recordType указва типа запис (VuFaultRecord). **Присвояване на стойност**: вж. RecordType.

recordSize е размерът на VuFaultRecord в байтове.

noOfRecords е броят на записите в набора от записи.

records е набор записи за неизправности.

2.203. **VuGNSSCDRecord**

Поколение 2:

Информация, съхранена в бордово устройство и отнасяща се за местоположението по GNSS на превозното средство, ако времето за непрекъснато управление на водача достигне кратно число на три часа (изисквания 108 и 110 от приложение 1B).

```
VuGNSSCDRecord ::= SEQUENCE {
   timeStamp                              TimeReal,
   cardNumberAndGenDriverSlot             FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlot           FullCardNumberAndGeneration,
   gnssPlaceRecord                        GNSSPlaceRecord
}
```

timeStamp е датата и часът, когато времето за непрекъснато управление на титуляря на картата достигне число, кратно на три часа.

cardNumberAndGenDriverSlot идентифицира картата, включително поколението ѝ, вкарана в процепа за водача.

cardNumberAndGenCodriverSlot идентифицира картата, включително поколението ѝ, вкарана в процепа за втория водач.

gnssPlaceRecord съдържа информация за местоположението на превозното средство.

2.204. **VuGNSSCDRecordArray**

Поколение 2:

Информация, съхранена в бордово устройство и отнасяща се за местоположението по GNSS на превозното средство, ако времето за непрекъснато управление на водача достигне число, кратно на три часа (изисквания 108 и 110 от приложение 1В).

```
VuGNSSCDRecordArray  ::= SEQUENCE {
   recordType                             RecordType,
   recordSize                             INTEGER(1..65535),
   noOfRecords                            INTEGER(0..65535),
   records                                SET SIZE(noOfRecords) OF VuGNSSCDRecord
}
```

recordType указва типа запис (VuGNSSCDRecord). **Присвояване на стойност**: вж. RecordType.

recordSize е размерът на VuGNSSCDRecord в байтове.

noOfRecords е броят на записите в набора от записи.

records е набор от записи за непрекъснато управление по GNSS.

2.205. **VuIdentification**

Информация, съхранена в бордово устройство и отнасяща се за идентификация на бордовото устройство (изискване 075 от приложение 1Б и изисквания 93 и 121 от приложение 1В).

Поколение 1:

```
VuIdentification ::= SEQUENCE {
   vuManufacturerName                     VuManufacturerName,
   vuManufacturerAddress                  VuManufacturerAddress,
   vuPartNumber                           VuPartNumber,
   vuSerialNumber                         VuSerialNumber,
   vuSoftwareIdentification               VuSoftwareIdentification,
   vuManufacturingDate                    VuManufacturingDate,
   vuApprovalNumber                       VuApprovalNumber
}
```

vuManufacturerName е наименованието на производителя на бордовото устройство.

v**vuManufacturerAddress** е адресът на производителя на бордовото устройство.

vuPartNumber е фабричният номер на бордовото устройство.

vuSerialNumber е серийният номер на бордовото устройство.

vuSoftwareIdentification идентифицира софтуера, използван в бордовото устройство.

vuManufacturingDate е датата на производство на бордовото устройство.

vuApprovalNumber е номерът на одобрение на типа на бордовото устройство.

Поколение 2:

```
VuIdentification ::= SEQUENCE {
   vuManufacturerName                  VuManufacturerName,
   vuManufacturerAddress               VuManufacturerAddress,
   vuPartNumber                        VuPartNumber,
   vuSerialNumber                      VuSerialNumber,
   vuSoftwareIdentification            VuSoftwareIdentification,
   vuManufacturingDate                 VuManufacturingDate,
   vuApprovalNumber                    VuApprovalNumber,
   vuGeneration                        Generation,
   vuAbility                           VuAbility
}
```

В допълнение към поколение 1 се използват следните елементи от данни:

vuGeneration идентифицира поколението на бордовото устройство.

vuAbility осигурява информация дали бордовото устройство поддържа тахографски карти от поколение 1.

2.206. **VuIdentificationRecordArray**

Поколение 2:

VuIdentification плюс метаданните, използвани в протокола за изтегляне на данни.

```
VuIdentificationRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF VuIdentification
}
```

recordType указва типа запис (VuIdentification). **Присвояване на стойност**: вж. RecordType.

recordSize е размерът на VuIdentification в байтове.

noOfRecords е броят на записите в набора от записи.

records е набор записи от VuIdentification.

2.207. **VuITSConsentRecord**

Поколение 2:

Информация, съхранена в бордово устройство и отнасяща се за съгласието на водача да използва интелигентни транспортни системи.

```
VuITSConsentRecord ::= SEQUENCE {
   cardNumberAndGen                    FullCardNumberAndGeneration,
   consent                             BOOLEAN
}
```

cardNumberAndGen идентифицира картата, включително поколението ѝ. Това трябва да е карта на водач или карта за монтаж и настройки.

consent е флаг, който указва дали водачът е дал съгласието си за използването на интелигентни транспортни системи на това превозно средство/бордово устройство.

Присвояване на стойност:

TRUE указва съгласието на водача да използва интелигентни транспортни системи

FALSE указва отказа на водача да използва интелигентни транспортни системи

2.208. **VuITSConsentRecordArray**

Поколение 2:

Информация, съхранена в бордово устройство и отнасяща се за съгласието на водачите да използват интелигентни транспортни системи (изискване 200 от приложение 1B).

```
VuITSConsentRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF VuITSConsentRecord
}
```

recordType указва типа запис (VuITSConsentRecord). **Присвояване на стойност**: вж. RecordType.

recordSize е размерът на VuITSConsentRecord в байтове.

noOfRecords е броят на записите в набора от записи.

records е наборът от записи за съгласието във връзка с интелигентните транспортни системи.

2.209. **VuManufacturerAddress**

Адрес на производителя на бордовото устройство.

```
VuManufacturerAddress ::= Address
```

Присвояване на стойност: не е указана.

2.210. **VuManufacturerName**

Наименование на производителя на бордовото устройство.

```
VuManufacturerName ::= Name
```

Присвояване на стойност: не е указана.

2.211. **VuManufacturingDate**

Дата на производство на бордовото устройство.

```
VuManufacturingDate ::= TimeReal
```

Присвояване на стойност: не е указана.

2.212. **VuOverSpeedingControlData**

Информация, съхранена в бордово устройство и отнасяща се за събитията „превишаване на скоростта“, настъпили след извършване на последната проверка за превишаване на скоростта (изискване 095 от приложение 1Б и изискване 117 от приложение 1В).

```
VuOverSpeedingControlData ::= SEQUENCE {
   lastOverspeedControlTime             TimeReal,
   firstOverspeedSince                  TimeReal,
   numberOfOverspeedSince               OverspeedNumber
}
```

lastOverspeedControlTime е датата и часът на последната проверка за превишаване на скоростта.

firstOverspeedSince е датата и часът на първото превишаване на скоростта след последната проверка за превишаване на скоростта.

numberOfOverspeedSince е броят на събитията „превишаване на скоростта“ след последната проверка за превишаване на скоростта.

2.213. **VuOverSpeedingControlDataRecordArray**

Поколение 2:

VuOverSpeedingControlData плюс метаданните, използвани в протокола за изтегляне на данни.

```
VuOverSpeedingControlDataRecordArray ::= SEQUENCE {
   recordType                           RecordType,
   recordSize                           INTEGER(1..65535),
   noOfRecords                          INTEGER(0..65535),
   records                              SET SIZE(noOfRecords) OF
                                        VuOverSpeedingControlData
}
```

recordType указва типа запис (VuOverSpeedingControlData). **Присвояване на стойност**: вж. RecordType.

recordSize е размерът на VuOverSpeedingControlData в байтове.

noOfRecords е броят на записите в набора от записи.

records е набор от записи с данни за проверките за превишаване на скоростта.

2.214. **VuOverSpeedingEventData**

Поколение 1:

Информация, съхранена в бордово устройство и отнасяща се до събитията „превишаване на скоростта“ (изискване 094 от приложение 1Б).

```
VuOverSpeedingEventData ::= SEQUENCE {
   noOfVuOverSpeedingEvents             INTEGER(0..255),
   vuOverSpeedingEventRecords           SET SIZE(noOfVuOverSpeedingEvents) OF
                                        VuOverSpeedingEventRecord
}
```

noOfVuOverSpeedingEvents е броят на събитията, посочени в набора vuOverSpeedingEventRecords.

vuOverSpeedingEventRecords е набор от записи на събития „превишаване на скоростта“.

2.215. **VuOverSpeedingEventRecord**

Поколение 1:

Информация, съхранена в бордово устройство и отнасяща се за събития „превишаване на скоростта“ (изискване 094 от приложение 1Б и изискване 117 от приложение 1В).

```
VuOverSpeedingEventRecord ::= SEQUENCE {
   eventType                          EventFaultType,
   eventRecordPurpose                 EventFaultRecordPurpose,
   eventBeginTime                     TimeReal,
   eventEndTime                       TimeReal,
   maxSpeedValue                      SpeedMax,
   averageSpeedValue                  SpeedAverage,
   cardNumberDriverSlotBegin          FullCardNumber,
   similarEventsNumber                SimilarEventsNumber
}
```

eventType е типът на събитието.

eventRecordPurpose е целта на записване на събитието.

eventBeginTime е датата и часът на начало на събитието.

eventEndTime е датата и часът на край на събитието.

maxSpeedValue е максималната скорост, измерена по време на събитието.

averageSpeedValue е средноаритметичната скорост, измерена по време на събитието.

cardNumberDriverSlotBegin идентифицира картата, вкарана в процепа за водача в началото на събитието.

similarEventsNumber е броят на сходните събития през същия ден.

Поколение 2:

Информация, съхранена в бордово устройство и отнасяща се за събития „превишаване на скоростта“ (изискване 094 от приложение 1Б и изискване 117 от приложение 1В).

```
VuOverSpeedingEventRecord ::= SEQUENCE {
   eventType                          EventFaultType,
   eventRecordPurpose                 EventFaultRecordPurpose,
   eventBeginTime                     TimeReal,
   eventEndTime                       TimeReal,
   maxSpeedValue                      SpeedMax,
   averageSpeedValue                  SpeedAverage,
   cardNumberAndGenDriverSlotBegin    FullCardNumberAndGeneration,
   similarEventsNumber                SimilarEventsNumber
}
```

Вместо cardNumberDriverSlotBegin структурата на данните от поколение 2 използва следния елемент от данни:

cardNumberAndGenDriverSlotBegin идентифицира картата, включително поколението ѝ, вкарана в процепа за водача в началото на събитието.

2.216. **VuOverSpeedingEventRecordArray**

Поколение 2:

Информация, съхранена в бордово устройство и отнасяща се до събитията „превишаване на скоростта“ (изискване 117 от приложение 1В).

```
VuOverSpeedingEventRecordArray ::= SEQUENCE {
   recordType                         RecordType,
   recordSize                         INTEGER(1..65535),
   noOfRecords                        INTEGER(0..65535),
   records                            SET SIZE(noOfRecords) OF
                                      VuOverSpeedingEventRecord
}
```

recordType указва типа запис (VuOverSpeedingEventRecord). **Присвояване на стойност**: вж. RecordType.

recordSize е размерът на VuOverSpeedingEventRecord в байтове.

noOfRecords е броят на записите в набора от записи.

records е набор от записи за събития „превишаване на скоростта“.

2.217. **VuPartNumber**

Фабричен номер на бордовото устройство.

```
VuPartNumber ::= IA5String(SIZE(16))
```

Присвояване на стойност: зависи от производителя на бордовото устройство.

2.218. **VuPlaceDailyWorkPeriodData**

Поколение 1:

Информация, съхранена в бордово устройство и отнасяща се за местоположенията в началото или края на дневен период на работа на водачите (изискване 087 от приложение 1Б и изисквания 108 и 110 от приложение 1В).

```
VuPlaceDailyWorkPeriodData ::= SEQUENCE {
   noOfPlaceRecords                    INTEGER(0..255),
   vuPlaceDailyWorkPeriodRecords       SET SIZE(noOfPlaceRecords) OF
                                       VuPlaceDailyWorkPeriodRecord
}
```

noOfPlaceRecords е броят на записите, посочени в набора vuPlaceDailyWorkPeriodRecords.

vuPlaceDailyWorkPeriodRecords е набор от записи във връзка с местоположения.

2.219. **VuPlaceDailyWorkPeriodRecord**

Поколение 1:

Информация, съхранена в бордово устройство и отнасяща се за местоположение в началото или края на дневен период на работа на водач (изискване 087 от приложение 1Б и изисквания 108 и 110 от приложение 1В).

```
VuPlaceDailyWorkPeriodRecord ::= SEQUENCE {
   fullCardNumber                      FullCardNumber,
   placeRecord                         PlaceRecord
}
```

fullCardNumber е типът карта на водач, държавата членка, която издава картата, и номерът на картата.

placeRecord съдържа данни относно въведеното местоположение.

Поколение 2:

Информация, съхранена в бордово устройство и отнасяща се за местоположение в началото или края на дневен период на работа на водач (изискване 087 от приложение 1Б и изисквания 108 и 110 от приложение 1В).

```
VuPlaceDailyWorkPeriodRecord ::= SEQUENCE {
   fullCardNumberAndGeneration         FullCardNumberAndGeneration,
   placeRecord                         PlaceRecord
}
```

Вместо fullCardNumber структурата на данните от поколение 2 използва следния елемент от данни:

fullCardNumberAndGeneration е типът карта, държавата членка, която я издава, нейният номер на карта и поколението, съхранени на картата.

2.220. **VuPlaceDailyWorkPeriodRecordArray**

Поколение 2:

Информация, съхранена в бордово устройство и отнасяща се до местоположенията в началото или края на дневен период на работа на водачи (изисквания 108 и 110 от приложение 1В).

```
VuPlaceDailyWorkPeriodRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       VuPlaceDailyWorkPeriodRecord
}
```

recordType указва типа запис (VuPlaceDailyWorkPeriodRecord). **Присвояване на стойност**: вж. RecordType.

recordSize е размерът на VuPlaceDailyWorkPeriodRecord в байтове.

noOfRecords е броят на записите в набора от записи.

records е набор записи във връзка с местоположението.

2.221. **VuPrivateKey**

Поколение 1:

Частен ключ на бордово устройство.

```
VuPrivateKey ::= RSAKeyPrivateExponent
```

2.222. **VuPublicKey**

Поколение 1:

Публичен ключ на бордово устройство.

```
VuPublicKey ::= PublicKey
```

2.223. **VuSerialNumber**

Сериен номер на бордовото устройство (изискване 075 от приложение 1Б и изискване 93 от приложение 1В).

```
VuSerialNumber ::= ExtendedSerialNumber
```

2.224. **VuSoftInstallationDate**

Дата на инсталиране на версията на софтуера на бордовото устройство.

```
VuSoftInstallationDate ::= TimeReal
```

Присвояване на стойност: не е указана.

2.225. **VuSoftwareIdentification**

Информация, съхранена в бордово устройство и отнасяща се за инсталирания софтуер.

```
VuSoftwareIdentification ::= SEQUENCE {
   vuSoftwareVersion                    VuSoftwareVersion,
   vuSoftInstallationDate               VuSoftInstallationDate
}
```

vuSoftwareVersion е номерът на версията на софтуера на бордовото устройство.

vuSoftInstallationDate е датата на инсталиране на версията на софтуера.

2.226. **VuSoftwareVersion**

Номер на версията на софтуера на бордовото устройство.

```
VuSoftwareVersion ::= IA5String(SIZE(4))
```

Присвояване на стойност: не е указана.

2.227. **VuSpecificConditionData**

Поколение 1:

Информация, съхранена в бордово устройство и отнасяща се до специфични условия.

```
VuSpecificConditionData ::= SEQUENCE {
   noOfSpecificConditionRecords         INTEGER(0..2^16-1)
   specificConditionRecords             SET SIZE (noOfSpecificConditionRecords) OF
                                        SpecificConditionRecord
}
```

noOfSpecificConditionRecords е броят на записите, посочени в набора от specificConditionRecords.

specificConditionRecords е набор записи във връзка със специфични условия.

2.228. **VuSpecificConditionRecordArray**

Поколение 2:

Информация, съхранена в бордово устройство и отнасяща се за специфични условия (изискване 130 от приложение 1B).

```
VuSpecificConditionRecordArray ::= SEQUENCE {
   recordType                           RecordType,
   recordSize                           INTEGER(1..65535),
   noOfRecords                          INTEGER(0..65535),
   records                              SET SIZE(noOfRecords) OF
                                        SpecificConditionRecord
}
```

recordType указва типа запис (SpecificConditionRecord). **Присвояване на стойност**: вж. RecordType.

recordSize е размерът на SpecificConditionRecord в байтове.

noOfRecords е броят на записите в набора от записи.

records е набор от записи във връзка със специфични условия.

2.229. **VuTimeAdjustmentData**

Поколение 1:

Информация, съхранена в бордово устройство и отнасяща се за сверяването на часовника, извършено извън рамките на редовното калибриране (изискване 101 от приложение 1Б).

```
VuTimeAdjustmentData ::= SEQUENCE {
   noOfVuTimeAdjRecords                INTEGER(0..6),
   vuTimeAdjustmentRecords             SET SIZE(noOfVuTimeAdjRecords) OF
                                       VuTimeAdjustmentRecord
}
```

noOfVuTimeAdjRecords е броят на записите в vuTimeAdjustmentRecords**.**

vuTimeAdjustmentRecords е набор записи относно сверяването на часовника.

2.230. **VuTimeAdjustmentGNSSRecord**

Поколение 2:

Информация, съхранена в бордово устройство и отнасяща се за сверяването на часовника въз основа на данните за времето от GNSS (изисквания 124 и 125 от приложение 1В).

```
VuTimeAdjustmentGNSSRecord ::= SEQUENCE {
   oldTimeValue                        TimeReal,
   newTimeValue                        TimeReal
}
```

oldTimeValue, newTimeValue са старите и новите стойности на датата и часа.

2.231. **VuTimeAdjustmentGNSSRecordArray**

Поколение 2:

Информация, съхранена в бордово устройство и отнасяща се за сверяването на часовника въз основа на данните за времето от GNSS (изисквания 124 и 125 от приложение 1В).

```
VuTimeAdjustmentGNSSRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       VuTimeAdjustmentGNSSRecord
}
```

recordType указва типа запис (VuTimeAdjustmentGNSSRecord). **Присвояване на стойност**: вж. RecordType.

recordSize е размерът на VuTimeAdjustmentGNSSRecord в байтове.

noOfRecords е броят на записите в набора от записи.

records е набор от записи за сверяване на часовника по GNSS.

2.232. **VuTimeAdjustmentRecord**

Информация, съхранена в бордово устройство и отнасяща се за сверяването на часовника, извършено извън рамките на редовното калибриране (изискване 101 от приложение 1Б и изисквания 124 и 125 от приложение 1В).

Поколение 1:

```
VuTimeAdjustmentRecord ::= SEQUENCE {
   oldTimeValue                         TimeReal,
   newTimeValue                         TimeReal,
   workshopName                         Name,
   workshopAddress                      Address,
   workshopCardNumber                   FullCardNumber
}
```

oldTimeValue, newTimeValue са старите и новите стойности на датата и часа.

workshopName, workshopAddress са наименованието и адресът на сервиза.

workshopCardNumber идентифицира картата за монтаж и настройки, използвана за сверяване на часовника.

Поколение 2:

```
VuTimeAdjustmentRecord ::= SEQUENCE {
   oldTimeValue                         TimeReal,
   newTimeValue                         TimeReal,
   workshopName                         Name,
   workshopAddress                      Address,
   workshopCardNumberAndGeneration      FullCardNumberAndGeneration
}
```

Вместо workshopCardNumber структурата на данните от поколение 2 използва следния елемент от данни.

workshopCardNumberAndGeneration идентифицира картата за монтаж и настройки, включително поколението ѝ, използвана за сверяване на часовника.

2.233. **VuTimeAdjustmentRecordArray**

Поколение 2:

Информация, съхранена в бордово устройство и отнасяща се за сверяването на часовника, извършено извън рамките на редовното калибриране (изисквания 124 и 125 от приложение 1В).

```
VuTimeAdjustmentRecordArray ::= SEQUENCE {
   recordType                           RecordType,
   recordSize                           INTEGER(1..65535),
   noOfRecords                          INTEGER(0..65535),
   records                              SET SIZE(noOfRecords) OF
                                        VuTimeAdjustmentRecord
}
```

recordType указва типа запис (VuTimeAdjustmentRecord). **Присвояване на стойност**: вж. RecordType.

recordSize е размерът на VuTimeAdjustmentRecord в байтове.

noOfRecords е броят на записите в набора от записи.

records е набор от записи за сверяване на часовника.

2.234. **WorkshopCardApplicationIdentification**

Информация, съхранена на карта за монтаж и настройки и отнасяща се за идентификация на приложението на картата (изисквания 307 и 330 от приложение 1B).

Поколение 1:

```
WorkshopCardApplicationIdentification ::= SEQUENCE {
   typeOfTachographCardId               EquipmentType,
   cardStructureVersion                 CardStructureVersion,
   noOfEventsPerType                    NoOfEventsPerType,
   noOfFaultsPerType                    NoOfFaultsPerType,
   activityStructureLength              CardActivityLengthRange,
   noOfCardVehicleRecords               NoOfCardVehicleRecords,
   noOfCardPlaceRecords                 NoOfCardPlaceRecords,
   noOfCalibrationRecords               NoOfCalibrationRecords
}
```

typeOfTachographCardId обозначава използвания тип карта.

cardStructureVersion указва версията на структурата, приложена в картата.

noOfEventsPerType е броят на събитията от всеки тип, които картата може да запише.

noOfFaultsPerType е броят на неизправностите от всеки тип, които картата може да запише.

activityStructureLength указва броя на байтовете, които могат да се използват за съхранение на записите за дейността.

noOfCardVehicleRecords е броят на записите за превозното средство, които картата може да съдържа.

noOfCardPlaceRecords е броят на местоположенията, които картата може да запише.

noOfCalibrationRecords е броят на записите за калибрированията, които картата може да съхрани.

Поколение 2:

```
WorkshopCardApplicationIdentification ::= SEQUENCE {
   typeOfTachographCardId               EquipmentType,
   cardStructureVersion                 CardStructureVersion,
   noOfEventsPerType                    NoOfEventsPerType,
   noOfFaultsPerType                    NoOfFaultsPerType,
   activityStructureLength              CardActivityLengthRange,
   noOfCardVehicleRecords               NoOfCardVehicleRecords,
   noOfCardPlaceRecords                 NoOfCardPlaceRecords,
   noOfCalibrationRecords               NoOfCalibrationRecords,
   noOfGNSSCDRecords                    NoOfGNSSCDRecords,
   noOfSpecificConditionRecords         NoOfSpecificConditionRecords
}
```

В допълнение към поколение 1 се използват следните елементи от данни:

noOfGNSSCDRecords е броят на записите за непрекъснато управление по GNSS, които картата може да съхранява.

noOfSpecificConditionRecords е броят на записите за специфични условия, които картата може да съхранява.

2.235. **WorkshopCardCalibrationData**

Информация, съхранена на карта за монтаж и настройки и отнасяща се до определена сервизна дейност, извършена с картата (изисквания 314, 316, 337 и 339 от приложение 1B).

```
WorkshopCardCalibrationData ::= SEQUENCE {
   calibrationTotalNumber              INTEGER(0 .. 2^16-1),
   calibrationPointerNewestRecord      INTEGER(0 .. NoOfCalibrationRecords-1),
   calibrationRecords                  SET SIZE(NoOfCalibrationRecords) OF
                                       WorkshopCardCalibrationRecord
}
```

calibrationTotalNumber е общият брой на извършените с картата калибрирания.

calibrationPointerNewestRecord е индексът на последния актуализиран запис за калибриране.

Присвояване на стойност: число, съответстващо на номератора на запис за калибриране, като се започва с 0 за първия случай на запис за калибриране в структурата.

calibrationRecords е набор от записи, съдържащи информация за калибрирането и/или сверяването на часовника.

2.236. **WorkshopCardCalibrationRecord**

Информация, съхранена на карта за монтаж и настройки и отнасяща се за калибриране, извършено с картата (изисквания 314 и 337 от приложение 1B).

Поколение 1:

```
WorkshopCardCalibrationRecord ::= SEQUENCE {
   calibrationPurpose                  CalibrationPurpose,
   vehicleIdentificationNumber         VehicleIdentificationNumber,
   vehicleRegistration                 VehicleRegistrationIdentification,
   wVehicleCharacteristicConstant      W-VehicleCharacteristicConstant,
   kConstantOfRecordingEquipment       K-ConstantOfRecordingEquipment,
   lTyreCircumference                  L-TyreCircumference,
   tyreSize                            TyreSize,
   authorisedSpeed                     SpeedAuthorised,
   oldOdometerValue                    OdometerShort,
   newOdometerValue                    OdometerShort,
   oldTimeValue                        TimeReal,
   newTimeValue                        TimeReal,
   nextCalibrationDate                 TimeReal,
   vuPartNumber                        VuPartNumber,
   vuSerialNumber                      VuSerialNumber,
   sensorSerialNumber                  SensorSerialNumber
}
```

calibrationPurpose е целта на калибрирането.

vehicleIdentificationNumber е VIN.

vehicleRegistration съдържа VRN и регистриращата държава членка.

wVehicleCharacteristicConstant е характеристичният коефициент на превозното средство.

kConstantOfRecordingEquipment е константата на уреда за регистриране на данните за движението.

lTyreCircumference е действителната обиколка на колелата.

tyreSize е обозначение на размерите на гумите, монтирани на превозното средство.

authorisedSpeed е разрешената максимална скорост на превозното средство.

oldOdometerValue и newOdometerValue са старата и новата стойност, отчетени от километражния брояч.

oldTimeValue, newTimeValue са старите и новите стойности на датата и часа.

nextCalibrationDate е датата на следващото калибриране на типа в CalibrationPurpose, което оправомощеният инспектиращ орган трябва да извърши.

vuPartNumber, **vuSerialNumber** и **sensorSerialNumber** са елементи от данни, необходими за идентификация на уредите за регистриране на данните за движението.

Поколение 2:

```
WorkshopCardCalibrationRecord ::= SEQUENCE {
   calibrationPurpose                  CalibrationPurpose,
   vehicleIdentificationNumber         VehicleIdentificationNumber,
   vehicleRegistration                 VehicleRegistrationIdentification,
   wVehicleCharacteristicConstant      W-VehicleCharacteristicConstant,
   kConstantOfRecordingEquipment       K-ConstantOfRecordingEquipment,
   lTyreCircumference                  L-TyreCircumference,
   tyreSize                            TyreSize,
   authorisedSpeed                     SpeedAuthorised,
   oldOdometerValue                    OdometerShort,
   newOdometerValue                    OdometerShort,
   oldTimeValue                        TimeReal,
   newTimeValue                        TimeReal,
   nextCalibrationDate                 TimeReal,
   vuPartNumber                        VuPartNumber,
   vuSerialNumber                      VuSerialNumber,
   sensorSerialNumber                  SensorSerialNumber,
   sensorGNSSSerialNumber              SensorGNSSSerialNumber,
   rcmSerialNumber                     RemoteCommunicationModuleSerialNumber,
   sealDataCard                        SealDataCard
}
```

В допълнение към поколение 1 се използват следните елементи от данни:

sensorGNSSSerialNumber идентифицира външното устройство за GNSS.

rcmSerialNumber идентифицира модула за връзка от разстояние.

sealDataVu дава информация за пломбите, поставени върху различните компоненти на превозното средство.

2.237. **WorkshopCardHolderIdentification**

Информация, съхранена на карта за монтаж и настройки и отнасяща се за идентификация на титуляря на картата (изисквания 311 и 334 от приложение 1B).

```
WorkshopCardHolderIdentification ::= SEQUENCE {
   workshopName                        Name,
   workshopAddress                     Address,
   cardHolderName                      HolderName,
   cardHolderPreferredLanguage         Language
}
```

workshopName е наименованието на сервиза на титуляря на картата.

workshopAddress е адресът на сервиза на титуляря на картата.

cardHolderName е фамилията и името (и презимето) на титуляря (например името на механика).

cardHolderPreferredLanguage е предпочитаният език на титуляря на картата.

2.238. **WorkshopCardPIN**

Персонален идентификационен номер на картата за монтаж и настройки (изисквания 309 и 332 от приложение 1B).

```
WorkshopCardPIN ::= IA5String(SIZE(8))
```

Присвояване на стойност: PIN, известен на титуляря на картата, запълнен отдясно със серия от байтове „FF“, която може да съдържа до 8 байта.

2.239. **W-VehicleCharacteristicConstant**

Характеристичен коефициент на превозното средство (определение к).

```
W-VehicleCharacteristicConstant ::= INTEGER(0..2^16-1))
```

Присвояване на стойност: импулси на километър в работния диапазон от 0 до 64 255 имп./km.

2.240. **VuPowerSupplyInterruptionRecord**

Поколение 2:

Информация, съхранена в бордово устройство и отнасяща се до събитията „прекъсване на електрическото захранване“ (изискване 117 от приложение 1B).

```
VuPowerSupplyInterruptionRecord ::= SEQUENCE {
   eventType                          EventFaultType,
   eventRecordPurpose                 EventFaultRecordPurpose,
   eventBeginTime                     TimeReal,
   eventEndTime                       TimeReal,
   cardNumberAndGenDriverSlotBegin    FullCardNumberAndGeneration,
   cardNumberAndGenDriverSlotEnd      FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotBegin  FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotEnd    FullCardNumberAndGeneration,
   similarEventsNumber                SimilarEventsNumber
}
```

eventType е типът на събитието.

eventRecordPurpose е целта на записване на събитието.

eventBeginTime е датата и часът на начало на събитието.

eventEndTime е датата и часът на край на събитието.

cardNumberAndGenDriverSlotBegin идентифицира картата, включително поколението ѝ, вкарана в процепа за водача в началото на събитието.

cardNumberAndGenDriverSlotEnd идентифицира картата, включително поколението ѝ, вкарана в процепа за водача в края на събитието.

cardNumberAndGenCodriverSlotBegin идентифицира картата, включително поколението ѝ, вкарана в процепа за втория водач в началото на събитието.

cardNumberAndGenCodriverSlotEnd идентифицира картата, включително поколението ѝ, вкарана в процепа за втория водач в края на събитието.

similarEventsNumber е броят на сходните събития през същия ден.

2.241. **VuPowerSupplyInterruptionRecordArray**

Поколение 2:

Информация, съхранена в бордово устройство и отнасяща се за събитията „прекъсване на електрическото захранване“ (изискване 117 от приложение 1B).

```
VuPowerSupplyInterruptionRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       VuPowerSupplyInterruptionRecord
}
```

recordType указва типа запис (VuPowerSupplyInterruptionRecord). **Присвояване на стойност**: вж. RecordType.

recordSize е размерът на VuPowerSupplyInterruptionRecord в байтове.

noOfRecords е броят на записите в набора от записи.

records е набор от записи за събития „прекъсване на електрическото захранване“.

2.242. **VuSensorExternalGNSSCoupledRecordArray**

Поколение 2:

Набор от SensorExternalGNSSCoupledRecord плюс метаданните, използвани в протокола за изтегляне на данни.

```
VuSensorExternalGNSSCoupledRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       SensorExternalGNSSCoupledRecord
}
```

recordType указва типа запис (SensorExternalGNSSCoupledRecord). **Присвояване на стойност**: вж. RecordType.

recordSize е размерът на SensorExternalGNSSCoupledRecord в байтове.

noOfRecords е броят на записите в набора от записи.

records е набор от Sensor External GNSS Coupled records.

2.243. **VuSensorPairedRecordArray**

Поколение 2:

Набор от SensorPairedRecord плюс метаданните, използвани в протокола за изтегляне на данни.

```
VuSensorPairedRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF SensorPairedRecord
}
```

recordType указва типа запис (SensorPairedRecord). **Присвояване на стойност**: вж. RecordType.

recordSize е размерът на SensorPairedRecord в байтове.

noOfRecords е броят на записите в набора от записи.

records е набор от записи за свързани датчици.

3. ОПРЕДЕЛЕНИЯ НА ДИАПАЗОНИТЕ ОТ СТОЙНОСТИ И РАЗМЕРИ

Определяне на стойностите на променливите, използвани в определенията в параграф 2.

```
TimeRealRange ::= 2^32-1
```

4. НАБОР ОТ СИМВОЛИ

Низовете IA5 се състоят от ASCII символи, както е определено в ISO/IEC 8824-1. За по-голяма четливост и за да се улесни указването на символите, определянето на стойностите се дава по-долу. В случай на различие прилагането на ISO/IEC 8824-1 има предимство пред настоящата информация.

```
  ! " # $ % & ' ( ) * + , - . / 0 1 2 3 4 5 6 7 8 9 : ; < = > ?
@ A B C D E F G H I J K L M N O P Q R S T U V W X Y Z [ \ ] ^ _
` a b c d e f g h i j k l m n o p q r s t u v w x y z { | } ~
```

В други низове от символи (Address, Name, VehicleRegistrationNumber) се използват освен това символи с десетични кодове в диапазона 161 — 255 от следните 8-битови стандартни набори от символи, указани от номера на кодовата страница: Стандартен набор от символи	Кодова страница (десетична)
ISO/IEC 8859-1 латиница 1 — Западна Европа	1
ISO/IEC 8859-2 латиница 2 — Централна Европа	2
ISO/IEC 8859-3 латиница 3 — Южна Европа	3
ISO/IEC 8859-5 латиница/кирилица	5
ISO/IEC 8859-7 латиница/гръцка азбука	7
ISO/IEC 8859-9 латиница 5/турска азбука	9
ISO/IEC 8859-13 латиница 7 — Балтийски регион	13
ISO/IEC 8859-15 латиница 9	15
ISO/IEC 8859-16 латиница 10 — Югоизточна Европа	16
KOI8-R латиница/кирилица	80
KOI8-U латиница/кирилица	85

5. КОДИРАНЕ

Ако се прилагат правилата за кодиране ASN.1, всички определени типове данни трябва да се кодират съгласно приведения в съответствие вариант на стандарт ISO/IEC 8825-2.

6. ИДЕНТИФИКАТОРИ НА ОБЕКТИ И ИДЕНТИФИКАТОРИ НА ПРИЛОЖЕНИЯ

6.1. **Идентификатори на обекти**

Идентификаторите на обекти (ИО), посочени в тази глава, се прилагат само към поколение 2. Тези ИО са определени в TR-03110-3 и тук са повторени само за пълнота. Тези ИО се съдържат в поддървото на bsi-de:

```
bsi-de OBJECT IDENTIFIER ::= {
   itu-t(0) identified-organization(4) etsi(0)
   reserved(127) etsi-identified-organization(0) 7
}
```

Идентификатори за протокол за удостоверяване на бордово устройство

```
id-TA         OBJECT IDENTIFIER ::= {bsi-de protocols(2) smartcard(2) 2}

id-TA-ECDSA                OBJECT IDENTIFIER ::= {id-TA 2}

id-TA-ECDSA-SHA-256 OBJECT IDENTIFIER ::= {id-TA-ECDSA 3}

id-TA-ECDSA-SHA-384 OBJECT IDENTIFIER ::= {id-TA-ECDSA 4}

id-TA-ECDSA-SHA-512 OBJECT IDENTIFIER ::= {id-TA-ECDSA 5}
```

Пример: да предположим, че удостоверяването на бордовото устройство трябва да се извърши със SHA-384, тогава идентификаторът на обект, който трябва да се използва, е (в ASN.1) `bsi-de protocols(2) smartcard(2) 2 2 4`. Стойността на този идентификатор на обект в точковата нотация е `0.4.0.127.0.7.2.2.2.2.4`.

	Точкова нотация	Байтова нотация
id-TA-ECDSA-SHA-256	0.4.0.127.0.7.2.2.2.2.3	‘04 00 7F 00 07 02 02 02 02 03’
id-TA-ECDSA-SHA-384	0.4.0.127.0.7.2.2.2.2.4	‘04 00 7F 00 07 02 02 02 02 04’
id-TA-ECDSA-SHA-512	0.4.0.127.0.7.2.2.2.2.5	‘04 00 7F 00 07 02 02 02 02 05’

Идентификатори за протокол за удостоверяване на чип

```
id-CA         OBJECT IDENTIFIER ::= {bsi-de protocols(2) smartcard(2) 3}

id-CA-ECDH                          OBJECT IDENTIFIER ::= {id-CA 2}

id-CA-ECDH-AES-CBC-CMAC-128         OBJECT IDENTIFIER ::= {id-CA-ECDH 2}

id-CA-ECDH-AES-CBC-CMAC-192         OBJECT IDENTIFIER ::= {id-CA-ECDH 3}

id-CA-ECDH-AES-CBC-CMAC-256         OBJECT IDENTIFIER ::= {id-CA-ECDH 4}
```

Пример: да предположим, че удостоверяването на чипа трябва да се извърши чрез използване на алгоритъм ECDH, водещо до дължина на ключа на сесията AES от 128 бита. Впоследствие този ключ на сесия ще се използва в работния режим CBC, за да се осигури поверителността на данните, а с алгоритъма CMAC — автентичността на данните. Следователно идентификаторът на обект, който трябва да се използва, е (в ASN.1) `bsi-de protocols(2) smartcard(2) 3 2 2`. Стойността на този идентификатор на обект в точковата нотация е `0.4.0.127.0.7.2.2.3.2.2`.

	Точкова нотация	Байтова нотация
id-CA-ECDH-AES-CBC-CMAC-128	0.4.0.127.0.7.2.2.3.2.2	‘04 00 7F 00 07 02 02 03 02 02’
id-CA-ECDH-AES-CBC-CMAC-192	0.4.0.127.0.7.2.2.3.2.3	‘04 00 7F 00 07 02 02 03 02 03’
id-CA-ECDH-AES-CBC-CMAC-256	0.4.0.127.0.7.2.2.3.2.4	‘04 00 7F 00 07 02 02 03 02 04’

6.2. Идентификатори на приложения

Поколение 2:

Идентификаторът на приложение (ИП) за външното устройство за GNSS (поколение 2) е даден от ‘FF 44 54 45 47 4D’. Това е ИП, който е обект на права на собственост, съгласно ISO/IEC 7816-4.

Забележка: последните пет байта кодират DTEGM за интелигентно тахографско външно устройство за GNSS.

Идентификаторът на приложение на тахографска карта от поколение 2 е даден от ‘FF 53 4D 52 44 54’. Това е ИП, който е обект на права на собственост, съгласно ISO/IEC 7816-4.

Допълнение 2

СПЕЦИФИКАЦИЯ НА ТАХОГРАФСКИТЕ КАРТИ

СЪДЪРЖАНИЕ

1. ВЪВЕДЕНИЕ

1.1. **Съкращения**

За целите на настоящото допълнение се използват следните съкращения.

AC	Access conditions (условия за достъп)
AES	Advanced Encryption Standard („Усъвършенстван стандарт за криптиране“)
AID	Application Identifier („Идентификатор на приложението“)
ALW	Always („Винаги“)
APDU	Application Protocol Data Unit (structure of a command) („Единица данни по приложния протокол“ — структура на команда)
ATR	Answer To Reset („Отговор на инициализиране“)
AUT	Authenticated („Удостоверен за автентичност“)
C6, C7	Contacts No 6 and 7 of the card as described in ISO/IEC 7816-2 („Контакти номера 6 и 7 на картата са описани съгласно стандарт ISO/IEC 7816-2“)
cc	clock cycles (тактови цикли)
CHV	Card Holder Verification information (информация за проверка самоличността на титуляря на картата)
CLA	Class byte of an APDU command (байт за определяне на класа на APDU команда)
DSRC	Dedicated Short Range Communication (специализирана връзка или специализирана съобщителна система с малък обсег на действие)
DF	Dedicated File („Специализиран файл“) Един DF може да съдържа други файлове (елементарни (EF) или специализирани)
ECC	Elliptic Curve Cryptography („Криптография по елиптична крива“)
EF	Elementary File („Елементарен файл“)
etu	elementary time unit („елементарна времева единица“)
G1	Generation 1 („Поколение 1“)
G2	Generation 2 („Поколение 2“)
IC	Integrated Circuit („Вграден чип“)
ICC	Integrated Circuit Card („Карта с вграден чип“)
ID	Identifier (идентификатор)
IFD	Interface Device (интерфейсно устройство)
IFS	Information Field Size („Дължина на зоната за информация“)
IFSC	Information Field Size for the card („Дължина на зоната за информация, запазена за картата“)

IFSD	Information Field Size Device (for the Terminal) („Дължина на зоната за информация, запазена за крайното устройство“)
INS	Instruction byte of an APDU command („Байт за инструкция на APDU команда“)
Lc	Length of the input data for a APDU command (дължина на входните данни за APDU команда)
Le	Length of the expected data (output data for a command) (дължина на очакваните данни (изходни данни, отнасящи се до определена команда)
MF	Master File (root DF) („Главен файл“ (специализиран файл, намиращ се в кореновата директория)
NAD	Node Address used in T = 1 protocol (възлов адрес, използван в протокол T = 1)
NEV	Never („Никога“)
P1-P2	Parameter bytes (байтове за параметри)
PIN	Personal Identification Number („Персонален идентификационен номер“)
PRO SM	Protected with secure messaging („Предпазен посредством защитен обмен на съобщения“)
PTS	Protocol Transmission Selection („Избор на протокола за предаване на данни“)
RFU	Reserved for Future Use („Запазено за бъдеща употреба“)
RST	Reset (of the card) („Инициализиране“ (на картата)
SFID	Short EF Identifier („Кратък идентификатор на елементарен файл“)
SM	Secure Messaging (защитен обмен на съобщения)
SW1-SW2	Status bytes (байтове за състоянието)
TS	Initial ATR character (начален символ на отговор на инициализиране)
VPP	Programming Voltage (напрежение при програмиране)
VU	Vehicle Unit („Бордово устройство“)
XXh	Стойност XX в шестнадесетична бройна система
‘XXh’	Стойност XX в шестнадесетична бройна система
||	Символ за конкатенация 03||04=0304

1.2. **Позовавания**

В настоящото допълнение се използват позовавания на следните стандарти:

ISO/IEC 7816-2 Идентификационни карти. Карти с интегрални схеми. Част 2: Размери и разположение на контактите. ISO/IEC 7816-2:2007.

ISO/IEC 7816-3 Идентификационни карти. Карти с интегрална(и) схема(и) с контакти. Част 3: Електронни сигнали и протоколи за предаване. ISO/IEC 7816-3:2006.

ISO/IEC 7816-4 Идентификационни карти. Карти с интегрална(и) схема(и) с контакти. Част 4: Организация, сигурност и команди за обмен. ISO/IEC 7816-4:2013 + Cor 1: 2014.

ISO/IEC 7816-6 Идентификационни карти. Карти с интегрални схеми. Част 6: Вътрешно-отраслови елементи от данни за взаимен обмен. ISO/IEC 7816-6:2004 + Cor 1: 2006.

ISO/IEC 7816-8 Идентификационни карти. Карти с интегрални схеми. Част 8: Команди за операции по сигурността. ISO/IEC 7816-8:2004.

ISO/IEC 9797-2 Информационни технологии. Техники за сигурност. Кодове за удостоверяване на съобщението (MACs). Част 2: Механизми, използващи специализирана хеш-функция. ISO/IEC 9797-2:2011

2. ЕЛЕКТРИЧЕСКИ И ФИЗИЧЕСКИ ХАРАКТЕРИСТИКИ

TCS_01 Всички електронни сигнали трябва да са в съответствие със стандарта ISO/IEC 7816-3, освен ако е указано друго.

TCS_02 Местоположението и размерите на контактите на картата трябва да са в съответствие със стандарта ISO/IEC 7816-2.

2.1. **Захранващо напрежение и потребление на електрически ток**

TCS_03 Картата трябва да функционира съгласно спецификациите с потребление в границите, определени в стандарта ISO/IEC 7816-3.

TCS_04 Картата функционира със захранващо напрежение Vcc = 3 V (+/– 0,3 V) или Vcc = 5 V (+/– 0,5 V).

Изборът на напрежението се извършва съгласно ISO/IEC 7816-3.

2.2. **Напрежение при програмиране V_{pp}**

TCS_05 За картата не се изисква върху краче C6 да се прилага напрежение при програмиране. Предвижда се крачето C6 да не е свързано в интерфейсно устройство (IFD). Контакт C6 може да бъде свързан към V_{cc} в картата, но не трябва да се свързва на маса. Това напрежение не подлежи на никакво интерпретиране.

2.3. **Генериране на тактове и тактова честота**

TCS_06 Картата трябва да функционира в честотния обхват 1—5 MHz и може да поддържа по-високи честоти. По време на една и съща сесия тактовата честота може да варира в рамките на ± 2 %. Тактовата честота се генерира от бордовото устройство, а не от самата карта. Коефициентът на запълване може да варира между 40 и 60 %.

TCS_07 Възможно е спирането на външния тактов генератор при условията, записани във файла EF ICC на картата. Чрез първия байт от тялото на файла EF ICC се програмират условията за режима Clockstop:

Долно равнище (L)	Горно равнище (H)		
Бит 3	Бит 2	Бит 1	
0	0	1	Clockstop е разрешен, няма предпочитано равнище
0	1	1	Clockstop е разрешен, с предпочитание към горното равнище
1	0	1	Clockstop е разрешен, с предпочитание към долното равнище
0	0	0	Clockstop не е разрешен
0	1	0	Clockstop е разрешен само на горното равнище
1	0	0	Clockstop е разрешен само на долното равнище

Битове 4—8 не се използват.

2.4. **Входно/изходен (I/O) контакт**

TCS_08 Входно/изходният контакт C7 се използва за приемането и предаването на данни, идващи от или предназначени за интерфейсното устройство (IFD). По време на работа в режим на предаване е или картата, или интерфейсното устройство, но не и двете едновременно. Ако и двете са в режим на предаване, това не трябва да причинява повреждане на картата. Когато картата не предава повече, тя преминава в режим на приемане.

2.5. **Състояния на картата**

TCS_09 Картата функционира в две състояния, когато е приложено захранващото напрежение:

активно състояние, докато изпълнява команди или се свързва с цифрово устройство,

пасивно състояние през останалото време; в това състояние картата трябва да запазва всички запаметени данни.

3. ХАРДУЕР И ОБМЕН НА ДАННИ

3.1. **Въведение**

В настоящия параграф се описват минималните функционални възможности, които трябва да притежават тахографските карти и бордовите устройства (VU), за да се гарантира правилно функциониране и оперативна съвместимост.

Тахографските карти трябва също така да са в съответствие с действащите стандарти ISO/IEC (и по-специално ISO/IEC 7816) в максималната възможна степен. Въпреки това се дава подробно описание на командите и протоколите, за да се посочат някои ограничения в използването или евентуални различия. Описаните команди са в пълно съответствие с посочените стандарти, освен ако е указано друго.

3.2. **Протокол за предаване на данни**

TCS_10 Протоколът за предаване на данни трябва да е в съответствие със стандарта ISO/IEC 7816-3 за T = 0 и T = 1. По-специално бордовото устройство трябва да бъде в състояние да разпознава удълженията на времето на изчакване, които му изпраща картата.

3.2.1 *Протоколи*

TCS_11 Картата трябва да може да предоставя и двата протокола T=0 и T=1. Освен това тя може да поддържа допълнителни контактно-ориентирани протоколи.

TCS_12 **T=0** е протоколът по подразбиране; така че е необходима команда **PTS** за преминаване към протокола **T=1**.

TCS_13 Устройствата трябва да могат да използват **прякото условие за връзка**, което съдържат тези два протокола: следователно прякото условие за връзка е задължително за картата.

TCS_14 Байтът **„Дължина на зоната за информация, запазена за картата“ (IFSC)** се представя при ATR („Отговор на инициализиране“) в символа TA3. Тази стойност трябва да е най-малко ‘F0h’ (= 240 байта).

Прилагат се следните ограничения за протоколите:

TCS_15 **T=0**

— Интерфейсното устройство трябва да може да възприема отговор по I/O след предния фронт на сигнала относно RST от 400 тактови цикли (cc).

— Интерфейсното устройство трябва да бъде в състояние да чете символите, разделени с 12 etu.

— Интерфейсното устройство трябва да бъде в състояние да разпознава грешен символ и неговото повторение, ако са разделени с 13 etu. В случай на откриване на грешен символ, сигналът за грешка (Error) може да се подаде по I/O в интервал от 1 до 2 etu. Устройството трябва да бъде в състояние да понася закъснение от 1 etu.

— Интерфейсното устройство трябва да бъде в състояние да приема ATR от 33 байта (TS+32).

— Ако TC1 присъства в ATR, трябва да се предвиди допълнително време за изчакване за символите, изпратени от интерфейсното устройство, въпреки че символите, изпратени от картата, все още могат да бъдат разделени с 12 etu. Това важи и за символа ACK („Удостоверяване на приемане“), изпратен от картата след издаване от интерфейсното устройство на символ P3.

— Интерфейсното устройство отчита символа NUL, издаден от картата.

— Интерфейсното устройство трябва да приема режима на допълване за удостоверяване на приемането на данни.

— Командата за получаване на отговор (get-response) не може да се използва в режим на обединяване на данните за получаване на блокове от данни, чиято дължина би могла да надвиши 255 байта.

TCS_16 **T=1**

— Байт NAD: не се използва (за NAD се задава „00“).

— S-block ABORT: не се използва.

— Грешка в състоянието на VPP, засягаща S-block: не се използва.

— Общата дължина на верижно свързаните данни (chaining length) в едно поле за данни не трябва да надвишава 255 байта (за да се поддържа от IFD).

— Information Field Size Device (IFSD) се указва от IFD непосредствено след ATR: IFD предава заявката за дължината на зоната за информация (IFS) на S-Block след ATR и картата отговаря с IFS на S-Block. Препоръчва се стойността на IFSD да е 254 байта.

— Картата не подава искане за промяна на IFS.

3.2.2 *ATR*

TCS_17 Устройството проверява байтовете на ATR съгласно стандарта ISO/IEC 7816-3. Не се проверяват символите, отбелязващи историята на ATR.

Пример за базов двупротоколен ATR съгласно стандарта ISO/IEC 7816-3.

Символ	Стойност	Забележки
TS	‘3Bh’	Указва пряко условие за връзка.
T0	‘85h’	TD1 наличен; наличие на 5 байта, отбелязващи историята.
TD1	‘80h’	TD2 наличен; използва се T=0
TD2	‘11h’	TA3 наличен; използва се T=1
TA3	‘XXh’ (най-малко ‘F0h’)	Дължина на зоната за информация, запазена за картата (IFSC)
TH1 до TH5	‘XXh’	Символи, използвани за отбелязване на историята
TCK	‘XXh’	Контролен символ (изключително ИЛИ)

TCS_18 След Answer To Reset (ATR) главният файл (MF) се избира по подразбиране и става текуща директория.

3.2.3 *PTS*

TCS_19 Протоколът по подразбиране е T=0. За да се зададе протоколът T=1, устройството изпраща на картата команда PTS (известна и като PPS).

TCS_20 Тъй като и двата протокола T=0 и T=1 са задължителни за картата, задължителна е и базовата команда PTS за превключване между протоколите.

PTS може да се използва, както е посочено в ISO/IEC 7816-3, за превключване към по-висока скорост на предаване на данни отколкото подразбиращата се, предложена от картата в ATR, ако има такава (байт TA(1).

Използването на по-висока скорост на предаване на данни не е задължително за картата.

TCS_21 Ако се поддържа само подразбиращата се скорост на предаване на данни (или ако избраната скорост на предаване на данни не се поддържа), картата отговаря на PTS правилно съгласно стандарта ISO/IEC 7816-3, като изпуска байта PPS1.

Следват примери за базова команда PTS за избор на протокола:

Символ	Стойност	Забележки
PPSS	‘FFh’	Символ за иницииране
PPS0	‘00h’ или ‘01h’	От PPS1 до PPS3 не са налични; ‘00h’ за избор на T0, ‘01h’ за избор на T1.
PK	‘XXh’	Контролен символ: ‘XXh’ = ‘FFh’ ако PPS0 = ‘00h’, ‘XXh’ = ‘FEh’ ако PPS0 = ‘01h’.

3.3. **Правила за достъп**

TCS_22 Правилата за достъп определят за даден режим на достъп, т.е. команда, съответните условия за сигурност. Ако тези условия за сигурност са изпълнени, съответната команда се изпълнява.

TCS_23 За тахографската карта се използват следните условия за сигурност:

Съкращение	Значение
ALW	Действието винаги е изпълнимо и може да се изпълнява без ограничения. APDU с команда или с отговор се изпраща като открит текст, т.е. без защитен обмен на съобщения.
NEV	Действието никога не е изпълнимо.
PLAIN-C	APDU с команда се изпраща като открит текст, т.е. без защитен обмен на съобщения.
PWD	Действието може да бъде изпълнено само след успешна проверка на PIN на картата за монтаж и настройки, т.е. ако е установено вътрешното състояние „PIN_Verified“ по отношение на сигурността на картата. Командата трябва да бъде изпратена без защитен обмен на съобщения.
EXT-AUT-G1	Действието може да бъде изпълнено само ако командата External Authenticate за удостоверяване от поколение 1 (виж също допълнение 11, част А) е била изпълнена успешно.
SM-MAC-G1	APDU (с команда или с отговор) трябва да се прилага със защитен обмен на съобщения от поколение 1 в режим само с удостоверяване (виж допълнение 11, част А).
SM-C-MAC-G1	APDU с команда трябва да се прилага със защитен обмен на съобщения от поколение 1 в режим само с удостоверяване (виж допълнение 11, част А).
SM-R-ENC-G1	APDU с отговор трябва да се прилага със защитен обмен на съобщения от поколение 1 (виж допълнение 11, част А), т.е. не се връща код за удостоверяване автентичността на съобщението.
SM-R-ENC-MAC-G1	APDU с отговор трябва да се прилага със защитен обмен на съобщения от поколение 1 в режим „криптиране и след това удостоверяване на автентичността“ (encrypt-then-authenticate) (виж допълнение 11, част А).
SM-MAC-G2	APDU (с команда или с отговор) трябва да се прилага със защитен обмен на съобщения от поколение 2 в режим само с удостоверяване (виж допълнение 11, част Б).
SM-C-MAC-G2	APDU с команда трябва да се прилага със защитен обмен на съобщения от поколение 2 в режим само с удостоверяване (виж допълнение 11, част Б).
SM-R-ENC-MAC-G2	APDU с отговор трябва да се прилага със защитен обмен на съобщения от поколение 2 в режим „криптиране и след това удостоверяване на автентичността“ (виж допълнение 11, част Б).

TCS_24 Тези условия могат да бъдат свързани помежду си по следните начини:

AND: трябва да бъдат изпълнени всички условия за сигурност

OR: трябва да бъде изпълнено поне едно от условията за сигурност.

Правилата за достъп до файловата система, т.е. командите SELECT, READ BINARY и UPDATE BINARY, са определени в глава 4. Правилата за достъп за останалите команди са определени в таблиците по-долу.

TCS_25 В приложението DF Tachograph G1 се използват следните правила за достъп:

Команда	Карта на водач	Карта за монтаж и настройки	Контролна карта	Карта на превозвач
External Authenticate				
— За удостоверяване от поколение 1	ALW	ALW	ALW	ALW
— За удостоверяване от поколение 2	ALW	PWD	ALW	ALW
Internal Authenticate	ALW	PWD	ALW	ALW
General Authenticate	ALW	ALW	ALW	ALW
Get Challenge	ALW	ALW	ALW	ALW
MSE:SET AT	ALW	ALW	ALW	ALW
MSE:SET DST	ALW	ALW	ALW	ALW
Process DSRC Message	Не се прилага	Не се прилага	Не се прилага	Не се прилага
PSO: Compute Digital Signature	ALW ИЛИ SM-MAC-G2	ALW ИЛИ SM-MAC-G2	Не се прилага	Не се прилага
PSO: Hash	Не се прилага	Не се прилага	ALW	Не се прилага
PSO: Hash of File	ALW ИЛИ SM-MAC-G2	ALW ИЛИ SM-MAC-G2	Не се прилага	Не се прилага
PSO: Verify Certificate	ALW	ALW	ALW	ALW
PSO: Verify Digital Signature	Не се прилага	Не се прилага	ALW	Не се прилага
Verify	Не се прилага	ALW	Не се прилага	Не се прилага

TCS_26 В приложението DF Tachograph_G2 се използват следните правила за достъп:

Команда	Карта на водач	Карта за монтаж и настройки	Контролна карта	Карта на превозвач
External Authenticate				
— За удостоверяване от поколение 1	Не се прилага	Не се прилага	Не се прилага	Не се прилага
— За удостоверяване от поколение 2	ALW	PWD	ALW	ALW
Internal Authenticate	Не се прилага	Не се прилага	Не се прилага	Не се прилага

Команда	Карта на водач	Карта за монтаж и настройки	Контролна карта	Карта на превозвач
General Authenticate	ALW	ALW	ALW	ALW
Get Challenge	ALW	ALW	ALW	ALW
MSE:SET AT	ALW	ALW	ALW	ALW
MSE:SET DST	ALW	ALW	ALW	ALW
Process DSRC Message	Не се прилага	ALW	ALW	Не се прилага
PSO: Compute Digital Signature	ALW ИЛИ SM-MAC-G2	ALW ИЛИ SM-MAC-G2	Не се прилага	Не се прилага
PSO: Hash	Не се прилага	Не се прилага	ALW	Не се прилага
PSO: Hash of File	ALW ИЛИ SM-MAC-G2	ALW ИЛИ SM-MAC-G2	Не се прилага	Не се прилага
PSO: Verify Certificate	ALW	ALW	ALW	ALW
PSO: Verify Digital Signature	Не се прилага	Не се прилага	ALW	Не се прилага
Verify	Не се прилага	ALW	Не се прилага	Не се прилага

TCS_27 В главния файл (MF) се използват следните правила за достъп:

Команда	Карта на водач	Карта за монтаж и настройки	Контролна карта	Карта на превозвач
External Authenticate				
— За удостоверяване от поколение 1	Не се прилага	Не се прилага	Не се прилага	Не се прилага
— За удостоверяване от поколение 2	ALW	PWD	ALW	ALW
Internal Authenticate	Не се прилага	Не се прилага	Не се прилага	Не се прилага
General Authenticate	ALW	ALW	ALW	ALW
Get Challenge	ALW	ALW	ALW	ALW
MSE:SET AT	ALW	ALW	ALW	ALW
MSE:SET DST	ALW	ALW	ALW	ALW
Process DSRC Message	Не се прилага	Не се прилага	Не се прилага	Не се прилага

Команда	Карта на водач	Карта за монтаж и настройки	Контролна карта	Карта на превозвач
PSO: Compute Digital Signature	Не се прилага	Не се прилага	Не се прилага	Не се прилага
PSO: Hash	Не се прилага	Не се прилага	Не се прилага	Не се прилага
PSO: Hash of File	Не се прилага	Не се прилага	Не се прилага	Не се прилага
PSO: Verify Certificate	ALW	ALW	ALW	ALW
Verify	Не се прилага	ALW	Не се прилага	Не се прилага

TCS_28 Тахографската карта може да възприема или да не възприема команда с по-високо равнище на сигурност от указаното в условията за сигурност. Т.е. ако условието за сигурност е ALW (или PLAIN-C) картата може да възприема команда със защитен обмен на съобщения (режим криптиране и/или удостоверяване на автентичността). Ако условието за сигурност изисква защитен обмен на съобщения с режим на удостоверяване на автентичността, тахографската карта може да възприема команда със защитен обмен на съобщения от същото поколение в режим на удостоверяване на автентичността и криптиране.

Забележка: описанията на командите предоставят повече информация относно поддръжката на командите за различните видове тахографски карти и различните специализирани файлове (DF).

3.4. **Общ преглед на командите и кодовете за грешка**

Командите и структурата на файловете са изведени от стандарта ISO/IEC 7816-4 и са в съответствие с него.

В настоящия раздел са описани следните двойки APDU команда—отговор. Поддържаните от приложения от поколение 1 и 2 варианти на команди са указани в описанията на съответните команди.

Команда	INS
SELECT	‘A4h’
READ BINARY	‘B0h’, ‘B1h’
UPDATE BINARY	‘D6h’, ‘D7h’
GET CHALLENGE	‘84h’
VERIFY	‘20h’
GET RESPONSE	‘C0h’
PERFORM SECURITY OPERATION	‘2Ah’
— VERIFY CERTIFICATE	
— COMPUTE DIGITAL SIGNATURE	
— VERIFY DIGITAL SIGNATURE	
— HASH	
— PERFORM HASH OF FILE	
— PROCESS DSRC MESSAGE	

Команда	INS
INTERNAL AUTHENTICATE	‘88h’
EXTERNAL AUTHENTICATE	‘82h’
MANAGE SECURITY ENVIRONMENT	‘22h’
— SET DIGITAL SIGNATURE TEMPLATE	
— SET AUTHENTICATION TEMPLATE	
GENERAL AUTHENTICATE	‘86h’

TCS_29 Байтовете за състояние SW1 и SW2 се връщат във всяко съобщение, съдържащо отговор, и обозначават състоянието на изпълнение на съответната команда.

SW1	SW2	Значение
90	00	Нормална обработка
61	XX	Нормална обработка. XX = брой на наличните байтове на отговора
62	81	Предупреждение за обработката. Възможно е част от върнатите данни да са увредени
63	00	Удостоверяването е неуспешно (предупреждение)
63	CX	Грешка при CHV (PIN). Брояч на оставащите опити, осигуряван от ‘X’
64	00	Грешка при изпълнението — непроменено състояние на енергонезависимата памет. Грешка в цялостността на данните
65	00	Грешка при изпълнението — променено състояние на енергонезависимата памет
65	81	Грешка при изпълнението — променено състояние на енергонезависимата памет. Неизправност на паметта
66	88	Грешка по сигурността: грешна криптографска контролна сума (по време на защитен обмен на съобщения) или грешен сертификат (по време на проверката на сертификата) или грешна криптограма (по време на външното удостоверяване) или грешен цифров подпис (по време на проверката на подписа)
67	00	Грешна дължина (грешна Lc или Le)
68	82	Не се поддържа защитен обмен на съобщения
68	83	Очаква се последната команда от веригата
69	00	Забранена команда (няма възможност за отговор при T=0)
69	82	Незадоволително състояние по отношение на сигурността
69	83	Блокиран метод за удостоверяване
69	85	Неизпълнени условия за използване
69	86	Неразрешена команда (няма активен елементарен файл)

SW1	SW2	Значение
69	87	Липса на очакваните обекти от данни при защитения обмен на съобщения
69	88	Неправилни обекти от данни при защитения обмен на съобщения
6A	80	Неправилни параметри в поле за данни
6A	82	Неоткриваем файл
6A	86	Грешни параметри P1-P2
6A	88	Неоткриваеми указани данни
6B	00	Грешни параметри (offset, т.е. изместване, извън елементарния файл)
6C	XX	Грешна дължина, SW2 указва точната дължина. Не се връща като отговор поле за данни
6D	00	Несъвместим или неправилен код на команда
6E	00	Несъвместим клас
6F	00	Други грешки при проверката

TCS_30 Ако в една APDU с команда е изпълнено повече от едно условие за грешка, картата може да върне който и да е от съответните байтове за състояние.

3.5. **Описание на командите**

В настоящата глава са описани задължителните команди за тахографските карти.

Още важни подробности относно използваните криптографски операции се дават в допълнение 11 „Общи механизми за сигурност за тахографи от поколение 1 и поколение 2“.

Всички команди са описани независимо от използвания протокол (T=0 или T=1). Винаги са посочени байтовете CLA, INS, P1, P2, Lc и Le на APDU. Ако за описаната команда не е необходим байт Lc или Le, за него не се дават дължина, стойност и описание.

TCS_31 Ако се изисква наличието и на двата байта за дължина (Lc и Le), описаната команда трябва да бъде разделена на две части, ако IFD използва протокола T=0: IFD изпраща командата, както е описано, с P3=Lc + данни, след което изпраща команда GET RESPONSE (виж точка 3.5.6) с P3=Le.

TCS_32 Ако се изисква наличието и на двата байта за дължина и ако Le=0 (защитен обмен на съобщения):

— когато се използва протоколът T=1, картата отговаря на Le=0, като изпраща всички налични изходни данни.

— Когато се използва протоколът T=0, IFD изпраща първата команда с P3=Lc + данни, а картата отговаря (на подразбиращия се Le=0) с байтовете за състояние '**61La**', където La е броят на наличните байтове на отговора. След това IFD издава команда GET RESPONSE с P3 = La за четене, т.е. извличане на данните.

TCS_33 Тахографската карта може да поддържа полета с увеличена дължина съгласно стандарт ISO/IEC 7816-4, без това да е задължително. Тахографската карта, която поддържа полета с увеличена дължина, трябва:

— да указва в ATR, че поддържа полета с увеличена дължина;

— предоставя поддържаните буферни размери посредством информация за увеличената дължина в EF ATR/INFO, виж TCS_146;

— да указва дали поддържа полета с увеличена дължина за T = 1 и/или T = 0 в EF Extended Length, виж TCS_147;

— да поддържа полета с увеличена дължина за тахографските приложения от поколения 1 и 2.

Забележки:

Всички команди са определени за полета с малка дължина. Използването на APDU с увеличена дължина се определя от стандарта ISO/IEC 7816-4.

По принцип командите са определени за открития режим, т.е. без защитен обмен на съобщения, тъй като слоят за защитен обмен на съобщения е определен в допълнение 11. От отнасящите се за дадена команда правила за достъп става ясно дали командата трябва или не трябва да поддържа защитен обмен на съобщения и дали командата трябва да поддържа защитен обмен на съобщения от поколение 1 и/или от поколение 2. За някои команди са описани варианти със защитен обмен на съобщения, за да се онагледи използването на такъв обмен.

TCS_34 Бордовото устройство (VU) изпълнява цялостния протокол от поколение 2 за взаимно удостоверяване на автентичността между него и картата за дадена сесия, включително проверката на сертификата (ако се изисква), или в специализирания файл (DF) Tachograph, или Tachograph_G2, или в главния файл (MF).

3.5.1 *SELECT*

Тази команда е в съответствие със стандарта ISO/IEC 7816-4, но е с по-ограничена употреба в сравнение с аналогичната команда, описана в този стандарт.

Командата SELECT се използва за:

— селектиране на специализиран файл на приложение (селектирането трябва да е по име);

— селектиране на елементарен файл, съответстващ на идентификатора на представения файл.

3.5.1.1 Селектиране по име (AID)

Тази команда позволява селектирането на специализиран файл на приложение, записан на картата.

TCS_35 Тази команда е изпълнима от всяка точка във файловата структура (след ATR или във всеки един момент).

TCS_36 Селектирането на определено приложение инициализира текущата среда за защита от неоторизиран достъп. След селектирането на приложението не се селектира повече никакъв активен публичен ключ. Условието за достъп EXT-AUT-G1 също така се деактивира. Ако командата е изпълнена без защитен обмен на съобщения, ключовете от предишната сесия със защитен обмен на съобщения не са повече на разположение.

TCS_37 **Командно съобщение**

Байт	Дължина	Стойност	Описание
CLA	1	‘00h’	
INS	1	‘A4h’	
P1	1	‘04h’	Селектиране по име (AID)
P2	1	‘0Ch’	Не се очаква отговор
Lc	1	‘NNh’	Брой байтове, изпратени на картата (дължина на AID): ‘06h’ за тахографското приложение
#6-#(5+NN)	NN	‘XX..XXh’	AID: ‘FF 54 41 43 48 4F’ за тахографското приложение от поколение 1 AID: ‘FF 53 4D 52 44 54’ за тахографското приложение от поколение 2

Не е нужно да се отговаря на командата SELECT (Le липсва при T=1 или не се изисква отговор при T=0).

TCS_38 **Ответно съобщение (не се изисква отговор)**

Байт	Дължина	Стойност	Описание
SW	2	‘XXXXh’	Байтове за състоянието (SW1, SW2)

— Ако командата бъде изпълнена успешно, картата връща ‘**9000**’.

— Ако приложението, съответстващо на AID, е неоткриваемо, за състоянието на обработката се връща ‘**6A82**’.

— При T=1 за състоянието се връща ‘**6700**’, ако е наличен байтът Le.

— При T=0 за състоянието се връща ‘**6900**’, ако се изисква отговор след командата SELECT.

— Ако селектираното приложение се смята за повредено (открита е грешка в цялостността на атрибутите на файла), за състоянието на обработката се връща ‘**6400**’ или ‘**6581**’.

3.5.1.2 Селектиране на елементарен файл чрез неговия файлов идентификатор

TCS_39 **Командно съобщение**

TCS_40 При този вариант на командата тахографската карта поддържа защитения обмен на съобщения от поколение 2, както е определено в допълнение 11, част Б.

Байт	Дължина	Стойност	Описание
CLA	1	‘00h’	
INS	1	‘A4h’	
P1	1	‘02h’	Селектиране на елементарен файл, който зависи от активния специализиран файл
P2	1	‘0Ch’	Не се очаква отговор
Lc	1	‘02h’	Брой байтове, изпратени на картата
#6-#7	2	‘XXXXh’	Файлов идентификатор

Не е нужно да се отговаря на командата SELECT (Le липсва при T=1 или не се изисква отговор при T=0).

TCS_41 **Ответно съобщение (не се изисква отговор)**

Байт	Дължина	Стойност	Описание
SW	2	‘XXXXh’	Байтове за състоянието (SW1, SW2)

— Ако командата бъде изпълнена успешно, картата връща ‘**9000**’.

— Ако файлът, съответстващ на файловия идентификатор, е неоткриваем, за състоянието на обработката се връща ‘**6A82**’.

— При T=1 за състоянието се връща ‘**6700**’, ако е наличен байтът Le.

— При T=0 за състоянието се връща ‘**6900**’, ако се изисква отговор след командата SELECT.

— Ако селектираният файл се смята за повреден (открита е грешка в цялостността на атрибутите на файла), за състоянието на обработката се връща ‘**6400**’ или ‘**6581**’.

3.5.2 *READ BINARY*

Тази команда е в съответствие със стандарта ISO/IEC 7816-4, но е с по-ограничена употреба в сравнение с аналогичната команда, описана в този стандарт.

Командата READ BINARY се използва за четене, т.е. извличане на данните от файл с прозрачна структура.

Отговорът на картата се състои във връщането на извлечените данни, като те се капсулират при необходимост в структура за защитен обмен на съобщения.

3.5.2.1 Команда с изместване (offset) в P1-P2

Тази команда позволява на IFD да извлича данни от селектирания елементарен файл, без да използва защитен обмен на съобщения.

Забележка: Тази команда може да се използва без защитен обмен на съобщения само за извличане на данни от файл, който поддържа условието за сигурност ALW за режима на достъп за извличане на данни.

TCS_42 **Командно съобщение**

Байт	Дължина	Стойност	Описание
CLA	1	'00h'	
INS	1	'B0h'	Read Binary
P1	1	'XXh'	Изместване в байтове, считано от началото на файла: най-старшият байт
P2	1	'XXh'	Изместване в байтове, считано от началото на файла: най-младшият байт
Le	1	'XXh'	Дължина на очакваните данни. Брой на байтовете, които трябва да се извлекат

Забележка: бит 8 на байт P1 трябва да бъде равен на нула.

TCS_43 **Ответно съобщение**

Байт	Дължина	Стойност	Описание
#1-#X	X	'XX..XXh'	Извлечени данни
SW	2	'XXXXh'	Байтове за състоянието (SW1, SW2)

— Ако командата бъде изпълнена успешно, картата връща '**9000**'.

— Ако не е селектиран елементарен файл (EF), за състоянието на обработката се връща '**6986**'.

— Ако условията за сигурност за селектирания файл не са изпълнени, изпълнението на командата се прекъсва с '**6982**'.

— Ако изместването не е съвместимо с размера на EF (изместването > размера на EF), за състоянието на обработката се връща '**6B00**':

— Ако обемът на подлежащите на извличане данни не е съвместим с размера на EF (изместването + Le > размера на EF), за състоянието на обработката се връща '**6700**' или '**6Cxx**', където 'xx' указва точната дължина.

— Ако е открита грешка в цялостността на атрибутите на файла, картата счита файла за повреден и невъзстановим, а за състоянието на обработката се връща '**6400**' или '**6581**'.

— Ако е открита грешка в цялостността на записаните данни, картата връща поисканите данни, а за състоянието на обработката се връща '**6281**'.

3.5.2.1.1 Команда със защитен обмен на съобщения (примери)

Тази команда позволява на IFD да извлече данни от селектирания елементарен файл, като използва защитен обмен на съобщения, за да провери цялостността на получените данни и да защити тяхната поверителност, ако се прилага условието за сигурност SM-R-ENC-MAC-G1 (поколение 1) или SM-R-ENC-MAC-G2 (поколение 2).

TCS_44 **Командно съобщение**

Байт	Дължина	Стойност	Описание
CLA	1	‘0Ch’	Изисква се защитен обмен на съобщения
INS	1	‘B0h’	Read Binary
P1	1	‘XXh’	P1 (изместване в байтове, считано от началото на файла): най-старшият байт
P2	1	‘XXh’	P2 (изместване в байтове, считано от началото на файла): най-младшият байт
Lc	1	‘XXh’	Дължина на входящите данни за защитения обмен на съобщения
#6	1	‘97h’	T_{LE}: таг за спецификацията на очакваната дължина
#7	1	‘01h’	L_{LE}: Очаквана дължина
#8	1	‘NNh’	Спецификация на очакваната дължина (първоначална Le): брой на байтовете, които трябва да се извлекат.
#9	1	‘8Eh’	T_{CC}: таг за криптографската контролна сума
#10	1	‘XXh’	L_{CC}: дължина на следната криптографска контролна сума ‘04h’ за защитения обмен на съобщения от поколение 1 (виж допълнение 11, част А) ‘08h’, ‘0Ch’ или ‘10h’ в зависимост от дължината на ключа по AES за защитен обмен на съобщения от поколение 2 (виж допълнение 11, част Б)
#11-#(10+L)	L	‘XX..XXh’	Криптографска контролна сума
Le	1	‘00h’	Съгласно стандарта ISO/IEC 7816-4

TCS_45 **Ответно съобщение, ако не се изисква SM-R-ENC-MAC-G1 (поколение 1) / SM-R-ENC-MAC-G2 (поколение 2) и ако форматът на входящите данни за защитения обмен на съобщения е правилен:**

Байт	Дължина	Стойност	Описание
#1	1	‘99h’	Таг за състоянието на обработката (SW1-SW2) — по избор за защитен обмен на съобщения от поколение 1
#2	1	‘02h’	Дължина на стойността за състоянието на обработката
#3 — #4	2	‘XX XXh’	Състояние на обработката на незащитената ответна APDU, т.е. с отговора
#5	1	‘81h’	T_{PV}: таг за простата стойност на данните
#6	L	‘NNh’ или ‘81 NNh’	L_{PV}: дължина на върнатите данни (= първоначална Le) L е 2 байта, ако L_{PV}>127 байта

Байт	Дължина	Стойност	Описание
#(6+L)-#(5+L+NN)	NN	‘XX..XXh’	Проста стойност на данните
#(6+L+NN)	1	‘8Eh’	T_{CC}: таг за криптографската контролна сума
#(7+L+NN)	1	‘XXh’	L_{CC}: дължина на следната криптографска контролна сума ‘04h’ за защитения обмен на съобщения от поколение 1 (виж допълнение 11, част А) ‘08h’, ‘0Ch’ или ‘10h’ в зависимост от дължината на ключа по AES за защитен обмен на съобщения от поколение 2 (виж допълнение 11, част Б)
#(8+L+NN)-#(7+M+L+NN)	M	‘XX..XXh’	Криптографска контролна сума
SW	2	‘XXXXh’	Байтове за състоянието (SW1, SW2)

TCS_46 **Ответно съобщение, ако се изисква SM-R-ENC-MAC-G1 (поколение 1) / SM-R-ENC-MAC-G2 (поколение 2) и ако форматът на входящите данни за защитения обмен на съобщения е правилен:**

Байт	Дължина	Стойност	Описание
#1	1	‘87h’	$T_{PI\ CG}$: таг за криптираните данни (криптограма)
#2	L	‘MMh’ или ‘81 MMh’	$L_{PI\ CG}$: дължина на върнатите криптирани данни (различна от първоначалната Le на командата поради запълване). L е 2 байта, ако $L_{PI\ CG}$ > 127 байта.
#(2+L)-#(1+L+MM)	MM	‘01XX..XXh’	Криптирани данни: индикатор за запълване и криптограма
#(2+L+MM)	1	‘99h’	Таг за състоянието на обработката (SW1-SW2) — по избор за защитен обмен на съобщения от поколение 1
#(3+L+MM)	1	‘02h’	Дължина на стойността за състоянието на обработката
#(4+L+MM) — #(5+L+MM)	2	‘XX XXh’	Състояние на обработката на незащитената ответна APDU
#(6+L+MM)	1	‘8Eh’	T_{CC}: таг за криптографската контролна сума
#(7+L+MM)	1	‘XXh’	L_{CC}: дължина на следната криптографска контролна сума ‘04h’ за защитения обмен на съобщения от поколение 1 (виж допълнение 11, част А) ‘08h’, ‘0Ch’ или ‘10h’ в зависимост от дължината на ключа по AES за защитен обмен на съобщения от поколение 2 (виж допълнение 11, част Б)
#(8+L+MM)-#(7+N+L+MM)	N	‘XX..XXh’	Криптографска контролна сума
SW	2	‘XXXXh’	Байтове за състоянието (SW1, SW2)

Командата READ BINARY може да върне стойности за нормални състояния на обработка, изброени в TCS_43 под тага ‘99h’, както е описано в TCS_59, използвайки за отговора структурата за защитен обмен на съобщения.

Освен това могат да възникнат някои грешки, конкретно свързани със защитения обмен на съобщения. В този случай се връща само стойност за състоянието на обработката без участието на структурата за защитен обмен на съобщения:

TCS_47 **Ответно съобщение, ако форматът на входящите данни за защитения обмен на съобщения не е правилен**

Байт	Дължина	Стойност	Описание
SW	2	‘XXXXh’	Байтове за състоянието (SW1, SW2)

— Ако не е наличен ключ на активна сесия, за състоянието на обработката се връща ‘**6A88**’. Това става, ако ключът за сесията все още не е генериран или ако валидността му е изтекла (в този случай IFD трябва да извърши отново съответния процес на взаимно удостоверяване за автентичност с цел генериране на нов ключ за сесията).

— Ако някои очаквани обекти от данни (както е определено по-горе) липсват в структурата за защитен обмен на съобщения, за състоянието на обработката се връща ‘**6987**’: тази грешка възниква, ако липсва очакван таг или ако тялото на командата не е конструирано правилно.

— Ако някои обекти от данни са неправилни, за състоянието на обработката се връща ‘**6988**’: тази грешка възниква, ако всички изисквани тагове са налични, но някои дължини се различават от очакваните.

— Ако проверката на криптографската контролна сума е неуспешна, за състоянието на обработката се връща ‘**6688**’.

3.5.2.2 Команда с кратък идентификатор на EF (елементарен файл)

Този вариант на командата позволява на IFD да селектира един EF чрез неговия кратък идентификатор и да извлече данни от този EF.

TCS_48 Тахографската карта трябва да поддържа този вариант на командата за всички елементарни файлове, които са с определен кратък идентификатор. Тези кратки идентификатори на EF са определени в глава 4.

TCS_49 **Командно съобщение**

Байт	Дължина	Стойност	Описание
CLA	1	‘00h’	
INS	1	‘B0h’	Read Binary
P1	1	‘XXh’	За бит 8 е зададена стойност 1 За битове 7 и 6 е зададена стойност 00. Битове 5 — 1 кодират краткия идентификатор на съответния EF
P2	1	‘XXh’	Кодира изместване от 0 до 255 байта в EF, посочен от P1
Le	1	‘XXh’	Дължина на очакваните данни Брой на байтовете, които трябва да се извлекат.

Забележка: Кратките идентификатори на EF, използвани за тахографското приложение от поколение 2, са определени в глава 4.

Ако P1 кодира кратък идентификатор на EF и командата бъде изпълнена успешно, идентифицираният EF се селектира като текущ (активен EF).

TCS_50 **Ответно съобщение**

Байт	Дължина	Стойност	Описание
#1-#L	L	‘XX..XXh’	Извлечени данни
SW	2	‘XXXXh’	Байтове за състоянието (SW1, SW2)

— Ако командата бъде изпълнена успешно, картата връща '**9000**'.

— Ако файлът, съответстващ на краткия EF идентификатор, е неоткриваем, за състоянието на обработката се връща '**6A82**'.

— Ако условията за сигурност за селектирания файл не са изпълнени, изпълнението на командата се прекъсва с '**6982**'.

— Ако изместването не е съвместимо с размера на EF (изместването > размера на EF), за състоянието на обработката се връща '**6B00**':

— Ако обемът на подлежащите на извличане данни не е съвместим с размера на EF (изместването + Le > размера на EF), за състоянието на обработката се връща '**6700**' или '**6Cxx**', където 'xx' указва точната дължина:

— Ако е открита грешка в цялостността на атрибутите на файла, картата счита файла за повреден и невъзстановим, а за състоянието на обработката се връща '**6400**' или '**6581**'.

— Ако е открита грешка в цялостността на записаните данни, картата връща поисканите данни, а за състоянието на обработката се връща '**6281**'.

3.5.2.3 Команда с нечетен байт за инструкция

Този вариант на командата позволява на IFD да извлича данни от един елементарен файл с големина 32 768 байта или повече.

TCS_51 Тахографска карта, която поддържа елементарни файлове с големина 32 768 байта или повече, трябва да поддържа за тях и този вариант на командата. Тахографската карта може да поддържа или да не поддържа този вариант на командата за други елементарни файлове с изключение на елементарния файл Sensor_Installation_Data — виж TCS_156 и TCS_160.

TCS_52 **Командно съобщение**

Байт	Дължина	Стойност	Описание
CLA	1	'00h'	
INS	1	'B1h'	Read Binary
P1	1	'00h'	Активен елементарен файл
P2	1	'00h'	
Lc	1	'NNh'	Дължина Lc на изместения обект от данни
#6-#(5+NN)	NN	'XX..XXh'	Изместване на обекта от данни: Таг '54h' Дължина '01h' или '02h' Стойност изместване
Le	1	'XXh'	Брой на байтовете, които трябва да се извлекат.

IFD кодира дължината на изместения обект от данни с минималния възможен брой октети, т.е. като използва байта за дължина '01h' IFD кодира изместване от 0 до 255, а като използва байта за дължина '02h' — изместване от '256' до '65 535' байта.

TCS_53 **Ответно съобщение**

Байт	Дължина	Стойност	Описание
#1-#L	L	'XX..XXh'	Извлечените данни, капсулирани в дискреционен обект от данни с таг '53h'.
SW	2	'XXXXh'	Байтове за състоянието (SW1, SW2)

— Ако командата бъде изпълнена успешно, картата връща '**9000**'.

— Ако не е селектиран елементарен файл (EF), за състоянието на обработката се връща '**6986**'.

— Ако условията за сигурност за селектирания файл не са изпълнени, изпълнението на командата се прекъсва с '**6982**'.

— Ако изместването не е съвместимо с размера на EF (изместването > размера на EF), за състоянието на обработката се връща '**6B00**':

— Ако обемът на подлежащите на извличане данни не е съвместим с размера на EF (изместването + Le > размера на EF), за състоянието на обработката се връща '**6700**' или '**6Cxx**', където 'xx' указва точната дължина.

— Ако е открита грешка в цялостността на атрибутите на файла, картата счита файла за повреден и невъзстановим, а за състоянието на обработката се връща '**6400**' или '**6581**'.

— Ако е открита грешка в цялостността на записаните данни, картата връща поисканите данни, а за състоянието на обработката се връща '**6281**'.

3.5.2.3.1 Команда със защитен обмен на съобщения (пример)

Следният пример онагледява използването на защитен обмен на съобщения, ако е валидно условието за сигурност SM-MAC-G2.

TCS_54 Командно съобщение

Байт	Дължина	Стойност	Описание
CLA	1	'0Ch'	Изисква се защитен обмен на съобщения
INS	1	'B1h'	Read Binary
P1	1	'00h'	Активен елементарен файл
P2	1	'00h'	
Lc	1	'XXh'	Дължина на защитеното поле за данни
#6	1	'B3h'	Таг за простата стойност на данните, кодирани по BER-TLV
#7	1	'NNh'	L_{PV}: дължина на предадените данни
#(8)-#(7+NN)	NN	'XX..XXh'	Прости данни, кодирани по BER-TLV, т.е. изместеният обект от данни с таг '54'
#(8+NN)	1	'97h'	T_{LE}: таг за спецификацията на очакваната дължина
#(9+NN)	1	'01h'	L_{LE}: Очаквана дължина
#(10+NN)	1	'XXh'	Спецификация на очакваната дължина (първоначална Le): брой на байтовете, които трябва да се извлекат.
#(11+NN)	1	'8Eh'	T_{CC}: таг за криптографската контролна сума
#(12+NN)	1	'XXh'	L_{CC}: дължина на следната криптографска контролна сума '08h', '0Ch' или '10h' в зависимост от дължината на ключа по AES за защитен обмен на съобщения от поколение 2 (виж допълнение 11, част Б)
#(13+NN)-#(12+M+NN)	M	'XX..XXh'	Криптографска контролна сума
Le	1	'00h'	Съгласно стандарта ISO/IEC 7816-4

TCS_55 Ответно съобщение, ако командата бъде изпълнена успешно

Байт	Дължина	Стойност	Описание
#1	1	‘B3h’	Прости данни, кодирани по BER-TLV
#2	L	‘NNh’ или ‘81 NNh’	L_{PV}: дължина на върнатите данни (= първоначална Le) L е 2 байта, ако L_{PV}>127 байта
#(2+L)-#(1+L+NN)	NN	‘XX..XXh’	Стойност на простите данни, кодирана по BER-TLV, т.е. извлечените данни, капсулирани в дискреционен обект от данни с таг ‘53h’.
#(2+L+NN)	1	‘99h’	Състояние на обработката на незащитената ответна APDU
#(3+L+NN)	1	‘02h’	Дължина на стойността за състоянието на обработката
#(4+L+NN) — #(5+L+NN)	2	‘XX XXh’	Състояние на обработката на незащитената ответна APDU
#(6+L+NN)	1	‘8Eh’	T_{CC}: таг за криптографската контролна сума
#(7+L+NN)	1	‘XXh’	L_{CC}: дължина на следната криптографска контролна сума ‘08h’, ‘0Ch’ или ‘10h’ в зависимост от дължината на ключа по AES за защитен обмен на съобщения от поколение 2 (виж допълнение 11, част Б)
#(8+L+NN)-#(7+M+L+NN)	M	‘XX..XXh’	Криптографска контролна сума
SW	2	‘XXXXh’	Байтове за състоянието (SW1, SW2)

3.5.3 *UPDATE BINARY*

Тази команда е в съответствие със стандарта ISO/IEC 7816-4, но е с по-ограничена употреба в сравнение с аналогичната команда, описана в този стандарт.

Съобщението с командата UPDATE BINARY инициализира актуализирането (изтриване + записване) на битовете, които вече присъстват в определен двоичен елементарен файл (EF), с битовете, които се съдържат в APDU с командата.

3.5.3.1 Команда с изместване в P1-P2

Тази команда позволява на IFD да запише данните в селектирания елементарен файл, без картата да проверява цялостността на получените данни.

Забележка: Тази команда може да се използва без защитен обмен на съобщения за актуализиране само на файл, който поддържа условието за сигурност ALW за режима на достъп за актуализиране.

TCS_56 **Командно съобщение**

Байт	Дължина	Стойност	Описание
CLA	1	‘00h’	
INS	1	‘D6h’	Update Binary

Байт	Дължина	Стойност	Описание
P1	1	‘XXh’	Изместване в байтове, считано от началото на файла: най-старшият байт
P2	1	‘XXh’	Изместване в байтове, считано от началото на файла: най-младшият байт
Lc	1	‘NNh’	Дължина Lc на данните, които подлежат на актуализиране Брой на байтовете, които трябва да се запишат
#6-#(5+NN)	NN	‘XX..XXh’	Данни, които трябва да се запишат

Забележка: бит 8 на байт P1 трябва да бъде равен на нула.

TCS_57 **Ответно съобщение**

Байт	Дължина	Стойност	Описание
SW	2	‘XXXXh’	Байтове за състоянието (SW1, SW2)

— Ако командата бъде изпълнена успешно, картата връща ‘**9000**’.

— Ако не е селектиран елементарен файл (EF), за състоянието на обработката се връща ‘**6986**’.

— Ако условията за сигурност за селектирания файл не са изпълнени, изпълнението на командата се прекъсва с ‘**6982**’.

— Ако изместването не е съвместимо с размера на EF (изместването > размера на EF), за състоянието на обработката се връща ‘**6B00**’:

— Ако обемът на данните, които ще се записват, не е съвместим с размера на елементарния файл (изместването + Lc > размера на елементарния файл), за състоянието на обработката се връща ‘**6700**’.

— Ако е открита грешка в цялостността на атрибутите на файла, картата счита файла за повреден и невъзстановим, а за състоянието на обработката се връща ‘**6400**’ или ‘**6500**’.

— Ако записването е неуспешно, за състоянието на обработката се връща ‘**6581**’.

3.5.3.1.1 Команда със защитен обмен на съобщения (примери)

Тази команда позволява на IFD да запише данните в селектирания елементарен файл, като картата проверява цялостността на получените данни. Тъй като няма изискване за поверителност, данните не са криптирани.

TCS_58 **Командно съобщение**

Байт	Дължина	Стойност	Описание
CLA	1	‘0Ch’	Изисква се защитен обмен на съобщения
INS	1	‘D6h’	Update Binary
P1	1	‘XXh’	Изместване в байтове, считано от началото на файла: най-старшият байт
P2	1	‘XXh’	Изместване в байтове, считано от началото на файла: най-младшият байт
Lc	1	‘XXh’	Дължина на защитеното поле за данни

Байт	Дължина	Стойност	Описание
#6	1	‘81h’	T_{PV}: таг за простата стойност на данните
#7	L	‘NNh’ или ‘81 NNh’	L_{PV}: дължина на предадените данни L е 2 байта, ако L_{PV} > 127 байта
#(7+L)-#(6+L+NN)	NN	‘XX..XXh’	Стойност на простите данни (данни, които трябва да се запишат)
#(7+L+NN)	1	‘8Eh’	T_{CC}: таг за криптографската контролна сума
#(8+L+NN)	1	‘XXh’	L_{CC}: дължина на следната криптографска контролна сума‘04h’ за защитения обмен на съобщения от поколение 1 (виж допълнение 11, част А) ‘08h’, ‘0Ch’ или ‘10h’ в зависимост от дължината на ключа по AES за защитен обмен на съобщения от поколение 2 (виж допълнение 11, част Б)
#(9+L+NN)-#(8+M+L+NN)	M	‘XX..XXh’	Криптографска контролна сума
Le	1	‘00h’	Съгласно стандарта ISO/IEC 7816-4

TCS_59 **Ответно съобщение ако форматът на входящите данни при защитения обмен на съобщения е правилен**

Байт	Дължина	Стойност	Описание
#1	1	‘99h’	T_{SW}: таг за байтовете за състояние (трябва защита с криптографски контрол)
#2	1	‘02h’	L_{SW}: дължина на върнатите байтове за състояние
#3-#4	2	‘XXXXh’	Състояние на обработката на незащитената ответна APDU
#5	1	‘8Eh’	T_{CC}: таг за криптографската контролна сума
#6	1	‘XXh’	L_{CC}: дължина на следната криптографска контролна сума ‘04h’ за защитения обмен на съобщения от поколение 1 (виж допълнение 11, част А) ‘08h’, ‘0Ch’ или ‘10h’ в зависимост от дължината на ключа по AES за защитен обмен на съобщения от поколение 2 (виж допълнение 11, част Б)
#7-#(6+L)	L	‘XX..XXh’	Криптографска контролна сума
SW	2	‘XXXXh’	Байтове за състоянието (SW1, SW2)

Стойностите за „нормалните“ състояния на обработка, описани за командата UPDATE BINARY без използване на защитен обмен на съобщения (виж точка 3.5.3.1), могат да бъдат върнати, като се използва описаната по-горе структура на ответно съобщение.

Освен това могат да възникнат някои грешки, конкретно свързани със защитения обмен на съобщения. В този случай се връща само стойността за състоянието на обработката без участието на структурата за защитен обмен на съобщения:

TCS_60 **Ответно съобщение в случай на грешка, засягаща защитения обмен на съобщения**

Байт	Дължина	Стойност	Описание
SW	2	‘XXXXh’	Байтове за състоянието (SW1, SW2)

— Ако не е наличен ключ на активна сесия, за състоянието на обработката се връща '**6A88**'.

— Ако някои очаквани обекти от данни (както е определено по-горе) липсват в структурата за защитен обмен на съобщения, за състоянието на обработката се връща '**6987**': тази грешка възниква, ако липсва очакван таг или ако тялото на командата не е конструирано правилно.

— Ако някои обекти от данни са неправилни, за състоянието на обработката се връща '**6988**': тази грешка възниква, ако всички изисквани тагове са налични, но някои дължини се различават от очакваните.

— Ако проверката на криптографската контролна сума е неуспешна, за състоянието на обработката се връща '**6688**'.

3.5.3.2 Команда с кратък идентификатор на EF

Този вариант на командата позволява на IFD да селектира един EF чрез неговия кратък идентификатор и да запише данни от този EF.

TCS_61 Тахографската карта трябва да поддържа този вариант на командата за всички елементарни файлове, които са с определен кратък идентификатор. Тези кратки идентификатори на EF са определени в глава 4.

TCS_62 **Командно съобщение**

Байт	Дължина	Стойност	Описание
CLA	1	'00h'	
INS	1	'D6h'	Update Binary
P1	1	'XXh'	За бит 8 е зададена стойност 1 За битове 7 и 6 е зададена стойност 00. Битове 5 — 1 кодират краткия идентификатор на съответния EF
P2	1	'XXh'	Кодира изместване от 0 до 255 байта в EF, посочен от P1
Lc	1	'NNh'	Дължина Lc на данните, които подлежат на актуализиране Брой на байтовете, които трябва да се запишат
#6-#(5+NN)	NN	'XX..XXh'	Данни, които трябва да се запишат

TCS_63 **Ответно съобщение**

Байт	Дължина	Стойност	Описание
SW	2	'XXXXh'	Байтове за състоянието (SW1, SW2)

Забележка: Кратките идентификатори на EF, използвани за тахографското приложение от поколение 2, са определени в глава 4.

Ако P1 кодира кратък идентификатор на EF и командата бъде изпълнена успешно, идентифицираният EF се селектира като текущ (активен EF).

— Ако командата бъде изпълнена успешно, картата връща '**9000**'.

— Ако файлът, съответстващ на краткия EF идентификатор, е неоткриваем, за състоянието на обработката се връща '**6A82**'.

— Ако условията за сигурност за селектирания файл не са изпълнени, изпълнението на командата се прекъсва с '**6982**'.

— Ако изместването не е съвместимо с размера на EF (изместване > размера на EF), за състоянието на обработката се връща '**6B00**':

— Ако обемът на данните, които ще се записват, не е съвместим с размера на елементарния файл (изместването + Lc > размера на елементарния файл), за състоянието на обработката се връща '**6700**'.

— Ако е открита грешка в цялостността на атрибутите на файла, картата счита файла за повреден и невъзстановим, а за състоянието на обработката се връща '**6400**' или '**6581**'.

— Ако записването е неуспешно, за състоянието на обработката се връща '**6581**'.

3.5.3.3 Команда с нечетен байт за инструкция

Този вариант на командата позволява на IFD да записва данни в елементарен файл с големина 32 768 байта или повече.

TCS_64 Тахографска карта, която поддържа елементарни файлове с големина 32 768 байта или повече, трябва да поддържа за тях и този вариант на командата. Тахографската карта може да поддържа или да не поддържа този вариант на командата за други елементарни файлове.

TCS_65 **Командно съобщение**

Байт	Дължина	Стойност	Описание
CLA	1	'00h'	
INS	1	'D7h'	Update Binary
P1	1	'00h'	Активен елементарен файл
P2	1	'00h'	
Lc	1	'NNh'	Lc дължина на данните в полето за данни на командата
#6-#(5+NN)	NN	'XX..XXh'	Изместване на обект от данни с таг '54h' || Дискреционен обект от данни с таг '53h', в който са капсулирани подлежащите на записване данни

IFD кодира дължината на изместения обект от данни и на дискреционния обект от данни с минималния възможен брой октети, т.е. като използва байта за дължина '01h' IFD кодира изместване / дължина от 0 до 255, а като използва байта за дължина '02h' — изместване / дължина от '256' до '65 535' байта.

TCS_66 **Ответно съобщение**

Байт	Дължина	Стойност	Описание
SW	2	'XXXXh'	Байтове за състоянието (SW1, SW2)

— Ако командата бъде изпълнена успешно, картата връща '**9000**'.

— Ако не е селектиран елементарен файл (EF), за състоянието на обработката се връща '**6986**'.

— Ако условията за сигурност за селектирания файл не са изпълнени, изпълнението на командата се прекъсва с '**6982**'.

— Ако изместването не е съвместимо с размера на EF (изместването > размера на EF), за състоянието на обработката се връща '**6B00**':

— Ако обемът на данните, които ще се записват, не е съвместим с размера на елементарния файл (изместването + Lc > размера на елементарния файл), за състоянието на обработката се връща '**6700**'.

— Ако е открита грешка в цялостността на атрибутите на файла, картата счита файла за повреден и невъзстановим, а за състоянието на обработката се връща '**6400**' или '**6500**'.

— Ако записването е неуспешно, за състоянието на обработката се връща '**6581**'.

3.5.3.3.1 Команда със защитен обмен на съобщения (пример)

Следният пример онагледява използването на защитен обмен на съобщения, ако е валидно условието за сигурност SM-MAC-G2.

TCS_67 Командно съобщение

Байт	Дължина	Стойност	Описание
CLA	1	'0Ch'	Изисква се защитен обмен на съобщения
INS	1	'D7h'	Update Binary
P1	1	'00h'	Активен елементарен файл
P2	1	'00h'	
Lc	1	'XXh'	Дължина на защитеното поле за данни
#6	1	'B3h'	Таг за простата стойност на данните, кодирани по BER-TLV
#7	L	'NNh' или '81 NNh'	L_{PV}: дължина на предадените данни L е 2 байта, ако L_{PV} > 127 байта
#(7+L)-#(6+L+NN)	NN	'XX..XXh'	Прости данни, кодирани по BER-TLV, т.е. изместване на обекта от данни с таг '54h' || Дискреционен обект от данни с таг '53h', в който са капсулирани подлежащите на записване данни
#(7+L+NN)	1	'8Eh'	T_{CC}: таг за криптографската контролна сума
#(8+L+NN)	1	'XXh'	L_{CC}: дължина на следната криптографска контролна сума '08h', '0Ch' или '10h' в зависимост от дължината на ключа по AES за защитен обмен на съобщения от поколение 2 (виж допълнение 11, част Б)
#(9+L+NN)-#(8+M+L+NN)	M	'XX..XXh'	Криптографска контролна сума
Le	1	'00h'	Съгласно стандарта ISO/IEC 7816-4

TCS_68 Ответно съобщение ако командата бъде изпълнена успешно

Байт	Дължина	Стойност	Описание
#1	1	'99h'	T_{SW}: таг за байтовете за състояние (трябва защита с криптографски контрол)
#2	1	'02h'	L_{SW}: дължина на върнатите байтове за състояние
#3-#4	2	'XXXXh'	Състояние на обработката на незащитената ответна APDU
#5	1	'8Eh'	T_{CC}: таг за криптографската контролна сума

Байт	Дължина	Стойност	Описание
#6	1	‘XXh’	L_{CC}: дължина на следната криптографска контролна сума ‘08h’, ‘0Ch’ или ‘10h’ в зависимост от дължината на ключа по AES за защитен обмен на съобщения от поколение 2 (виж допълнение 11, част Б)
#7-#(6+L)	L	‘XX..XXh’	Криптографска контролна сума
SW	2	‘XXXXh’	Байтове за състоянието (SW1, SW2)

3.5.4 *GET CHALLENGE*

Тази команда е в съответствие със стандарта ISO/IEC 7816-4, но е с по-ограничена употреба в сравнение с аналогичната команда, описана в този стандарт.

С командата GET CHALLENGE от картата се иска да издаде произволно число, за да се използва то в свързана със сигурността процедура, при която на картата се изпращат някои криптирани данни или криптограма.

TCS_69 Произволното число, издадено от картата, важи единствено за следващата команда, при която се използва произволно число, изпратено на картата.

TCS_70 **Командно съобщение**

Байт	Дължина	Стойност	Описание
CLA	1	‘00h’	
INS	1	‘84h’	INS
P1	1	‘00h’	P1
P2	1	‘00h’	P2
Le	1	‘08h’	Le (дължина на очакваното произволно число)

TCS_71 **Ответно съобщение**

Байт	Дължина	Стойност	Описание
#1-#8	8	‘XX..XXh’	Произволно число
SW	2	‘XXXXh’	Байтове за състоянието (SW1, SW2)

— Ако командата бъде изпълнена успешно, картата връща ‘**9000**’.

— Ако байтът Le се различава от ‘08h’, състоянието на обработката е ‘**6700**’.

— Ако параметрите P1-P2 са неправилни, състоянието на обработката е ‘**6A86**’.

3.5.5 *VERIFY*

Тази команда е в съответствие със стандарта ISO/IEC 7816-4, но е с по-ограничена употреба в сравнение с аналогичната команда, описана в този стандарт.

Само за картата за монтаж и настройки се изисква да поддържа тази команда.

Другите видове тахографски карти могат или не могат да изпълняват тази команда, но за тях референтната информация за CHV не е персонализирана. Поради това тези карти не могат да изпълняват успешно тази команда. Ако тази команда бъде подадена на други видове тахографски карти, различни от картите за монтаж и настройки, тяхното поведение, т.е. връщаният код за грешка, е извън обхвата на настоящата спецификация.

Командата VERIFY стартира сравняването на равнището на картата между изпратените данни за CHV (PIN) и референтните данни за CHV, записани в паметта на картата.

TCS_72 Въведеният от потребителя PIN трябва да е по стандарта ASCII за кодиране на символи и да е допълнен от IFD отдясно с байтове 'FFh' до дължина от 8 байта — виж също в допълнение 1 за типа на данните WorkshopCardPIN.

TCS_73 За тахографските приложения от поколения 1 и 2 се използват едни и същи референтни данни за CHV.

TCS_74 Тахографската карта проверява дали командата е кодирана правилно. Ако командата не е кодирана правилно, картата не сравнява стойностите за CHV, не намалява стойността на брояча за оставащите опити за CHV и не инициализира състоянието „PIN_Verified" по отношение на сигурността, а прекратява изпълнението на командата. Командата е кодирана правилно, ако байтовете CLA, INS, P1, P2 и Lc са с указаните стойности, Le отсъства и полето за данни на командата е с правилната дължина.

TCS_75 Ако командата бъде изпълнена успешно, броячът на оставащите опити за CHV се връща на първоначалната си стойност. Първоначалната стойност на брояча на оставащите опити за CHV е 5. Ако командата бъде изпълнена успешно, картата установява „PIN_Verified" за вътрешното състояние по отношение на сигурността. Картата инициализира това състояние по отношение на сигурността, ако картата бъде инициализирана или ако предаденият в командата код за CHV не съвпада със съхраняваните референтни данни за CHV.

Забележка: Чрез използването на същите референтни данни за CHV и на общо състояние по отношение на сигурността се избягва необходимостта сервизният служител да въвежда повторно PIN след селектиране на специализиран файл (DF) на друго тахографско приложение.

TCS_76 Ако сравняването завърши неуспешно, това се регистрира в картата, т.е. стойността на брояча за оставащите опити за CHV се намалява с единица, за да се ограничи броят на следващите опити за използване на референтните данни за CHV.

TCS_77 **Командно съобщение**

Байт	Дължина	Стойност	Описание
CLA	1	'00h'	
INS	1	'20h'	INS
P1	1	'00h'	P1
P2	1	'00h'	P2 (проверените данни за CHV са известни по подразбиране)
Lc	1	'08h'	Дължина на предадения код за CHV
#6-#13	8	'XX..XXh'	CHV

TCS_78 **Ответно съобщение**

Байт	Дължина	Стойност	Описание
SW	2	'XXXXh'	Байтове за състоянието (SW1, SW2)

— Ако командата бъде изпълнена успешно, картата връща '**9000**'.

— Ако референтните данни за CHV са неоткриваеми, за състоянието на обработката се връща '**6A88**'.

— Ако проверката CHV е блокирана (броячът на оставащите опити за CHV е на нула), за състоянието на обработката се връща '**6983**'. След като се достигне това състояние, повече не е възможно данните за CHV да бъдат представени успешно.

— Ако сравняването не завърши успешно, стойността на брояча за оставащите опити се намалява с единица и за състоянието се връща '**63CX**' (X>0 и X е равно на стойността на брояча за оставащите опити).

— Ако референтните данни за CHV се считат за повредени, за състоянието на обработката се връща '**6400**' или '**6581**'.

— Ако Lc се различава от '08h', състоянието на обработката е '**6700**'.

3.5.6 *GET RESPONSE*

Тази команда е в съответствие със стандарта ISO/IEC 7816-4.

Тази команда (която е необходима и налична само за протокола T=0) се използва за предаване на подготвените данни от картата към интерфейсното устройство (когато и двата байта Lc и Le са включени в командата).

Командата GET RESPONSE трябва да бъде изпратена непосредствено след командата за подготовка на данните, тъй като в противен случай данните се загубват. След изпълнението на командата GET RESPONSE подготвените преди това данни не са налични повече (освен ако възникне грешката '**61xx**' или '**6Cxx**', виж по-долу).

TCS_79 **Командно съобщение**

Байт	Дължина	Стойност	Описание
CLA	1	'00h'	
INS	1	'C0h'	
P1	1	'00h'	
P2	1	'00h'	
Le	1	'XXh'	Брой на очакваните байтове

TCS_80 **Ответно съобщение**

Байт	Дължина	Стойност	Описание
#1-#X	X	'XX..XXh'	Данни
SW	2	'XXXXh'	Байтове за състоянието (SW1, SW2)

— Ако командата бъде изпълнена успешно, картата връща '**9000**'.

— Ако картата не е подготвила никакви данни, за състоянието на обработката се връща '**6900**' или '**6F00**'.

— Ако байтът Le надвишава броя на наличните байтове или ако този байт е нулев, за състоянието на обработката се връща '**6Cxx**', където xx указва точния брой на наличните байтове. В този случай подготвените данни остават на разположение за изпълнението по-късно на командата GET RESPONSE.

— Ако байтът Le представлява ненулева стойност, която е по-малка от броя на наличните байтове, картата нормално изпраща исканите данни и за състоянието на обработката се връща '**61xx**', където 'xx' указва броя на допълнителните байтове, които все още са на разположение за изпълнението по-късно на командата GET RESPONSE.

— Ако командата не се поддържа (за протокола T=1), картата връща '**6D00**'.

3.5.7 *PSO: VERIFY CERTIFICATE*

Тази команда е в съответствие със стандарта ISO/IEC 7816-8, но е с по-ограничена употреба в сравнение с аналогичната команда, описана в този стандарт.

Картата използва командата VERIFY CERTIFICATE, за да получи публичен ключ, идващ от публичното пространство, и за проверка на неговата валидност.

3.5.7.1 Двойка команда—отговор от поколение 1

TCS_81 Този вариант на командата се поддържа само от тахографско приложение от поколение 1.

TCS_82 Когато командата VERIFY CERTIFICATE бъде изпълнена успешно, съответният публичен ключ се запаметява в средата, свързана със защитата от неоторизиран достъп, с цел по-късното му използване. Този ключ трябва да бъде специално конфигуриран, за да бъде използван в рамките на командите, имащи отношение към сигурността (INTERNAL AUTHENTICATE, EXTERNAL AUTHENTICATE или VERIFY CERTIFICATE), чрез командата MSE (виж точка 3.5.11), като се използва неговият идентификатор.

TCS_83 При всички положения командата VERIFY CERTIFICATE използва публичния ключ, избран преди това чрез командата MSE, за да отвори определен сертификат. Това трябва да бъде публичен ключ на определена държава членка или на Европа.

TCS_84 **Командно съобщение**

Байт	Дължина	Стойност	Описание
CLA	1	‘00h’	
INS	1	‘2Ah’	Извършване на операция, свързана със защитата от неоторизиран достъп
P1	1	‘00h’	P1
P2	1	‘AEh’	P2: данни, които не са кодирани по BER-TLV (конкатенация на елементи на данни)
Lc	1	‘C2h’	Lc: дължина на сертификата, 194 байта
#6-#199	194	‘XX..XXh’	Сертификат: конкатенация на елементи на данни (съгласно описанието в допълнение 11)

TCS_85 **Ответно съобщение**

Байт	Дължина	Стойност	Описание
SW	2	‘XXXXh’	Байтове за състоянието (SW1, SW2)

— Ако командата бъде изпълнена успешно, картата връща ‘**9000**’.

— Ако проверката на сертификата е неуспешна, за състоянието на обработката се връща ‘**6688**’. Процесът на проверка и на отваряне на сертификата е описан в допълнение 11 за поколения 1 и 2.

— Ако не е наличен ключ в средата, свързана със защитата от неоторизиран достъп, се връща ‘**6A88**’.

— Ако избраният публичен ключ (използван за отваряне на сертификата) се счита за повреден, за състоянието на обработката се връща **‘6400’ или ‘6581’**.

— Само за поколение 1: ако избраният публичен ключ (използван за отваряне на сертификата) има CHA.LSB (`CertificateHolderAuthorisation.equipmentType`), различен от ‘00’ (т.е. не принадлежи на държава членка или на Европа), за състоянието на обработката се връща ‘**6985**’.

3.5.7.2 Двойка команда—отговор от поколение 2

В зависимост от размера на кривата ECC сертификатите могат да бъдат толкова дълги, че да не е възможно предаването им в една-единствена APDU. В този случай трябва да се приложи верижно свързване на команди в съответствие с ISO/IEC 7816-4 и сертификатът се предава в две последователни APDU PSO: Verify Certificate.

Структурата на сертификата и параметрите на домейна са определени в допълнение 11.

TCS_86 Тази команда може да бъде изпълнена в MF, DF Tachograph и DF Tachograph_G2, виж също TCS_33.

TCS_87 **Командно съобщение**

Байт	Дължина	Стойност	Описание
CLA	1	‘X0h’	Байт CLA, указващ верижно свързване на команди: ‘00h’ за единствена или последна команда във веригата ‘10h’ за команда, която не е последна във веригата
INS	1	‘2Ah’	Извършване на операция, свързана със защитата от неоторизиран достъп
P1	1	‘00h’	
P2	1	‘BEh’	Проверка на самоописващ се (self-descriptive) сертификат
Lc	1	‘XXh’	Дължина на полето за данни на командата, виж TCS_88 и TCS_89.
#6-#5+L	L	‘XX..XXh’	Данни, кодирани по DER-TLV: обектът от данни в тялото на ECC сертификата е съединен като първи обект от данни с обекта от данни в подписа на ECC сертификата като втори обект от данни или част от тази конкатенация. Тагът ‘7F21’ и съответната дължина не се предават. Тези обекти от данни са във фиксирана последователност.

TCS_88 За APDU с малка дължина се прилагат следните разпоредби: IFD трябва да използва минималния брой APDU, необходими за предаването на командите, и да предава максималния брой байтове в първата APDU с команда съгласно стойността на байта за зоната за информация, запазена за картата, виж TCS_14. Ако IFD действа по различен начин, поведението на картата е извън обхвата на настоящата спецификация.

TCS_89 За APDU с увеличена дължина се прилагат следните разпоредби: Ако сертификатът не се побира в една-единствена APDU, картата трябва да поддържа верижно свързване на команди. IFD трябва да използва минималния брой APDU, необходими за предаването на командите, и да предава максималния брой байтове в първата APDU с команда. Ако IFD действа по различен начин, поведението на картата е извън обхвата на настоящата спецификация.

Забележка: съгласно допълнение 11 картата съхранява сертификата или съответното съдържание на сертификата и актуализира своето currentAuthenticatedTime.

Структурата на ответното съобщение и байтовете за състоянието са определени в TCS_85.

TCS_90 В допълнение към кодовете за грешка, посочени в TCS_85, картата може да върне следните кодове за грешка:

— ако избраният публичен ключ (използван за отваряне на сертификата) има CHA.LSB (CertificateHolderAuthorisation.equipmentType), който не е подходящ за проверка на сертификата съгласно допълнение 11, за състоянието на обработката се връща ‘**6985**’.

— Ако currentAuthenticatedTime на картата е по-късно от датата на изтичане на срока на сертификата, а състоянието на обработката се връща ‘**6985**’.

— Ако се очаква последната команда от верижната последователност, картата връща ‘**6883**’.

— Ако са изпратени неправилни параметри в полето за данни на командата, картата връща ‘**6A80**’ (използва се и когато обектите от данни не са изпратени в указаната последователност).

3.5.8 *INTERNAL AUTHENTICATE*

Тази команда е в съответствие със стандарта ISO/IEC 7816-4.

TCS_91 Всички тахографски карти трябва да поддържат тази команда в специализирания файл (DF) Tachograph от поколение 1. Тази команда може или не може да е достъпна в MF и/или в DF Tachograph_G2. Ако командата е достъпна, нейното изпълнение се прекратява с подходящ код за грешка, тъй като частният ключ на картата (Card.SK) за протокола от поколение 1 за удостоверяване на автентичността е достъпен само в DF_Tachograph от поколение 1.

Чрез командата INTERNAL AUTHENTICATE интерфейсното устройство (IFD) може да удостовери автентичността на картата. Процесът на удостоверяване е описан в допълнение 11. Той включва следните оператори:

TCS_92 Командата INTERNAL AUTHENTICATE използва частния ключ на картата (избран по подразбиране), за да подпише данните от удостоверяването, включително K1 (първият елемент, указващ съпоставянето на ключовете на сесията) и RND1, и също така използва избрания публичен ключ (посредством последната команда MSE), за да криптира подписа и да състави маркера за удостоверяването (за повече подробности виж допълнение 11).

TCS_93 **Командно съобщение**

Байт	Дължина	Стойност	Описание
CLA	1	‘00h’	CLA
INS	1	‘88h’	INS
P1	1	‘00h’	P1
P2	1	‘00h’	P2
Lc	1	‘10h’	Дължина на данните, изпратени на картата
#6 — #13	8	‘XX..XXh’	Искане за достъп, използвано за удостоверяване автентичността на картата
#14 -#21	8	‘XX..XXh’	VU.CHR (виж допълнение 11)
Le	1	‘80h’	Дължина на очакваните данни, идващи от картата

TCS_94 **Ответно съобщение**

Байт	Дължина	Стойност	Описание
#1-#128	128	‘XX..XXh’	Маркер за удостоверяването на картата (виж допълнение 11)
SW	2	‘XXXXh’	Байтове за състоянието (SW1, SW2)

— Ако командата бъде изпълнена успешно, картата връща ‘**9000**’.

— Ако не е наличен публичен ключ в средата, свързана със защитата от неоторизиран достъп, за състоянието на обработката се връща ‘**6A88**’.

— Ако не е наличен частен ключ в средата, свързана със защитата от неоторизиран достъп, за състоянието на обработката се връща ‘**6A88**’.

— Ако VU.CHR не съвпада с идентификатора на активния публичен ключ, за състоянието на обработката се връща ‘**6A88**’.

— Ако избраният частен ключ се счита за повреден, за състоянието на обработката се връща ‘**6400**’ или ‘**6581**’.

TCS_95 Ако командата INTERNAL_AUTHENTICATE бъде изпълнена успешно, активният ключ на сесията, ако има такъв, се изтрива и не е повече наличен. За да се разполага с нов ключ на сесия, е необходимо да се изпълни успешно командата EXTERNAL AUTHENTICATE за механизма от поколение 1 за удостоверяване на автентичността.

3.5.9 *EXTERNAL AUTHENTICATE*

Тази команда е в съответствие със стандарта ISO/IEC 7816-4.

Чрез командата EXTERNAL AUTHENTICATE картата може да удостовери автентичността на IFD. Процесът на удостоверяване е описан в допълнение 11 за Tachograph G1 и G2 (удостоверяване на автентичността на VU, т.е. на бордовото устройство).

TCS_96 Вариантът на командата за механизма от поколение 1 за взаимно удостоверяване се поддържа само от тахографско приложение от поколение 1.

TCS_97 Вариантът на командата за механизма от второ поколение за взаимно удостоверяване на VU и картата, може да се изпълнява в MF, DF Tachograph и DF Tachograph_G2, виж също TCS_34.

TCS_98 **Командно съобщение**

Байт	Дължина	Стойност	Описание
CLA	1	'00h'	CLA
INS	1	'82h'	INS
P1	1	'00h'	Ключове и алгоритми, известни по подразбиране
P2	1	'00h'	
Lc	1	'XXh'	Lc (дължина на данните, изпратени на картата)
#6-#(5+L)	L	'XX..XXh'	Удостоверяване от поколение 1: криптограма (виж допълнение 11, част А) Удостоверяване от поколение 2: подпис, генериран от IFD (виж допълнение 11, част Б)

TCS_99 **Ответно съобщение**

Байт	Дължина	Стойност	Описание
SW	2	'XXXXh'	Байтове за състоянието (SW1, SW2)

— Ако командата бъде изпълнена успешно, картата връща '**9000**'.

— Ако CHA на избрания публичен ключ не съответства на конкатенацията на AID на тахографското приложение с данните за типа оборудване на бордовото устройство (VU equipment Type), за състоянието на обработката се връща '**6F00**'.

— Ако командата не е непосредствено предшествана от команда GET CHALLENGE, за състоянието на обработката се връща '**6985**'.

Тахографското приложение от поколение 1 може да върне следните допълнителни кодове за грешка:

— Ако не е наличен публичен ключ в средата, свързана със защитата от неоторизиран достъп, се връща '**6A88**'.

— Ако не е наличен частен ключ в средата, свързана със защитата от неоторизиран достъп, за състоянието на обработката се връща '**6A88**'.

— Ако проверката на криптограмата е неуспешна, за състоянието на обработката се връща '**6688**'.

— Ако избраният частен ключ се счита за повреден,, за състоянието на обработката се връща '**6400**' или '**6581**'.

Вариантът на командата за удостоверяване от поколение 2 може да върне следния допълнителен код за грешка:

— Ако проверката на подписа е неуспешна, картата връща '**6300**'.

3.5.10 *GENERAL AUTHENTICATE*

Тази команда се използва при протокола от поколение 2 за удостоверяване автентичността на чип съгласно допълнение 11, част Б и е в съответствие със стандарта ISO/IEC 7816-4.

TCS_100 Командата може да бъде изпълнена в MF, DF Tachograph и DF Tachograph_G2, виж също TCS_34.

TCS_101 **Командно съобщение**

Байт	Дължина	Стойност	Описание
CLA	1	‘00h’	
INS	1	‘86h’	
P1	1	‘00h’	Ключове и протокол, известни по подразбиране
P2	1	‘00h’	
Lc	1	‘NNh’	Lc: дължина на последващото поле за данни
#6-#(5+L)	L	‘7Ch’ + L_{7C} + ‘80h’ + L_{80} + ‘XX..XXh’	Стойност на краткотраен публичен ключ, кодиран по DER-TLV (виж допълнение 11) VU изпраща обектите от данни в тази последователност.

TCS_102 **Ответно съобщение**

Байт	Дължина	Стойност	Описание
#1-#L	L	‘7Ch’ + L_{7C} + ‘81h’ + ‘08h’ + ‘XX..XXh’ + ‘82h’ + L_{82} + ‘XX..XXh’	Кодирани по DER-TLV данни за динамично удостоверяване: еднократен код (nonce) и маркер за удостоверяване на автентичността (виж допълнение 11)
SW	2	‘XXXXh’	Байтове за състоянието (SW1, SW2)

— Ако командата бъде изпълнена успешно, картата връща ‘**9000**’.

— Картата връща ‘**6A80**’, за да укаже за неправилни параметри в полето за данни.

— Картата връща ‘**6982**’, ако командата External Authenticate не е била изпълнена успешно.

Ответният обект Dynamic Authentication Data ‘7Ch’:

— трябва да е наличен, ако операцията е била успешна, т.е. байтовете за състоянието са ‘**9000**’;

— трябва да отсъства в случай на грешка при изпълнението или при проверката, т.е. ако байтовете за състоянието са в интервала ‘**6400**’ — ‘**6FFF**’, и

— може да отсъства в случай на предупреждение, т.е. ако байтовете за състоянието са в интервала ‘**6200**’ — ‘**63FF**’.

3.5.11 *MANAGE SECURITY ENVIRONMENT*

Тази команда служи за определяне на публичен ключ за целите на удостоверяването на автентичността.

3.5.11.1 Двойка команда—отговор от поколение 1

Тази команда е в съответствие със стандарта ISO/IEC 7816-4. Нейното използване е по-ограничено, отколкото съгласно въпросния стандарт.

TCS_103 Тази команда се поддържа само от тахографско приложение от поколение 1.

TCS_104 Ключът, указан в полето за данни MSE, остава активен публичен ключ до следващата правилна команда MSE, селектиране на DF или инициализиране на картата.

TCS_105 Ако указаният ключ не е (вече) наличен в паметта на картата, средата, свързана със защитата от неоторизиран достъп, остава непроменена.

TCS_106 **Командно съобщение**

Байт	Дължина	Стойност	Описание
CLA	1	‘00h’	CLA
INS	1	‘22h’	INS
P1	1	‘C1h’	P1: указан ключ, който е валиден за всички криптографски операции
P2	1	‘B6h’	P2 (указани данни, отнасящи се до цифровия подпис)
Lc	1	‘0Ah’	Lc: дължина на последващото поле за данни
#6	1	‘83h’	Таг, указващ публичен ключ в случаи на асиметрия
#7	1	‘08h’	Дължина на указанието за ключа (идентификатора на ключа)
#8-#15	8	‘XX..XXh’	Идентификатор на ключ съгласно допълнение 11

TCS_107 **Ответно съобщение**

Байт	Дължина	Стойност	Описание
SW	2	‘XXXXh’	Байтове за състоянието (SW1, SW2)

— Ако командата бъде изпълнена успешно, картата връща ‘**9000**’.

— Ако указаният ключ не е наличен в паметта на картата, за състоянието на обработката се връща ‘**6A88**’.

— Ако някои очаквани обекти от данни липсват във формата за защитен от неоторизиран достъп обмен на съобщения, за състоянието на обработката се връща ‘**6987**’. Това може да се случи, ако липсва тагът ‘83h’.

— Ако някои обекти от данни са неправилни, за състоянието на обработката се връща ‘**6988**’. Това може да се случи, ако дължината на идентификатора на ключа не е ‘08h’.

— Ако избраният ключ се счита за повреден, за състоянието на обработката се връща ‘**6400**’ или ‘**6581**’.

3.5.11.2 Двойки команда—отговор от поколение 2

За удостоверяването от поколение 2 тахографската карта поддържа следните версии на командата MSE: Set, които са в съответствие със стандарта ISO/IEC 7816-4. Тези версии на командата не се поддържат от удостоверяването от поколение 1.

3.5.11.2.1 MSE:SET AT за удостоверяване автентичността на чипа

Следната команда MSE:SET AT се използва за избор на параметрите за удостоверяване автентичността на чипа (Chip Authentication), което се извършва от последващата команда General Authenticate.

TCS_108 Командата може да бъде изпълнена в MF, DF Tachograph и DF Tachograph_G2, виж също TCS_34.

TCS_109 **Командно съобщение MSE:SET AT за удостоверяване автентичността на чипа**

Байт	Дължина	Стойност	Описание
CLA	1	‘00h’	
INS	1	‘22h’	

Байт	Дължина	Стойност	Описание
P1	1	‘41h’	Зададена за вътрешно удостоверяване на автентичността
P2	1	‘A4h’	Удостоверяване на автентичността
Lc	1	‘NNh’	Lc: дължина на последващото поле за данни
#6-#(5+L)	L	‘80h’ + ‘0Ah’ + ‘XX..XXh’	Кодирано по DER-TLV указание към криптографския механизъм: идентификатор на обекта за удостоверяване автентичността на чипа (само стойност, тагът ‘06h’ се изпуска). Виж допълнение 1 за стойностите на идентификаторите на обекти; трябва да се използва обозначаването по байтове. Виж допълнение 11 за указания относно това как да се избере един от тези идентификатори на обекти.

3.5.11.2.2 MSE:SET AT за удостоверяване автентичността на бордовото устройство (VU)

Следната команда MSE:SET AT се използва за избор на параметрите и ключовете за удостоверяване автентичността на бордовото устройство (VU Authentication), което се извършва от последващата команда External Authenticate.

TCS_110 Командата може да бъде изпълнена в MF, DF Tachograph и DF Tachograph_G2, виж също TCS_34.

TCS_111 **Командно съобщение MSE:SET AT за удостоверяване автентичността на VU**

Байт	Дължина	Стойност	Описание
CLA	1	‘00h’	
INS	1	‘22h’	
P1	1	‘81h’	Зададена за външно удостоверяване на автентичността
P2	1	‘A4h’	Удостоверяване на автентичността
Lc	1	‘NNh’	Lc: дължина на последващото поле за данни
#6-#(5+L)	L	‘80h’ + ‘0Ah’ + ‘XX..XXh’	Кодирано по DER-TLV указание към криптографския механизъм: идентификатор на обекта за удостоверяване автентичността на VU (само стойност, тагът ‘06h’ се изпуска). Виж допълнение 1 за стойностите на идентификаторите на обекти; трябва да се използва обозначаването по байтове. Виж допълнение 11 за указания относно това как да се избере един от тези идентификатори на обекти.
		‘83h’ + ‘08h’ + ‘XX..XXh’	Кодирано по DER-TLV указание за публичния ключ на VU чрез указанието за титуляря на сертификата (Certificate Holder Reference), посочено в този сертификат.
		‘91h’ + L_{91} + ‘XX..XXh’	Кодирано по DER-TLV компресирано представяне на краткотрайния публичен ключ на VU, който ще се използва по време на удостоверяването на автентичността на чипа (виж допълнение 11)

3.5.11.2.3 MSE:SET DST

Следната команда MSE:SET DST се използва за установяването на публичен ключ или

— за проверка на подпис, който се предоставя в последваща команда PSO: Verify Digital Signature, или

— за проверка по подпис на сертификат, който се предоставя в последваща команда PSO: Verify Certificate

TCS_112 Тази команда може да бъде изпълнена в MF, DF Tachograph и DF Tachograph_G2, виж също TCS_33.

TCS_113 **Командно съобщение MSE:SET DST**

Байт	Дължина	Стойност	Описание
CLA	1	‘00h’	
INS	1	‘22h’	
P1	1	‘81h’	Установяване за проверка
P2	1	‘B6h’	Цифров подпис
Lc	1	‘NNh’	Lc: дължина на последващото поле за данни
#6-#(5+L)	L	‘83h’ + ‘08h’ + ‘XX...XXh’	Кодирано по DER-TLV указание за публичен ключ, т.е. указание за титуляря на сертификата (Certificate Holder Reference) в сертификата на публичния ключ (виж допълнение 11)

За всички версии на командата структурата и байтовете за състоянието на ответното съобщение се дават от:

TCS_114 **Ответно съобщение**

Байт	Дължина	Стойност	Описание
SW	2	‘XXXXh’	Байтове за състоянието (SW1, SW2)

— Ако командата бъде изпълнена успешно, картата връща ‘**9000**’. Протоколът е избран и активиран.

— ‘**6A80**’ сочи неправилни параметри в полето за данни на командата.

— ‘**6A88**’ сочи, че указаните данни (т.е. указан ключ) не са налични.

3.5.12 *PSO: HASH*

Тази команда се използва за прехвърляне към картата на резултата от изчисляването на хеш-стойността за някои данни. Тази команда служи за проверката на цифрови подписи. Хеш-стойността се съхранява временно за последващата команда PSO: Verify Digital Signature.

Тази команда е в съответствие със стандарта ISO/IEC 7816-8. Нейното използване е по-ограничено, отколкото съгласно въпросния стандарт.

Само за контролната карта се изисква да поддържа тази команда в DF Tachograph и DF Tachograph_G2.

Другите видове тахографски карти могат или не могат да изпълняват тази команда. Тази команда може или не може да е достъпна в MF.

Приложението от поколение 1 за контролната карта поддържа само SHA-1.

TCS_115 Временно съхранената хеш-стойност се заличава, ако бъде изчислена нова хеш-стойност посредством командата PSO: HASH, ако бъде селектиран DF и ако тахографската карта бъде инициализирана.

TCS_116 **Командно съобщение**

Байт	Дължина	Стойност	Описание
CLA	1	‘00h’	CLA
INS	1	‘2Ah’	Извършване на операция, свързана със защитата от неоторизиран достъп
P1	1	‘90h’	Връщане на хеш-кода
P2	1	‘A0h’	Таг: поле за данни, съдържащо съответните обекти от данни (DO) за хеширането
Lc	1	‘XXh’	Дължина Lc на последващото поле за данни
#6	1	‘90h’	Таг за хеш-кода
#7	1	‘XXh’	Дължина L на хеш-кода: ‘14h’ в приложение от поколение 1 (виж допълнение 11, част А) ‘20h’, ‘30h’ или ‘40h’ в приложение от поколение 2 (виж допълнение 11, част Б)
#8-#(7+L)	L	‘XX..XXh’	Хеш-код

TCS_117 **Ответно съобщение**

Байт	Дължина	Стойност	Описание
SW	2	‘XXXXh’	Байтове за състоянието (SW1, SW2)

— Ако командата бъде изпълнена успешно, картата връща ‘**9000**’.

— Ако някои очаквани обекти от данни (както е определено по-горе) липсват, за състоянието на обработката се връща ‘**6987**’ Това може да се случи, ако един от таговете ‘90h’ липсва.

— Ако някои обекти от данни са неправилни, за състоянието на обработката се връща ‘**6988**’. Тази грешка възниква, ако изискваният таг е наличен, но неговата дължина се различава от ‘14h’ за SHA-1, ‘20h’ за SHA-256, ‘30h’ за SHA-384 и ‘40h’ за SHA-512 (за приложение от поколение 2).

3.5.13 *PERFORM HASH of FILE*

Тази команда не е в съответствие със стандарта ISO/IEC 7816-8. Поради това байтът CLA на тази команда указва, че е налице частно използване на PERFORM SECURITY OPERATION / HASH.

Само за картата на водач и за контролната карта се изисква да поддържат тази команда в DF Tachograph и DF Tachograph_G2.

Другите видове тахографски карти могат или не могат да изпълняват тази команда. Ако карта на превозвач или контролна карта изпълнява тази команда, това трябва да става, както е определено в настоящата глава.

Тази команда може или не може да е достъпна в MF. Ако командата е достъпна, тя се изпълнява, както е определено в настоящата глава, т.е. не позволява изчисляването на хеш-стойност, а се прекратява с подходящ код за грешка.

TCS_118 Командата PERFORM HASH of FILE се използва за хеширане на зоната за данни на селектирания елементарен файл (EF) с прозрачна структура.

TCS_119 Тахографската карта поддържа тази команда само за EF, които са изброени в глава 4 в рамките на DF_Tachograph и DF_Tachograph_G2, със следното изключение. Тахографската карта не трябва да поддържа командата за елементарния файл Sensor_Installation_Data на DF Tachograph_G2.

TCS_120 Резултатът от операцията по хеширане се съхранява временно в картата. След това тя може да се използва, за да се получи цифров подпис за файла посредством командата PSO: COMPUTE DIGITAL SIGNATURE.

TCS_121 Временно съхраняваната хеш-стойност на файла се заличава, ако бъде изчислена нова хеш-стойност на файла посредством командата PSO: Hash of File command, ако бъде селектиран DF и ако тахографската карта бъде инициализирана.

TCS_122 Тахографското приложение от поколение 1 трябва да поддържа SHA-1.

TCS_123 Тахографското приложение от поколение 2 трябва да поддържа SHA-1 и SHA-2 (256, 384 и 512 бита).

TCS_124 **Командно съобщение**

Байт	Дължина	Стойност	Описание
CLA	1	‘80h’	CLA
INS	1	‘2Ah’	Извършване на операция, свързана със защитата от неоторизиран достъп
P1	1	‘90h’	Tar: Hash
P2	1	‘XXh’	P2: Посочва алгоритъма, който трябва да се използва за хеширане на данните, записани в селектирания файл с прозрачна структура: ‘00h’ за SHA-1 ‘01h’ за SHA-256 ‘02h’ за SHA-384 ‘03h’ за SHA-512

TCS_125 **Ответно съобщение**

Байт	Дължина	Стойност	Описание
SW	2	‘XXXXh’	Байтове за състоянието (SW1, SW2)

— Ако командата бъде изпълнена успешно, картата връща ‘**9000**’.

— Ако активният EF не позволява тази команда (EF Sensor_Installation_Data в DF Tachograph_G2), за състоянието на обработката се връща ‘**6985**’.

— Ако селектираният EF се счита за повреден (открита е грешка в цялостността на атрибутите на файла или в съхранените в него данни), за състоянието на обработката се връща ‘**6400**’ или ‘**6581**’.

— Ако селектираният файл не е с прозрачна структура или ако няма активен EF, за състоянието на обработката се връща ‘**6986**’.

3.5.14 *PSO: COMPUTE DIGITAL SIGNATURE*

Тази команда служи за изчисляване на цифровия подпис на изчислен преди това хеш-код (виж PERFORM HASH of FILE, точка 3.5.13).

Само за картата на водач и за контролната карта се изисква да поддържат тази команда в DF Tachograph и DF Tachograph_G2.

Другите видове тахографски карти могат или не могат да изпълняват тази команда, но не трябва да имат ключ за подписа. Поради това тези карти не могат да изпълняват командата успешно, а прекратяват изпълнението с подходящ код за грешка.

Тази команда може или не може да е достъпна в MF. Ако командата е достъпна, нейното изпълнение се прекратява с подходящ код за грешка.

Тази команда е в съответствие със стандарта ISO/IEC 7816-8. Нейното използване е по-ограничено, отколкото съгласно въпросния стандарт.

TCS_126 Тази команда не изчислява цифров подпис за изчислен преди това хеш-код с командата PSO: HASH.

TCS_127 За изчисляване на цифровия подпис се използва частния ключ на картата, на която той е известен по подразбиране.

TCS_128 Тахографското приложение от поколение 1 изпълнява цифров подпис, като използва метод на запълване в съответствие с PKCS1 (виж в допълнение 11 за подробности).

TCS_129 Тахографското приложение от поколение 2 изчислява цифров подпис въз основа на елиптична крива (виж допълнение 11 за подробности).

TCS_130 **Командно съобщение**

Байт	Дължина	Стойност	Описание
CLA	1	'00h'	CLA
INS	1	'2Ah'	Извършване на операция, свързана със защитата от неоторизиран достъп
P1	1	'9Eh'	Цифров подпис, който трябва да се върне
P2	1	'9Ah'	Таг: поле за данни съдържащо данните, които трябва да се подпишат. Тъй като не е включено поле за данни, се приема, че данните вече са налични в картата (хеширане на файла)
Le	1	'NNh'	Дължина на очаквания подпис

TCS_131 **Ответно съобщение**

Байт	Дължина	Стойност	Описание
#1-#L	L	'XX..XXh'	Подпис за изчисленото преди това хеширане
SW	2	'XXXXh'	Байтове за състоянието (SW1, SW2)

— Ако командата бъде изпълнена успешно, картата връща '**9000**'.

— Ако избраният по подразбиране частен ключ се счита за повреден, за състоянието на обработката се връща '**6400**' или '**6581**'.

— Ако хеширането, изчислено с предходна команда Perform Hash of File не е налично, за състоянието на обработката се връща '**6985**'.

3.5.15 *PSO: VERIFY DIGITAL SIGNATURE*

Тази команда служи за проверка на въведения цифров подпис, чието хеширане е известно на картата. Алгоритъмът на подписа е известен по подразбиране на картата.

Тази команда е в съответствие със стандарта ISO/IEC 7816-8. Нейното използване е по-ограничено, отколкото съгласно въпросния стандарт.

Само за контролната карта се изисква да поддържа тази команда в DF Tachograph и DF Tachograph_G2.

Другите видове тахографски карти могат или не могат да изпълняват тази команда. Тази команда може или не може да е достъпна в MF.

TCS_132 Командата VERIFY DIGITAL SIGNATURE използва винаги публичния ключ, избран посредством предходната команда Manage Security Environment MSE: Set DST, и предишния хеш-код, въведен с команда PSO: HASH.

TCS_133 **Командно съобщение**

Байт	Дължина	Стойност	Описание
CLA	1	‘00h’	CLA
INS	1	‘2Ah’	Извършване на операция, свързана със защитата от неоторизиран достъп
P1	1	‘00h’	
P2	1	‘A8h’	Таг: поле за данни, съдържащо съответните обекти от данни (DO) за проверката
Lc	1	‘83h’	Дължина Lc на последващото поле за данни
6	1	‘9Eh’	Таг за цифров подпис
#7-#8	2	‘81 XXh’	Дължина на цифровия подпис: 128 байта, кодирани в съответствие с допълнение 11, част А за тахографско приложение от поколение 1 в зависимост от избраната крива за тахографско приложение от поколение 2 (виж допълнение 11, част Б)
#9-#(8+L)	L	‘XX..XXh’	Съдържание на цифровия подпис

TCS_134 **Ответно съобщение**

Байт	Дължина	Стойност	Описание
SW	2	‘XXXXh’	Байтове за състоянието (SW1, SW2)

— Ако командата бъде изпълнена успешно, картата връща ‘**9000**’.

— Ако проверката на подписа е неуспешна, за състоянието на обработката се връща ‘**6688**’. Процесът на проверка е описан подробно в допълнение 11.

— Ако не е избран публичен ключ, за състоянието на обработката се връща ‘**6A88**’.

— Ако някои очаквани обекти от данни (както е определено по-горе) липсват, за състоянието на обработката се връща ‘**6987**’ Това може да стане, ако липсва един от изискваните тагове.

— Ако не е наличен хеш-код за изпълнение на командата (в резултат на предходна команда PSO: Hash), за състоянието на обработката се връща ‘**6985**’.

— Ако някои обекти от данни са неправилни, за състоянието на обработката се връща ‘**6988**’. Това може да се случи, ако дължината на някой от изискваните обекти от данни е неправилна.

— Ако избраният публичен ключ се счита за повреден, за състоянието на обработката се връща ‘**6400**’ или ‘**6581**’.

3.5.16 *PROCESS DSRC MESSAGE*

Тази команда служи за проверка на цялостността и автентичността на съобщения по специализирана връзка с малък обсег на действие („DSRC съобщения“) и за дешифриране на данните, съобщени от VU на контролен орган или сервиз по такава връзка. Картата извлича криптографския ключ и MAC ключовете, използвани за защитата на DSRC съобщението от неоторизиран достъп, както е описано в допълнение 11, част Б, глава 13.

Само за контролната карта и картата за монтаж и настройки се изисква да поддържат тази команда в DF Tachograph_G2.

Другите видове тахографски карти могат или не могат да изпълняват тази команда, но не трябва да имат главен ключ за DSRC съобщения. Поради това тези карти не могат да изпълняват командата успешно, а прекратяват изпълнението с подходящ код за грешка.

Тази команда може или не може да е достъпна в MF и/или DF Tachograph. Ако командата е достъпна, нейното изпълнение се прекратява с подходящ код за грешка.

TCS_135 Главният ключ за DSRC съобщения е достъпен само в DF Tachograph_G2, т.е. контролната карта и картата за монтаж и настройки трябва да поддържат успешното изпълнение на командата само в DF Tachograph_G2.

TCS_136 Командата само декриптира DSRC данните и проверява криптографската контролна сума, но не интерпретира входящите данни.

TCS_137 Последователността на обектите от данни в полето за данни на командата е неизменна и се определя от настоящата спецификация.

TCS_138 **Командно съобщение**

Байт	Дължина	Стойност	Описание
CLA	1	‘80h’	Собствен CLA
INS	1	‘2Ah’	Извършване на операция, свързана със защитата от неоторизиран достъп
P1	1	‘80h’	Данни за отговора: проста стойност
P2	1	‘B0h’	Данни за командата: проста стойност, кодирана по BER-TLV и включваща обекти от данни (DO) със защитен обмен на съобщения (SM)
Lc	1	‘NNh’	Дължина Lc на последващото поле за данни
#6-#(5+L)	L	‘87h’ + L_{87} + ‘XX..XXh’	Кодиран по DER-TLV указателен байт за запълващото съдържание, последван от криптирани данни за натоварването на тахографа. Указателният байт за запълващото съдържание трябва да бъде със стойност ‘00h’ (‘no further indication’, т. е. „без допълнително указване“, съгласно ISO/IEC 7816-4:2013, таблица 52). За механизма за криптиране виж допълнение 11, част Б, глава 13. Позволени стойности за дължината L_{87} са кратните на дължината на AES блока плюс 1 за указателния байт за запълващото съдържание, т.е. от 17 байта до 193 байта включително. *Забележка:* виж ISO/IEC 7816-4:2013, таблица 49 за обекта от данни със защитен обмен на съобщения с таг ‘87h’.
		‘81h’ + ‘10h’	Кодирано по DER-TLV вместване съгласно стандартния модел за контрол с оглед на поверителността (Control Reference Template for Confidentiality) на конкатенацията на следните елементи на данните (виж допълнение 1 DSRCSecurityData и допълнение 11, част Б, глава 13): — времеви печат от 4 байта — брояч от 3 байта — сериен номер на VU от 8 байта — версия от 1 байт на главния ключ за DSRC съобщения *Забележка:* виж ISO/IEC 7816-4:2013, таблица 49 за обекта от данни със защитен обмен на съобщения с таг ‘81h’.
		‘8Eh’ + L_{8E} + ‘XX..XXh’	Кодиран по DER-TLV MAC за DSRC съобщението. За алгоритъма за MAC и неговото изчисляване виж допълнение 11, част Б, глава 13. *Забележка:* виж ISO/IEC 7816-4:2013, таблица 49 за обекта от данни със защитен обмен на съобщения с таг ‘8Eh’.

TCS_139 **Ответно съобщение**

Байт	Дължина	Стойност	Описание
#1-#L	L	‘XX..XXh’	Отсъства (в случай на грешка) или дешифрирани данни (запълването е отстранено)
SW	2	‘XXXXh’	Байтове за състоянието (SW1, SW2)

— Ако командата бъде изпълнена успешно, картата връща ‘**9000**’.

— ‘**6A80**’ указва за неправилни параметри в полето за данни на командата, (използва се и когато обектите от данни не са изпратени в определената последователност).

— ‘**6A88**’ сочи, че указаните данни, т.е. указаният главен ключ за DSRC съобщения, не са налични.

— ‘**6900**’ указва, че проверката на криптографската контролна сума или на описанието на данните не е била успешна.

4. СТРУКТУРА НА ТАХОГРАФСКИТЕ КАРТИ

В настоящата глава се определя структурата на файловете в тахографските карти за съхраняване на достъпните данни.

Не се определя вътрешната структура, която зависи от производителя от картата — например заглавната част на файла, нито съхраняването и обработването на необходимите само за вътрешна употреба елементи на данните — например `EuropeanPublicKey`, `CardPrivateKey`, `TdesSessionKey` или `WorkshopCardPin`.

TCS_140 Тахографската карта от поколение 2 трябва да съдържа главния файл (MF) и тахографско приложение от поколение 1 и от поколение 2 от същия вид (например приложение за карта на водач).

TCS_141 Тахографската карта трябва да поддържа поне минималния брой записи, определен за съответните приложения, и да поддържа не повече от максималния брой записи, определен за съответните приложения.

Максималният и минималният брой на записите за различните приложения са определени в настоящата глава.

Условията за сигурност, използвани в правилата за достъп в рамките на тази глава, са посочени в глава 3.3. По принцип режимът на достъп „Четене“ („Read“) означава командата READ BINARY с четен и, ако се поддържа, нечетен байт INS — с изключение на елементарния файл (EF) Sensor_Installation_Data на картата за монтаж и настройки, виж TCS_156 и TCS_160. Режимът на достъп „Актуализация“ („Update“) означава командата READ BINARY с четен и, ако се поддържа, нечетен байт INS, а режимът на достъп „Селектиране“ („Select“) — командата SELECT.

4.1. Главен файл (MF)

TCS_142 След персонализирането на главния файл (MF) той трябва да е със следната постоянна файлова структура и правила за достъп до файловете:

Забележка: краткият идентификатор на EF (SFID) се дава като десетично число — например стойността 30 съответства на 11110 в двоичната бройна система.

			Праила за достъп	
Файл	**Идентификатор на файла**	**SFID**	**Четене / Селектиране**	**Актуализация**
MF	‘3F00h’			
├─ EF ICC	‘0002h’		ALW	NEV
├─ EF IC	‘0005h’		ALW	NEV
├─ EF DIR	‘2F00h’	30	ALW	NEV
├─ EF ATR/INFO (условен)	‘2F01h’	29	ALW	NEV
├─ EF Extended_Length (условен)	‘0006h’	28	ALW	NEV
├─ DF Tachograph	‘0500h’		SC1	
└─ DF Tachograph_G2			SC1	

В тази таблица се използва следното съкращение за условието за сигурност:

SC1 ALW ИЛИ SM-MAC-G2

TCS_143 Структурите на всички EF трябва да бъдат прозрачни.

TCS_144 Главният файл (MF) трябва да е със следната структура на данните:

Файл / елемент на данни	Брой записи	Размер (байтове) Мин.	Макс.	Стойности по подразбиране
MF		*63*	*184*	
EF ICC		*25*	*25*	
CardIccIdentification		*25*	*25*	
clockStop		1	1	{00}
cardExtendedSerialNumber		8	8	{00..00}
cardApprovalNumber		8	8	{20..20}
cardPersonaliserID		1	1	{00}
embedderIcAssemblerId		5	5	{00..00}
icIdentifier		2	2	{00 00}
EF IC		*8*	*8*	
CardChipIdentification		*8*	*8*	
icSerialNumber		4	4	{00..00}
icManufacturingReferences		4	4	{00..00}
EF DIR		*20*	*20*	
See TCS_145		*20*	*20*	{00..00}
EF ATR/INFO		*7*	*128*	
See TCS_146		*7*	*128*	{00..00}
EF EXTENDED_LENGTH		*3*	*3*	
See TCS_147		*3*	*3*	{00..00}
DF Tachograph				
DF Tachograph_G2				

TCS_145 Елементарният файл EF DIR трябва да съдържа следните обекти от данни, свързани с приложението: ‘61 08 4F 06 FF 54 41 43 48 4F 61 08 4F 06 FF 53 4D 52 44 54’

TCS_146 Елементарният файл EF ATR/INFO трябва да е наличен, ако тахографската карта указва в своя ATR, че поддържа полета с увеличена дължина. В този случай EF ATR/INFO трябва да съдържа обекта от данни с увеличена дължина (DO‘7F66’), определен в ISO/IEC 7816-4:2013, клауза 12.7.1.

TCS_147 Елементарният файл EF Extended_Length трябва да е наличен, ако тахографската карта указва в своя ATR, че поддържа полета с увеличена дължина. В този случай EF трябва да съдържа следния обект от данни: ‘02 01 xx’ където стойността ‘xx’ указва дали за протокола T = 1 и / или T = 0 се поддържат полета с увеличена дължина.

Стойността ‘01’ указва, че за протокола T = 1 се поддържат полета с увеличена дължина.

Стойността ‘10’ указва, че за протокола T = 0 се поддържат полета с увеличена дължина.

Стойността ‘11’ указва, че за протоколите T = 1 и T = 0 се поддържат полета с увеличена дължина.

4.2. Приложения за картата на водач

4.2.1 *Приложение от поколение 1 за картата на водач*

TCS_148 След персонализирането на приложението от поколение 1 за картата на водач то трябва да е със следната постоянна файлова структура и правила за достъп до файловете:

Файл	Идентификатор на файла	Правила за достъп		
		Четене	Селектиране	Актуализация
└─DF Tachograph	‘0500h’		SC1	
├─EF Application_Identification	‘0501h’	SC2	SC1	NEV
├─EF Card_Certificate	‘C100h’	SC2	SC1	NEV
├─EF CA_Certificate	‘C108h’	SC2	SC1	NEV
├─EF Identification	‘0520h’	SC2	SC1	NEV
├─EF Card_Download	‘050Eh’	SC2	SC1	SC1
├─EF Driving_Licence_Info	‘0521h’	SC2	SC1	NEV
├─EF Events_Data	‘0502h’	SC2	SC1	SC3
├─EF Faults_Data	‘0503h’	SC2	SC1	SC3
├─EF Driver_Activity_Data	‘0504h’	SC2	SC1	SC3
├─EF Vehicles_Used	‘0505h’	SC2	SC1	SC3
├─EF Places	‘0506h’	SC2	SC1	SC3
├─EF Current_Usage	‘0507h’	SC2	SC1	SC3
├─EF Control_Activity_Data	‘0508h’	SC2	SC1	SC3
└─EF Specific_Conditions	‘0522h’	SC2	SC1	SC3

В тази таблица се използват следните съкращения за условията за сигурност:

SC1 ALW ИЛИ SM-MAC-G2

SC2 ALW ИЛИ SM-MAC-G1 ИЛИ SM-MAC-G2

SC3 SM-MAC-G1 ИЛИ SM-MAC-G2

TCS_149 Структурите на всички EF трябва да бъдат прозрачни.

TCS_150 Приложението от поколение 1 за картата на водач трябва да е със следната структура на данните:

Файл / елемент на данни	Брой записи	Размер (байтове) Мин.	Макс.	Стойности по подразбиране
DF Tachograph		*11378*	*24926*	
EF Application_Identification		*10*	*10*	
DriverCardApplicationIdentification		*10*	*10*	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfEventsPerType		1	1	{00}
noOfFaultsPerType		1	1	{00}
activityStructureLength		2	2	{00 00}
noOfCardVehicleRecords		2	2	{00 00}
noOfCardPlaceRecords		1	1	{00}
EF Card_Certificate		*194*	*194*	
CardCertificate		194	194	{00..00}
EF CA_Certificate		*194*	*194*	
MemberStateCertificate		194	194	{00..00}
EF Identification		*143*	*143*	
CardIdentification		*65*	*65*	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
DriverCardHolderIdentification		*78*	*78*	
cardHolderName		*72*	*72*	
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00, 20..20}
cardHolderBirthDate		4	4	{00..00}
cardHolderPreferredLanguage		2	2	{20 20}
EF Card_Download		*4*	*4*	
LastCardDownload		4	4	
EF Driving_Licence_Info		*53*	*53*	
CardDrivingLicenceInformation		*53*	*53*	
drivingLicenceIssuingAuthority		36	36	{00, 20..20}
drivingLicenceIssuingNation		1	1	{00}
drivingLicenceNumber		16	16	{20..20}
EF Events_Data		*864*	*1728*	
CardEventData		*864*	*1728*	
cardEventRecords	6	*144*	*288*	
CardEventRecord	n_1	*24*	*24*	
eventType		1	1	{00}
eventBeginTime		4	4	{00..00}
eventEndTime		4	4	{00..00}
eventVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Faults_Data		*576*	*1152*	
CardFaultData		*576*	*1152*	
cardFaultRecords	2	*288*	*576*	
CardFaultRecord	n_2	*24*	*24*	
faultType		1	1	{00}
faultBeginTime		4	4	{00..00}
faultEndTime		4	4	{00..00}
faultVehicleRegistration				

├─vehicleRegistrationNation		1	1	{00}
└─vehicleRegistrationNumber		14	14	{00, 20..20}
EF Driver_Activity_Data		*5548*	*13780*	
└CardDriverActivity		*5548*	*13780*	
├─activityPointerOldestDayRecord		2	2	{00 00}
├─activityPointerNewestRecord		2	2	{00 00}
└─activityDailyRecords	n_6	5544	13776	{00..00}
EF Vehicles_Used		*2606*	*6202*	
└CardVehiclesUsed		*2606*	*6202*	
├─vehiclePointerNewestRecord		2	2	{00 00}
└─cardVehicleRecords		*2604*	*6200*	
└─CardVehicleRecord	n_3	*31*	*31*	
├─vehicleOdometerBegin		3	3	{00..00}
├─vehicleOdometerEnd		3	3	{00..00}
├─vehicleFirstUse		4	4	{00..00}
├─vehicleLastUse		4	4	{00..00}
├─vehicleRegistration				
├─vehicleRegistrationNation		1	1	{00}
└─vehicleRegistrationNumber		14	14	{00, 20..20}
└─vuDataBlockCounter		2	2	{00 00}
EF Places		*841*	*1121*	
└CardPlaceDailyWorkPeriod		*841*	*1121*	
├─placePointerNewestRecord		1	1	{00}
└─placeRecords		*840*	*1120*	
└─PlaceRecord	n_4	*10*	*10*	
├─entryTime		4	4	{00..00}
├─entryTypeDailyWorkPeriod		1	1	{00}
├─dailyWorkPeriodCountry		1	1	{00}
├─dailyWorkPeriodRegion		1	1	{00}
└─vehicleOdometerValue		3	3	{00..00}
EF Current_Usage		*19*	*19*	
└CardCurrentUse		*19*	*19*	
├─sessionOpenTime		4	4	{00..00}
└─sessionOpenVehicle				
├─vehicleRegistrationNation		1	1	{00}
└─vehicleRegistrationNumber		14	14	{00, 20..20}
EF Control_Activity_Data		*46*	*46*	
└CardControlActivityDataRecord		*46*	*46*	
├─controlType		1	1	{00}
├─controlTime		4	4	{00..00}
├─controlCardNumber				
├─cardType		1	1	{00}
├─cardIssuingMemberState		1	1	{00}
└─cardNumber		16	16	{20..20}
├─controlVehicleRegistration				
├─vehicleRegistrationNation		1	1	{00}
└─vehicleRegistrationNumber		14	14	{00, 20..20}
├─controlDownloadPeriodBegin		4	4	{00..00}
└─controlDownloadPeriodEnd		4	4	{00..00}
EF Specific_Conditions		*280*	*280*	
└SpecificConditionRecord	56	*5*	*5*	
├─entryTime		4	4	{00..00}
└─SpecificConditionType		1	1	{00}

TCS_151 Следните стойности, използвани за указване на размери в таблицата по-горе, определят минималния и максималния брой на записите, който трябва да се използва за приложение от поколение 1 в структурата на данните в картата на водача:

		Мин.	Макс.
n_1	NoOfEventsPerType	6	12
n_2	NoOfFaultsPerType	12	24
n_3	NoOfCardVehicleRecords	84	200
n_4	NoOfCardPlaceRecords	84	112
n_6	CardActivityLengthRange	5 544 байта (28 дни * 93 промени на дейността)	13 776 байта (28 дни * 240 промени на дейността)

4.2.2 *Приложение от поколение 2 за картата на водача*

TCS_152 След персонализирането на приложението от поколение 2 за картата на водача то трябва да е със следната постоянна файлова структура и правила за достъп до файловете:

Забележка: краткият идентификатор на EF (SFID) се дава като десетично число — например стойността 30 съответства на 11110 в двоичната бройна система.

			Правила за достъп	
Файл	**Идентификатор на файла**	**SFID**	**Четене / Селектиране**	**Актуализация**
└─ DF Tachograph_G2			SC1	
├─ EF Application_Identification	‘0501h’	1	SC1	NEV
├─ EF CardMA_Certificate	‘C100h’	2	SC1	NEV
├─ EF CardSignCertificate	‘C101h’	3	SC1	NEV
├─ EF CA_Certificate	‘C108h’	4	SC1	NEV
├─ EF Link_Certificate	‘C109h’	5	SC1	NEV
├─ EF Identification	‘0520h’	6	SC1	NEV
├─ EF Card_Download	‘050Eh’	7	SC1	SC1
├─ EF Driving_Licence_Info	‘0521h’	10	SC1	NEV
├─ EF Events_Data	‘0502h’	12	SC1	SM-MAC-G2
├─ EF Faults_Data	‘0503h’	13	SC1	SM-MAC-G2
├─ EF Driver_Activity_Data	‘0504h’	14	SC1	SM-MAC-G2
├─ EF Vehicles_Used	‘0505h’	15	SC1	SM-MAC-G2
├─ EF Places	‘0506h’	16	SC1	SM-MAC-G2
├─ EF Current_Usage	‘0507h’	17	SC1	SM-MAC-G2
├─ EF Control_Activity_Data	‘0508h’	18	SC1	SM-MAC-G2
├─ EF Specific_Conditions	‘0522h’	19	SC1	SM-MAC-G2
├─ EF VehicleUnits_Used	‘0523h’	20	SC1	SM-MAC-G2
└─ EF GNSS_Places	‘0524h’	21	SC1	SM-MAC-G2

В тази таблица се използва следното съкращение за условието за сигурност:

SC1 ALW ИЛИ SM-MAC-G2

TCS_153 Структурите на всички EF трябва да бъдат прозрачни.

TCS_154 Приложението от поколение 2 за картата на водача трябва да е със следната структура на данните:

Файл / елемент на данни	Брой записи	Размер (байтове) Мин.	Макс.	Стойности по подразбиране
DF Tachograph_G2		*19510*	*39306*	
EF Application_Identification		*15*	*15*	
DriverCardApplicationIdentification		*15*	*15*	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfEventsPerType		1	1	{00}
noOfFaultsPerType		1	1	{00}
activityStructureLength		2	2	{00 00}
noOfCardVehicleRecords		2	2	{00 00}
noOfCardPlaceRecords		2	2	{00}
noOfGNSSCDRecords		2	2	{00 00}
noOfSpecificConditionRecords		2	2	{00}
EF CardMA_Certificate		*204*	*341*	
CardMACertificate		204	341	{00..00}
EF CardSignCertificate		*204*	*341*	
CardSignCertificate		204	341	{00..00}
EF CA_Certificate		*204*	*341*	
MemberStateCertificate		204	341	{00..00}
EF Link_Certificate		*204*	*341*	
LinkCertificate		204	341	{00..00}
EF Identification		*143*	*143*	
CardIdentification		*65*	*65*	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
DriverCardHolderIdentification		*78*	*78*	
cardHolderName		*72*	*72*	
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00, 20..20}
cardHolderBirthDate		4	4	{00..00}
cardHolderPreferredLanguage		2	2	{20 20}
EF Card_Download		*4*	*4*	
LastCardDownload		4	4	
EF Driving_Licence_Info		*53*	*53*	
CardDrivingLicenceInformation		*53*	*53*	
drivingLicenceIssuingAuthority		36	36	{00, 20..20}
drivingLicenceIssuingNation		1	1	{00}
drivingLicenceNumber		16	16	{20..20}
EF Events_Data		*1584*	*3168*	
CardEventData		*1584*	*3168*	
cardEventRecords	11	*144*	*288*	
CardEventRecord	n_1	*24*	*24*	
eventType		1	1	{00}
eventBeginTime		4	4	{00..00}
eventEndTime		4	4	{00..00}
eventVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Faults_Data		*576*	*1152*	
CardFaultData		*576*	*1152*	
cardFaultRecords	2	*288*	*576*	
CardFaultRecord	n_2	*24*	*24*	

faultType		1	1	{00}
faultBeginTime		4	4	{00..00}
faultEndTime		4	4	{00..00}
faultVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Driver_Activity_Data		*5548*	*13780*	
CardDriverActivity		*5548*	*13780*	
activityPointerOldestDayRecord		2	2	{00 00}
activityPointerNewestRecord		2	2	{00 00}
activityDailyRecords	n_6	5544	13776	{00..00}
EF Vehicles_Used		*4034*	*9602*	
CardVehiclesUsed		*4034*	*9602*	
vehiclePointerNewestRecord		2	2	{00 00}
cardVehicleRecords		*4032*	*9600*	
CardVehicleRecord	n_3	*48*	*48*	
vehicleOdometerBegin		3	3	{00..00}
vehicleOdometerEnd		3	3	{00..00}
vehicleFirstUse		4	4	{00..00}
vehicleLastUse		4	4	{00..00}
vehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
vuDataBlockCounter		2	2	{00 00}
vehicleIdentificationNumber		17	17	{20..20}
EF Places		*1766*	*2354*	
CardPlaceDailyWorkPeriod		*1766*	*2354*	
placePointerNewestRecord		2	2	{00 00}
placeRecords		*1764*	*2352*	
PlaceRecord	n_4	*21*	*21*	
entryTime		4	4	{00..00}
entryTypeDailyWorkPeriod		1	1	{00}
dailyWorkPeriodCountry		1	1	{00}
dailyWorkPeriodRegion		1	1	{00}
vehicleOdometerValue		3	3	{00..00}
entryGNSSPlaceRecord		11	11	
timeStamp		4	4	{00..00}
gnssAccuracy		1	1	{00}
geoCoordinates		6	6	{00..00}
EF Current_Usage		*19*	*19*	
CardCurrentUse		*19*	*19*	
sessionOpenTime		4	4	{00..00}
sessionOpenVehicle				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Control_Activity_Data		*46*	*46*	
CardControlActivityDataRecord		*46*	*46*	
controlType		1	1	{00}
controlTime		4	4	{00..00}
controlCardNumber				
cardType		1	1	{00}
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
controlVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
controlDownloadPeriodBegin		4	4	{00..00}
controlDownloadPeriodEnd		4	4	{00..00}

EF Specific_Conditions		*282*	*562*	
SpecificConditions		*282*	*562*	
conditionPointerNewestRecord		2	2	{00 00}
specificConditionRecords		*280*	*560*	
SpecificConditionRecord	n_9	*5*	*5*	
entryTime		4	4	{00..00}
specificConditionType		1	1	{00}
EF VehicleUnits_Used		*842*	*2002*	
CardVehicleUnitsUsed		*842*	*2002*	
vehicleUnitPointerNewestRecord		2	2	{00 00}
cardVehicleUnitRecords		*840*	*2000*	
CardVehicleUnitRecord	n_7	*10*	*10*	
timeStamp		4	4	{00..00}
manufacturerCode		1	1	{00}
deviceID		1	1	{00}
vuSoftwareVersion		4	4	{00..00}
EF GNSS_Places		*3782*	*5042*	
GNSSContinuousDriving		*3782*	*5042*	
gnssCDPointerNewestRecord		2	2	{00 00}
gnssContinuousDrivingRecords		3780	5040	{00}
GNSSContinuousDrivingRecord	n_8	*15*	*15*	
timeStamp		4	4	{00..00}
gnssPlaceRecord		11	11	
timeStamp		4	4	{00..00}
gnssAccuracy		1	1	{00}
geoCoordinates		6	6	{00..00}

TCS_155 Следните стойности, използвани за указване на размери в таблицата по-горе, определят минималния и максималния брой на записите, който трябва да се използва за приложение от поколение 2 в структурата на данните в картата на водача:

		Мин.	Макс.
n_1	NoOfEventsPerType	6	12
n_2	NoOfFaultsPerType	12	24
n_3	NoOfCardVehicleRecords	84	200
n_4	NoOfCardPlaceRecords	84	112
n_6	CardActivityLengthRange	5 544 байта (28 дни * 93 промени на дейността)	13 776 байта (28 дни * 240 промени на дейността)
n_7	NoOfCardVehicleUnitRecords	84	200
n_8	NoOfGNSSCDRecords	252	336
n_9	NoOfSpecificConditionRecords	56	112

4.3. Приложения за картата за монтаж и настройки

4.3.1 *Приложение от поколение 1 за картата за монтаж и настройки*

TCS_156 След персонализирането на приложението от поколение 1 за картата за монтаж и настройки то трябва да е със следната постоянна файлова структура и правила за достъп до файловете:

Файл	Идентификатор на файла	Правила за достъп		
		Четене	Селектиране	Актуализация
└DF Tachograph	‘0500h’		SC1	
├EF Application_Identification	‘0501h’	SC2	SC1	NEV
├EF Card_Certificate	‘C100h’	SC2	SC1	NEV
├EF CA_Certificate	‘C108h’	SC2	SC1	NEV
├EF Identification	‘0520h’	SC2	SC1	NEV
├EF Card_Download	‘0509h’	SC2	SC1	**SC1**
├EF Calibration	‘050Ah’	SC2	SC1	SC3
├EF Sensor_Installation_Data	‘050Bh’	**SC4**	SC1	NEV
├EF Events_Data	‘0502h’	SC2	SC1	SC3
├EF Faults_Data	‘0503h’	SC2	SC1	SC3
├EF Driver_Activity_Data	‘0504h’	SC2	SC1	SC3
├EF Vehicles_Used	‘0505h’	SC2	SC1	SC3
├EF Places	‘0506h’	SC2	SC1	SC3
├EF Current_Usage	‘0507h’	SC2	SC1	SC3
├EF Control_Activity_Data	‘0508h’	SC2	SC1	SC3
└EF Specific_Conditions	‘0522h’	SC2	SC1	SC3

В тази таблица се използват следните съкращения за условията за сигурност:

SC1 ALW ИЛИ SM-MAC-G2

SC2 ALW ИЛИ SM-MAC-G1 ИЛИ SM-MAC-G2

SC3 SM-MAC-G1 ИЛИ SM-MAC-G2

SC4 За командата READ BINARY с четен байт INS:

(PLAIN-C И SM-R-ENC-G1) ИЛИ (SM-C-MAC-G1 И SM-R-ENC-MAC-G1) ИЛИ

(SM-C-MAC-G2 И SM-R-ENC-MAC-G2)

За командата READ BINARY с нечетен байт INS (ако се поддържа): NEV

TCS_157 Структурите на всички EF трябва да бъдат прозрачни.

TCS_158 Приложението от поколение 1 за картата за монтаж и настройки трябва да е със следната структура на данните:

Файл / елемент на данни	Брой записи	Размер (байтове) Мин.	Макс.	Стойности по подразбиране
DF Tachograph		*11055*	*29028*	
EF Application_Identification		*11*	*11*	
WorkshopCardApplicationIdentification		*11*	*11*	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfEventsPerType		1	1	{00}
noOfFaultsPerType		1	1	{00}
activityStructureLength		2	2	{00 00}
noOfCardVehicleRecords		2	2	{00 00}
noOfCardPlaceRecords		1	1	{00}
noOfCalibrationRecords		1	1	{00}
EF Card_Certificate		*194*	*194*	
CardCertificate		194	194	{00..00}
EF CA_Certificate		*194*	*194*	
MemberStateCertificate		194	194	{00..00}
EF Identification		*211*	*211*	
CardIdentification		65	65	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{00, 20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
WorkshopCardHolderIdentification		*146*	*146*	
workshopName		36	36	{00, 20..20}
workshopAddress		36	36	{00, 20..20}
cardHolderName				
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00, 20..20}
cardHolderPreferredLanguage		2	2	{20 20}
EF Card_Download		*2*	*2*	
NoOfCalibrationsSinceDownload		2	2	{00 00}
EF Calibration		*9243*	*26778*	
WorkshopCardCalibrationData		*9243*	*26778*	
calibrationTotalNumber		2	2	{00 00}
calibrationPointerNewestRecord		1	1	{00}
calibrationRecords		*9240*	*26775*	
WorkshopCardCalibrationRecord	n_5	*105*	*105*	
calibrationPurpose		1	1	{00}
vehicleIdentificationNumber		17	17	{20..20}
vehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
wVehicleCharacteristicConstant		2	2	{00 00}
kConstantOfRecordingEquipment		2	2	{00 00}
lTyreCircumference		2	2	{00 00}
tyreSize		15	15	{20..20}
authorisedSpeed		1	1	{00}
oldOdometerValue		3	3	{00..00}
newOdometerValue		3	3	{00..00}
oldTimeValue		4	4	{00..00}
newTimeValue		4	4	{00..00}
nextCalibrationDate		4	4	{00..00}
vuPartNumber		16	16	{20..20}
vuSerialNumber		8	8	{00..00}
sensorSerialNumber		8	8	{00..00}

EF Sensor_Installation_Data		*16*	*16*	
└SensorInstallationSecData		16	16	{00..00}
EF Events_Data		*432*	*432*	
└CardEventData		*432*	*432*	
└cardEventRecords	6	*72*	*72*	
└CardEventRecord	n_1	*24*	*24*	
├eventType		1	1	{00}
├eventBeginTime		4	4	{00..00}
├eventEndTime		4	4	{00..00}
└eventVehicleRegistration				
├vehicleRegistrationNation		1	1	{00}
└vehicleRegistrationNumber		14	14	{00, 20..20}
EF Faults_Data		*288*	*288*	
└CardFaultData		*288*	*288*	
└cardFaultRecords	2	*144*	*144*	
└CardFaultRecord	n_2	*24*	*24*	
├faultType		1	1	{00}
├faultBeginTime		4	4	{00..00}
├faultEndTime		4	4	{00..00}
└faultVehicleRegistration				
├vehicleRegistrationNation		1	1	{00}
└vehicleRegistrationNumber		14	14	{00, 20..20}
EF Driver_Activity_Data		*202*	*496*	
└CardDriverActivity		*202*	*496*	
├activityPointerOldestDayRecord		2	2	{00 00}
├activityPointerNewestRecord		2	2	{00 00}
└activityDailyRecords	n_6	198	492	{00..00}
EF Vehicles_Used		*126*	*250*	
└CardVehiclesUsed		*126*	*250*	
├vehiclePointerNewestRecord		2	2	{00 00}
└cardVehicleRecords		*124*	*248*	
└CardVehicleRecord	n_3	*31*	*31*	
├vehicleOdometerBegin		3	3	{00..00}
├vehicleOdometerEnd		3	3	{00..00}
├vehicleFirstUse		4	4	{00..00}
├vehicleLastUse		4	4	{00..00}
├vehicleRegistration				
├vehicleRegistrationNation		1	1	{00}
└vehicleRegistrationNumber		14	14	{00, 20..20}
└vuDataBlockCounter		2	2	{00 00}
EF Places		*61*	*81*	
└CardPlaceDailyWorkPeriod		*61*	*81*	
├placePointerNewestRecord		1	1	{00}
└placeRecords		*60*	*80*	
└PlaceRecord	n_4	*10*	*10*	
├entryTime		4	4	{00..00}
├entryTypeDailyWorkPeriod		1	1	{00}
├dailyWorkPeriodCountry		1	1	{00}
├dailyWorkPeriodRegion		1	1	{00}
└vehicleOdometerValue		3	3	{00..00}
EF Current_Usage		*19*	*19*	
└CardCurrentUse		*19*	*19*	
├sessionOpenTime		4	4	{00..00}
└sessionOpenVehicle				
├vehicleRegistrationNation		1	1	{00}
└vehicleRegistrationNumber		14	14	{00, 20..20}

EF Control_Activity_Data		*46*	*46*	
CardControlActivityDataRecord		*46*	*46*	
controlType		1	1	{00}
controlTime		4	4	{00..00}
controlCardNumber				
cardType		1	1	{00}
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
controlVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
controlDownloadPeriodBegin		4	4	{00..00}
controlDownloadPeriodEnd		4	4	{00..00}
EF Specific_Conditions		*10*	*10*	
SpecificConditionRecord	2	*5*	*5*	
entryTime		4	4	{00..00}
SpecificConditionType		1	1	{00}

TCS_159 Следните стойности, използвани за указване на размери в таблицата по-горе, определят минималния и максималния брой на записите, който трябва да се използва за приложение от поколение 1 в структурата на данните в картата за монтаж и настройки:

		Мин.	**Макс.**
n_1	NoOfEventsPerType	3	3
n_2	NoOfFaultsPerType	6	6
n_3	NoOfCardVehicleRecords	4	8
n_4	NoOfCardPlaceRecords	6	8
n_5	NoOfCalibrationRecords	88	255
n_6	CardActivityLengthRange	198 байта (1 ден * 93 промени на дейността)	492 байта (1 ден * 240 промени на дейността)

4.3.2 *Приложение от поколение 2 за картата за монтаж и настройки*

TCS_160 След персонализирането на приложението от поколение 2 за картата за монтаж и настройки то трябва да е със следната постоянна файлова структура и правила за достъп до файловете:

Забележка: краткият идентификатор на EF (SFID) се дава като десетично число — например стойността 30 съответства на 11110 в двоичната бройна система.

			Правила за достъп		
Файл	**Идентификатор на файла**	**SFID**	**Четене**	**Селектиране**	**Актуализация**
└─DF Tachograph_G2			SC1	SC1	
├─EF Application_Identification	‘0501h’	1	SC1	SC1	NEV
├─EF CardMA_Certificate	‘C100h’	2	SC1	SC1	NEV
├─EF CardSignCertificate	‘C101h’	3	SC1	SC1	NEV
├─EF CA_Certificate	‘C108h’	4	SC1	SC1	NEV
├─EF Link_Certificate	‘C109h’	5	SC1	SC1	NEV
├─EF Identification	‘0520h’	6	SC1	SC1	NEV
├─EF Card_Download	‘0509h’	7	SC1	SC1	SC1
├─EF Calibration	‘050Ah’	10	SC1	SC1	SM-MAC-G2
├─EF Sensor_Installation_Data	‘050Bh’	11	**SC5**	SM-MAC-G2	NEV
├─EF Events_Data	‘0502h’	12	SC1	SC1	SM-MAC-G2
├─EF Faults_Data	‘0503h’	13	SC1	SC1	SM-MAC-G2
├─EF Driver_Activity_Data	‘0504h’	14	SC1	SC1	SM-MAC-G2
├─EF Vehicles_Used	‘0505h’	15	SC1	SC1	SM-MAC-G2
├─EF Places	‘0506h’	16	SC1	SC1	SM-MAC-G2
├─EF Current_Usage	‘0507h’	17	SC1	SC1	SM-MAC-G2
├─EF Control_Activity_Data	‘0508h’	18	SC1	SC1	SM-MAC-G2
├─EF Specific_Conditions	‘0522h’	19	SC1	SC1	SM-MAC-G2
├─EF VehicleUnits_Used	‘0523h’	20	SC1	SC1	SM-MAC-G2
└─EF GNSS_Places	‘0524h’	21	SC1	SC1	SM-MAC-G2

В тази таблица се използват следните съкращения за условията за сигурност:

SC1 ALW ИЛИ SM-MAC-G2

SC 5 За командата Read Binary с четен байт INS: SM-C-MAC-G2 И SM-R-ENC-MAC-G2

За командата Read Binary с нечетен байт INS (ако се поддържа): NEV

TCS_161 Структурите на всички EF трябва да бъдат прозрачни.

TCS_162 Приложението от поколение 2 за картата за монтаж и настройки трябва да е със следната структура на данните:

Файл / елемент на данни	Брой записи	Размер (байтове) Мин.	Макс.	Стойности по подразбиране
DF Tachograph_G2		*17837*	*47163*	
EF Application_Identification		*17*	*17*	
WorkshopCardApplicationIdentification		*17*	*17*	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfEventsPerType		1	1	{00}
noOfFaultsPerType		1	1	{00}
activityStructureLength		2	2	{00 00}
noOfCardVehicleRecords		2	2	{00 00}
noOfCardPlaceRecords		2	2	{00}
noOfCalibrationRecords		2	2	{00}
noOfGNSSCDRecords		2	2	{00..00}
noOfSpecificConditionRecords		2	2	{00..00}
EF CardMA_Certificate		*204*	*341*	
CardMACertificate		204	341	{00..00}
EF CardSignCertificate		*204*	*341*	
CardSignCertificate		204	341	{00..00}
EF CA_Certificate		*204*	*341*	
MemberStateCertificate		204	341	{00..00}
EF Link_Certificate		*204*	*341*	
LinkCertificate		204	341	{00..00}
EF Identification		*211*	*211*	
CardIdentification		*65*	*65*	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{00, 20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
WorkshopCardHolderIdentification		*146*	*146*	
workshopName		36	36	{00, 20..20}
workshopAddress		36	36	{00, 20..20}
cardHolderName				
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00, 20..20}
cardHolderPreferredLanguage		2	2	{20 20}
EF Card_Download		*2*	*2*	
NoOfCalibrationsSinceDownload		2	2	{00 00}
EF Calibration		*14788*	*42844*	
WorkshopCardCalibrationData		*14788*	*42844*	
calibrationTotalNumber		2	2	{00 00}
calibrationPointerNewestRecord		2	2	{00}
calibrationRecords		*14784*	*42840*	
WorkshopCardCalibrationRecord	n_5	*168*	*168*	
calibrationPurpose		1	1	{00}
vehicleIdentificationNumber		17	17	{20..20}
vehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
wVehicleCharacteristicConstant		2	2	{00 00}
kConstantOfRecordingEquipment		2	2	{00 00}
lTyreCircumference		2	2	{00 00}
tyreSize		15	15	{20..20}
authorisedSpeed		1	1	{00}
oldOdometerValue		3	3	{00..00}
newOdometerValue		3	3	{00..00}

├─oldTimeValue		4	4	{00..00}
├─newTimeValue		4	4	{00..00}
├─nextCalibrationDate		4	4	{00..00}
├─vuPartNumber		16	16	{20..20}
├─vuSerialNumber		8	8	{00..00}
├─sensorSerialNumber		8	8	{00..00}
├─sensorGNSSSerialNumber		8	8	{00..00}
├─rcmSerialNumber		8	8	{00..00}
├─vuAbility		1	1	{00}
└─sealDataCard		46	46	
├─noOfSealRecords		1	1	{00}
└─SealRecords		45	45	
└─SealRecord	5	9	9	
├─equipmentType		1	1	{00}
└─extendedSealIdentifier		8	8	{00..00}
EF Sensor_Installation_Data		*18*	*102*	
└─SensorInstallationSecData		18	102	{00..00}
EF Events_Data		*792*	*792*	
└─CardEventData		*792*	*792*	
└─cardEventRecords	11	*72*	*72*	
└─CardEventRecord	n_1	*24*	*24*	
├─eventType		1	1	{00}
├─eventBeginTime		4	4	{00..00}
├─eventEndTime		4	4	{00..00}
└─eventVehicleRegistration				
├─vehicleRegistrationNation		1	1	{00}
└─vehicleRegistrationNumber		14	14	{00, 20..20}
EF Faults_Data		*288*	*288*	
└─CardFaultData		*288*	*288*	
└─cardFaultRecords	2	*144*	*144*	
└─CardFaultRecord	n_2	*24*	*24*	
├─faultType		1	1	{00}
├─faultBeginTime		4	4	{00..00}
├─faultEndTime		4	4	{00..00}
└─faultVehicleRegistration				
├─vehicleRegistrationNation		1	1	{00}
└─vehicleRegistrationNumber		14	14	{00, 20..20}
EF Driver_Activity_Data		*202*	*496*	
└─CardDriverActivity		*202*	*496*	
├─activityPointerOldestDayRecord		2	2	{00 00}
├─activityPointerNewestRecord		2	2	{00 00}
└─activityDailyRecords	n_6	198	492	{00..00}
EF Vehicles_Used		*194*	*386*	
└─CardVehiclesUsed		*194*	*386*	
├─vehiclePointerNewestRecord		2	2	{00 00}
└─cardVehicleRecords		*192*	*384*	
└─CardVehicleRecord	n_3	*48*	*48*	
├─vehicleOdometerBegin		3	3	{00..00}
├─vehicleOdometerEnd		3	3	{00..00}
├─vehicleFirstUse		4	4	{00..00}
├─vehicleLastUse		4	4	{00..00}
├─vehicleRegistration				
├─vehicleRegistrationNation		1	1	{00}
└─vehicleRegistrationNumber		14	14	{00, 20..20}
├─vuDataBlockCounter		2	2	{00 00}
└─vehicleIdentificationNumber		*17*	17	{20..20}
EF Places		*128*	*170*	

└CardPlaceDailyWorkPeriod		*128*	*170*	
├placePointerNewestRecord		2	2	{00 00}
└placeRecords		*126*	*168*	
└PlaceRecord	n_4	*21*	*21*	
├entryTime		4	4	{00..00}
├entryTypeDailyWorkPeriod		1	1	{00}
├dailyWorkPeriodCountry		1	1	{00}
├dailyWorkPeriodRegion		1	1	{00}
├vehicleOdometerValue		3	3	{00..00}
└entryGNSSPlaceRecord		11	11	{00..00}
├timeStamp		4	4	{00..00}
├gnssAccuracy		1	1	{00}
└geoCoordinates		6	6	{00..00}
EF Current_Usage		*19*	*19*	
└CardCurrentUse		*19*	*19*	
├sessionOpenTime		4	4	{00..00}
└sessionOpenVehicle				
├vehicleRegistrationNation		1	1	{00}
└vehicleRegistrationNumber		14	14	{00, 20..20}
EF Control_Activity_Data		*46*	*46*	
└CardControlActivityDataRecord		*46*	*46*	
├controlType		1	1	{00}
├controlTime		4	4	{00..00}
├controlCardNumber				
├cardType		1	1	{00}
├cardIssuingMemberState		1	1	{00}
└cardNumber		16	16	{20..20}
├controlVehicleRegistration				
├vehicleRegistrationNation		1	1	{00}
└vehicleRegistrationNumber		14	14	{00, 20..20}
├controlDownloadPeriodBegin		4	4	{00..00}
└controlDownloadPeriodEnd		4	4	{00..00}
EF VehicleUnits_Used		*42*	*42*	
└CardVehicleUnitsUsed		*42*	*82*	
├vehicleUnitPointerNewestRecord		2	2	{00 00}
└cardVehicleUnitRecords		*40*	*80*	
└CardVehicleUnitRecord	n_7	*10*	*10*	
├timeStamp		4	4	{00..00}
├manufacturerCode		1	1	{00..00}
├deviceID		1	1	{00..00}
└vuSoftwareVersion		4	4	{00..00}
EF GNSS_Places		*262*	*362*	
└GNSSContinuousDriving		*262*	*362*	
├gnssCDPointerNewestRecord		2	2	{00 00}
└gnssContinuousDrivingRecords		*260*	*360*	
└GNSSContinuousDrivingRecord	n_8	*15*	*15*	
├timeStamp		4	4	{00..00}
└gnssPlaceRecord		11	11	
├timeStamp		4	4	{00..00}
├gnssAccuracy		1	1	{00}
└geoCoordinates		6	6	{00..00}
EF Specific_Conditions		*12*	*22*	
└SpecificConditions		*12*	*22*	
├conditionPointerNewestRecord		2	2	{00 00}
└specificConditionRecords		10	20	
└SpecificConditionRecord	n_9	*5*	*5*	
├entryTime		4	4	{00..00}
└specificConditionType		1	1	{00}

TCS_163 Следните стойности, използвани за указване на размери в таблицата по-горе, определят минималния и максималния брой на записите, който трябва да се използва за приложение от поколение 2 в структурата на данните в картата за монтаж и настройки:

		Мин.	Макс.
n_1	NoOfEventsPerType	3	3
n_2	NoOfFaultsPerType	6	6
n_3	NoOfCardVehicleRecords	4	8
n_4	NoOfCardPlaceRecords	6	8
n_5	NoOfCalibrationRecords	88	255
n_6	CardActivityLengthRange	198 байта (1 ден * 93 промени на дейността)	492 байта (1 ден * 240 промени на дейността)
n_7	NoOfCardVehicleUnitRecords	4	8
n_8	NoOfGNSSCDRecords	18	24
n_9	NoOfSpecificConditionRecords	2	4

4.4. Приложения за контролната карта

4.4.1 *Приложение от поколение 1 за контролната карта*

TCS_164 След персонализирането на приложението от поколение 1 за контролната карта то трябва да е със следната постоянна файлова структура и правила за достъп до файловете:

		Правила за достъп		
Файл	**Идентификатор на файла**	**Четене**	**Селектиране**	**Актуализация**
└─DF Tachograph	'0500h'			
├─EF Application_Identification	'0501h'	SC2	SC1	NEV
├─EF Card_Certificate	'C100h'	SC2	SC1	NEV
├─EF CA_Certificate	'C108h'	SC2	SC1	NEV
├─EF Identification	'0520h'	**SC6**	SC1	NEV
└─EF Controller_Activity_Data	'050Ch'	SC2	SC1	SC3

В тази таблица се използват следните съкращения за условията за сигурност:

SC1 ALW ИЛИ SM-MAC-G2

SC2 ALW ИЛИ SM-MAC-G1 ИЛИ SM-MAC-G2

SC3 SM-MAC-G1 ИЛИ SM-MAC-G2

SC6 EXT-AUT-G1 ИЛИ SM-MAC-G1 ИЛИ SM-MAC-G2

TCS_165 Структурите на всички EF трябва да бъдат прозрачни.

TCS_166 Приложението от поколение 1 за контролната карта трябва да е със следната структура на данните:

Файл / елемент на данни	Брой записи	Размер (байтове) Мин.	Макс.	
DF Tachograph		*11186*	*24526*	
EF Application_Identification		*5*	*5*	
ControlCardApplicationIdentification		*5*	*5*	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfControlActivityRecords		2	2	{00 00}
EF Card_Certificate		*194*	*194*	
CardCertificate		194	194	{00..00}
EF CA_Certificate		*194*	*194*	
MemberStateCertificate		194	194	{00..00}
EF Identification		*211*	*211*	
CardIdentification		*65*	*65*	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{00, 20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
ControlCardHolderIdentification		*146*	*146*	
controlBodyName		36	36	{00, 20..20}
controlBodyAddress		36	36	{00, 20..20}
cardHolderName				
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00, 20..20}
cardHolderPreferredLanguage		2	2	{20 20}
EF Controller_Activity_Data		*10582*	*23922*	
ControlCardControlActivityData		*10582*	*23922*	
controlPointerNewestRecord		2	2	{00 00}
controlActivityRecords		*10580*	*23920*	
controlActivityRecord	n_7	*46*	*46*	
controlType		1	1	{00}
controlTime		4	4	{00..00}
controlledCardNumber				
cardType		1	1	{00}
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
controlledVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
controlDownloadPeriodBegin		4	4	{00..00}
controlDownloadPeriodEnd		4	4	{00..00}

TCS_167 Следните стойности, използвани за указване на размери в таблицата по-горе, определят минималния и максималния брой на записите, който трябва да се използва за приложение от поколение 1 в структурата на данните в контролната карта:

		Мин.	Макс.
n_7	NoOfControlActivityRecords	230	520

4.4.2 *Приложение от поколение 2 за контролната карта*

TCS_168 След персонализирането на приложението от поколение 2 за контролната карта то трябва да е със следната постоянна файлова структура и правила за достъп до файловете:

Забележка: краткият идентификатор на EF (SFID) се дава като десетично число — например стойността 30 съответства на 11110 в двоичната бройна система.

Файл	Идентификатор на файла	SFID	Правила за достъп	
			Четене / Селектиране	Актуализация
└─DF Tachograph_G2			SC1	
├─EF Application_Identification	‘0501h’	1	SC1	NEV
├─EF CardMA_Certificate	‘C100h’	2	SC1	NEV
├─EF CA_Certificate	‘C108h’	4	SC1	NEV
├─EF Link_Certificate	‘C109h’	5	SC1	NEV
├─EF Identification	‘0520h’	6	SC1	NEV
└─EF Controller_Activity_Data	‘050Ch’	14	SC1	SM-MAC-G2

В тази таблица се използва следното съкращение за условието за сигурност:

SC1 ALW ИЛИ SM-MAC-G2

TCS_169 Структурите на всички EF трябва да бъдат прозрачни.

TCS_170 Приложението от поколение 2 за контролната карта трябва да е със следната структура на данните:

Файл / елемент на данни	Брой записи	Размер (байтове) Мин.	Макс.	
DF Tachograph_G2		*11410*	*25161*	
EF Application_Identification		*5*	*5*	
ControlCardApplicationIdentification		*5*	*5*	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfControlActivityRecords		2	2	{00 00}
EF CardMA_Certificate		*204*	*341*	
CardMACertificate		204	341	{00..00}
EF CA_Certificate		*204*	*341*	
MemberStateCertificate		204	341	{00..00}
EF Link_Certificate		*204*	*341*	
LinkCertificate		204	341	{00..00}
EF Identification		*211*	*211*	
CardIdentification		*65*	*65*	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{00, 20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
ControlCardHolderIdentification		*146*	*146*	
controlBodyName		36	36	{00, 20..20}
controlBodyAddress		36	36	{00, 20..20}
cardHolderName				
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00, 20..20}
cardHolderPreferredLanguage		2	2	{20 20}
EF Controller_Activity_Data		*10582*	*23922*	
ControlCardControlActivityData		*10582*	*23922*	
controlPointerNewestRecord		2	2	{00 00}
controlActivityRecords		*10580*	*23920*	
controlActivityRecord	n_7	*46*	*46*	
controlType		1	1	{00}
controlTime		4	4	{00..00}
controlledCardNumber				
cardType		1	1	{00}
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
controlledVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
controlDownloadPeriodBegin		4	4	{00..00}
controlDownloadPeriodEnd		4	4	{00..00}

TCS_171 Следните стойности, използвани за указване на размери в таблицата по-горе, определят минималния и максималния брой на записите, който трябва да се използва за приложение от поколение 2 в структурата на данните в контролната карта:

		Мин.	Макс.
n_7	NoOfControlActivityRecords	230	520

4.5. Приложения за картата на превозвач

4.5.1 *Приложение от поколение 1 за картата на превозвач*

TCS_172 След персонализирането на приложението от поколение 1 за картата на превозвач то трябва да е със следната постоянна файлова структура и правила за достъп до файловете:

Файл	Идентификатор на файла	Правила за достъп: Четене	Селектиране	Актуализация
└DF Tachograph	'0500h'		SC1	
├EF Application_Identification	'0501h'	SC2	SC1	NEV
├EF Card_Certificate	'C100h'	SC2	SC1	NEV
├EF CA_Certificate	'C108h'	SC2	SC1	NEV
├EF Identification	'0520h'	**SC6**	SC1	NEV
└EF Company_Activity_Data	'050Dh'	SC2	SC1	SC3

В тази таблица се използват следните съкращения за условията за сигурност:

SC1 ALW ИЛИ SM-MAC-G2

SC2 ALW ИЛИ SM-MAC-G1 ИЛИ SM-MAC-G2

SC3 SM-MAC-G1 ИЛИ SM-MAC-G2

SC6 EXT-AUT-G1 ИЛИ SM-MAC-G1 ИЛИ SM-MAC-G2

TCS_173 Структурите на всички EF трябва да бъдат прозрачни.

TCS_174 Приложението от поколение 1 за картата на превозвач трябва да е със следната структура на данните:

Файл / елемент на данни	Брой записи	Размер (байтове) Мин.	Макс.	Стойности по подразбиране
└DF Tachograph		*11114*	*24454*	
├EF Application_Identification		*5*	*5*	
│└CompanyCardApplicationIdentification		*5*	*5*	
│├typeOfTachographCardId		1	1	{00}
│├cardStructureVersion		2	2	{00 00}
│└noOfCompanyActivityRecords		2	2	{00 00}
├EF Card_Certificate		*194*	*194*	
│└CardCertificate		194	194	{00..00}
├EF CA_Certificate		*194*	*194*	
│└MemberStateCertificate		194	194	{00..00}
├EF Identification		*139*	*139*	
│├CardIdentification		*65*	*65*	
││├cardIssuingMemberState		1	1	{00}
││├cardNumber		16	16	{20..20}
││├cardIssuingAuthorityName		36	36	{00, 20..20}
││├cardIssueDate		4	4	{00..00}
││├cardValidityBegin		4	4	{00..00}
││└cardExpiryDate		4	4	{00..00}
│└CompanyCardHolderIdentification		*74*	*74*	
│├companyName		36	36	{00, 20..20}
│├companyAddress		36	36	{00, 20..20}
│└cardHolderPreferredLanguage		2	2	{20 20}
├EF Company_Activity_Data		*10582*	*23922*	
│└CompanyActivityData		*10582*	*23922*	
│├companyPointerNewestRecord		2	2	{00 00}
│└companyActivityRecords		*10580*	*23920*	
│└companyActivityRecord	n_8	*46*	*46*	
│├companyActivityType		1	1	{00}
│├companyActivityTime		4	4	{00..00}
│├cardNumberInformation				
││├cardType		1	1	{00}
││├cardIssuingMemberState		1	1	{00}
││└cardNumber		16	16	{20..20}
│├vehicleRegistrationInformation				
││├vehicleRegistrationNation		1	1	{00}
││└vehicleRegistrationNumber		14	14	{00, 20..20}
│├downloadPeriodBegin		4	4	{00..00}
│└downloadPeriodEnd		4	4	{00..00}

TCS_175 Следните стойности, използвани за указване на размери в таблицата по-горе, определят минималния и максималния брой на записите, който трябва да се използва за приложение от поколение 1 в структурата на данните в картата на превозвач:

		Мин.	Макс.
n_8	NoOfCompanyActivityRecords	230	520

4.5.2 *Приложение от поколение 2 за картата на превозвач*

TCS_176 След персонализирането на приложението от поколение 2 за картата на превозвач то трябва да е със следната постоянна файлова структура и правила за достъп до файловете:

Забележка: краткият идентификатор на EF (SFID) се дава като десетично число — например стойността 30 съответства на 11110 в двоичната бройна система.

			Правила за достъп	
Файл	**Идентификатор на файла**	**SFID**	**Четене / Селектиране**	**Актуализация**
└─DF Tachograph_G2			SC1	
├─EF Application_Identification	'0501h'	1	SC1	NEV
├─EF CardMA_Certificate	'C100h'	2	SC1	NEV
├─EF CA_Certificate	'C108h'	4	SC1	NEV
├─EF Link_Certificate	'C109h'	5	SC1	NEV
├─EF Identification	'0520h'	6	SC1	NEV
└─EF Company_Activity_Data	'050Dh'	14	SC1	SM-MAC-G2

В тази таблица се използва следното съкращение за условието за сигурност:

SC1 ALW ИЛИ SM-MAC-G2

TCS_177 Структурите на всички EF трябва да бъдат прозрачни.

TCS_178 Приложението от поколение 2 за картата на превозвач трябва да е със следната структура на данните:

Файл / елемент на данни	Брой записи	Размер (байтове) Мин.	Макс.	Стойности по подразбиране
DF Tachograph_G2		*11338*	*25089*	
EF Application_Identification		*5*	*5*	
CompanyCardApplicationIdentification		*5*	*5*	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfCompanyActivityRecords		2	2	{00 00}
EF CardMA_Certificate		*204*	*341*	
CardMACertificate		204	341	{00..00}
EF CA_Certificate		*204*	*341*	
MemberStateCertificate		204	341	{00..00}
EF Link_Certificate		*204*	*341*	
LinkCertificate		204	341	{00..00}
EF Identification		*139*	*139*	
CardIdentification		*65*	*65*	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{00, 20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
CompanyCardHolderIdentification		*74*	*74*	
companyName		36	36	{00, 20..20}
companyAddress		36	36	{00, 20..20}
cardHolderPreferredLanguage		2	2	{20 20}
EF Company_Activity_Data		*10582*	*23922*	
CompanyActivityData		*10582*	*23922*	
companyPointerNewestRecord		2	2	{00 00}
companyActivityRecords		*10580*	*23920*	
companyActivityRecord	n_8	*46*	*46*	
companyActivityType		1	1	{00}
companyActivityTime		4	4	{00..00}
cardNumberInformation				
cardType		1	1	{00}
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
vehicleRegistrationInformation				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
downloadPeriodBegin		4	4	{00..00}
downloadPeriodEnd		4	4	{00..00}

TCS_179 Следните стойности, използвани за указване на размери в таблицата по-горе, определят минималния и максималния брой на записите, който трябва да се използва за приложение от поколение 2 в структурата на данните в картата на превозвач:

		Мин.	Макс.
n_8	NoOfCompanyActivityRecords	230	520

Допълнение 3

ПИКТОГРАМИ

PIC_001 При тахографите може по избор да се използват следните пиктограми и комбинации от пиктограми (или пиктограми и комбинации, които да са достатъчно сходни на тях, така че еднозначно да бъдат отъждествими с тях):

1. ОСНОВНИ ПИКТОГРАМИ

	Хора	**Действия**	**Режими на работа**
	Предприятие		Режим на предприятие
	Контрольор	Контрол	Контролен режим
	Водач	Управление на МПС	Работен режим
	Сервиз/изпитателен пункт	Техн. преглед/калибриране	Режим на калибриране
	Производител		
	Дейности	**Времетраене**	
	На разположение	Текущ период на разположение	
	Управление на МПС	Време на непрекъснато управление на МПС	
	Почивка	Текущ период на почивка	
	Друга работа	Текущ период на работа	
	Прекъсване	Общо време на прекъсване	
	Неизвестна дейност		
	Оборудване	**Функции**	
	Четящо устройство с процеп за картата на водача		
	Четящо устройство с процеп за картата на втория водач		
	Карта		
	Часовник		
	Дисплей	Показване върху дисплея	
	Външна памет	Изтегляне на данни	
	Електрическо захранване		
	Принтер / разпечатка	Разпечатване	
	Датчик		
	Размер на гумите		
	Превозно средство / бордово устройство		
	Устройство за GNSS		
	Устройство за откриване от разстояние		
	Интерфейс с ITS		
	Особени условия		
	Извън обсег		
	Преминаване с ферибот/влак		

Други

!	Събития	⤫	Неизправности
⏵	Начало на дневен период на работа	⏴	Край на дневен период на работа
●	Местоположение		
M	Ръчно въвеждане на дейностите, извършвани от водача		
🔒	Сигурност		
›	Скорост		
◷	Час		
Σ	Общо/обобщение (справка)		

Определения

24h	За деня
I	За седмица
II	За две седмици
+	От или към

2. КОМБИНАЦИИ ОТ ПИКТОГРАМИ

Други

⊓●	Контролен пункт		
●⏵	Местоположение в началото на дневния период на работа	⏴●	Местоположение в края на дневния период на работа
◷+	От … часа	+◷	До … часа
🚚+	От превозното средство		
OUT+	Начало на излизането извън обсег	+OUT	Край на излизането извън обсег

Карти

⊙▮	Карта на водач
⌂▮	Карта на превозвач
⊓▮	Контролна карта
T▮	Карта за монтаж и настройки
▮– – –	Без карта

Управление на МПС

⊙⊙	Управление на МПС в екип
⊙ I	Време на управление на МПС за една седмица
⊙ II	Време на управление на МПС за две седмици

Разпечатки

24h ▮▼	Ежедневна разпечатка на дейностите, извършвани от водача, извлечени от картата
24h 🚚▼	Ежедневна разпечатка на дейностите, извършвани от водача, извлечени от VU (бордовото устройство)
!⤫▮▼	Разпечатка на събитията и неизправностите, извлечени от картата
!⤫🚚▼	Разпечатка на събитията и неизправностите, извлечени от VU
T◷▼	Разпечатка на техническите данни
››▼	Разпечатка за превишаването на допустимата скорост

Събития

	Вкарване на невалидна карта
	Конфликт, предизвикан от картата
	Припокриване във времето
	Управление на МПС без съответната карта
	Вкарване на карта по време на управление на МПС
	Неправилно приключване на последната картова сесия
	Превишаване на допустимата скорост
	Прекъсване на електрическото захранване
	Грешка в данните за движението
	Противоречие в данните относно движението на превозното средство
	Нарушаване на сигурността
	Сверяване на часовника (в сервиз)
	Контрол на превишаването на допустимата скорост

Неизправности

	Дефектна карта (в процепа на четящото устройство за картата на водача)
	Дефектна карта (в процепа на четящото устройство за картата на втория водач)
	Неизправност в дисплея
	Грешка при изтеглянето на данни
	Неизправност в принтера (печатащото устройство)
	Неизправност на датчика
	Неизправност вътре във VU
	Неизправност във връзка с GNSS
	Неизправност във връзка с откриването от разстояние

Процедура по ръчно въвеждане

	За същия дневен период на работа?
	Край на предишен период на работа?
	Потвърждение или въвеждане на местоположението в края на дневния период на работа
	Въвеждане на часа на тръгване
	Въвеждане на местоположението в началото на периода на работа.

Забележка: в допълнение 4 са определени допълнителни комбинации от пиктограми с оглед да се получат блокове за разпечатване или идентификатори на записи.

Допълнение 4

РАЗПЕЧАТКИ

СЪДЪРЖАНИЕ

1. ОБЩИ ПОЛОЖЕНИЯ

Всяка разпечатка се състои от поредица последователни блокове от данни, които могат да бъдат определени от идентификатор на блока.

Един блок данни съдържа един или няколко записа, които при необходимост могат да бъдат определени от идентификатор на записа.

PRT_001 Ако идентификатор на блок предхожда непосредствено идентификатор на запис, идентификаторът на запис не се отпечатва.

PRT_002 Ако някакъв елемент от данните е неизвестен или не трябва да се отпечатва поради права за достъп до данните, на мястото на този елемент остава празно пространство при разпечатването.

PRT_003 Ако съдържанието на цял ред е неизвестно или не се налага да бъде отпечатано, целият този ред се пропуска.

PRT_004 Полетата с цифрови данни се отпечатват с подравняване отдясно и без нули в началото на числата, като групите от цифри за хилядите и за милионите се разделят с празен интервал.

PRT_005 Полетата за данни, състоящи се от символни низове, се отпечатват с подравняване отляво и при необходимост се допълват с празни интервали или се отрязват съобразно дължината на елемента от данните (имена и адреси).

PRT_006 Ако се налага пренос на нов ред поради дълъг текст, като първи символ на новия ред следва да се отпечата специален знак (точка на половината височина на реда „•“).

2. СПЕЦИФИКАЦИЯ ЗА БЛОКОВЕТЕ ДАННИ

В настоящата глава се прилагат следните условни обозначения за формата:

— символите, които са изписани с **удебелен** шрифт, обозначават обикновен текст (отпечатват се същите символи, но с нормален шрифт);

— символите с нормален шрифт обозначават променливи (пиктограми или данни), които се заместват при отпечатването с техните съответни стойности;

— имената на променливите се допълват от знаци за подчертаване, за да се посочи допустимата дължина на елемента от данни за съответната променлива;

— датите се указват във формата „дд/мм/гггг“ (ден/месец/година). Може да се използва и формат „дд.мм.гггг“.

— Терминът „Идентификация на картата“ обхваща съвкупността от: типа на картата, обозначен чрез комбинация от пиктограми, кода на държавата членка, която е издала картата, наклонена надясно черта и номер на картата с индекс за замяна и индекс за подновяване, разделени от един празен интервал:

P	■	x	x	x	/	x	x	x	x	x	x	x	x	x	x	x	x	x		x		x
Комбинация от пиктограми за картата		Код на издаващата държава членка				Първите 14 символа от номера на картата (евентуално включително индекс за последователност)														Индекс за подмяна		Индекс за подновяване

PRT_007 Разпечатките се състоят от следните блокове и/или записи от данни със следните значения и формати:

Номер на блока или записа Значение	Формат на данните
1 ***Дата и час:минути (hh:mm) на отпечатване на документа.***	▼ дд/мм/гггг hh:mm **(UTC)**
2 ***Тип на разпечатката.*** Идентификатор на блока Комбинация от пиктограми за разпечатката (виж допълнение 3), настройка на ограничителя за скоростта (разпечатка само при превишаване на допустимата скорост)	----------▼---------- Пиктограма xxx **km/h**
3 ***Идентификация на титуляря на картата.*** Идентификатор на блока. P = пиктограма за хора Фамилно име на титуляря на картата Собствено име и презиме (ако има такова) на титуляря на картата Идентификация на картата Краен срок на валидност на картата (ако има такъв) и номер на поколението на картата (GEN 1 или GEN 2) (*)	----------P---------- P Фамилно_име_____ Собствено_име_____ Идентификация_на_картата_____ дд/мм/гггг - GEN 2

Когато картата не е на определено лице и не съдържа фамилно име на титуляр на картата, вместо него се отпечатва наименованието на превозвача, сервиза или контролния орган.

(*) Номерът на поколението на картата може да бъде отпечатан само от интелигентен тахограф.

4 ***Идентификация на превозното средство*** Идентификатор на блока Идентификационен номер на превозното средство (VIN) Държава членка, в която е регистрирано превозното средство, и регистрационен номер на превозното средство (VRN)	----------🚚---------- 🚚 VIN_____ Нац./VRN_____
5 ***Идентификация на бордовото устройство (VU)*** Идентификатор на блока Име на производителя на VU Идентификационен номер на VU Номер на поколението на VU (*)	----------⊟---------- ⊟ Производител_на_VU_____ Номер_на_VU__ GEN 2

(*) Номерът на поколението на картата може да бъде отпечатан само от интелигентен тахограф.

6 ***Последно калибриране на тахографа*** Идентификатор на блока Наименование на сервиза Идентификация на картата за монтаж и настройки Дата на калибрирането	----------🔧---------- 🔧 Наименование_____ Идентификация_на_картата_____ 🔧 дд/мм/гггг

7 ***Последна проверка (от контролен орган)***

Идентификатор на блока
Идентификация на контролната карта
Дата, време и вид на проверката

```
----------▫----------
Идентификация_на_картата_____
▫ дд/мм/гггг hh:mm ppppp
```

Вид на проверката: до пет пиктограми (p). Видът на проверката може да бъде представен чрез (комбинация от):

▪: изтегляне на данни от картата, ↓: изтегляне на данни от VU, ↓: разпечатване, ▫: показване върху дисплея, ↑: крайпътна проверка на калибрирането

8 ***Дейности на водача, записани в хронологична последователност върху картата***

Идентификатор на блока
Дата на събиране на данните (календарен ден, за който се отнася разпечатката) + картов брояч за ежедневно присъствие

```
----------⊙----------
    дд/мм/гггг  xxx
```

8a *Условие „Извън обсег“ (OUT) в началото на този ден* (да се остави празно, ако не е зададено условие „Извън обсег“)

```
----------OUT----------
```

8.1 *Период, през който картата не е била вкарана*

8.1a Идентификатор на записа (начало на периода)
8.1б *Период на неизвестна дейност*. Час на започване, времетраене
8.1в *Ръчно въведена дейност*.
Пиктограма за дейност (A), час на започване, времетраене

```
  --------------------
?       hh:mm hhhmm
A       hh:mm hhhmm
```

8.2 *Вкарване на картата в процепа S на четящото устройство*

Идентификатор на записа; S = пиктограма за процеп на четящо устройство
Държава членка, в която е регистрирано превозното средство, и регистрационен номер на превозното средство (VRN)
Показание на сумиращия, т.е. километражния брояч на превозното средство при вкарването на картата

```
  ---------S---------
▪ Нац./VRN___________
  x xxx xxx km
```

8.3 *Дейност (докато е била вкарана картата)*

Пиктограма за дейност (A), час на започване, времетраене, статус на екипа водачи (пиктограма за екип, ако той се състои от няколко водача (CREW), и празни интервали, ако има само един водач (SINGLE))

```
A       hh:mm hhhmm ⊙⊙
```

8.3a *Особено условие*. Час на въвеждането, пиктограма (или комбинация от пиктограми — „pppp“) за особеното условие.

```
        hh:mm ---pppp---
```

8.4 *Изваждане на картата*

Показание на километражния брояч на превозното средство и изминато разстояние от последното вкарване на картата, за което е известно показанието на километражния брояч.

```
  x xxx xxx km; x xxx km
```

9 ***Дейности на водача, записани във VU в хронологична последователност по четящи устройства***

Идентификатор на блока
Дата на събиране на данните (календарен ден, за който се отнася разпечатката)
Показание на километражния брояч на превозното средство в 00:00 часа и в 24:00 часа

```
----------⊙----------
       дд/мм/гггг

x xxx xxx - x xxx xxx km
```

10 ***Дейности, извършени според четящото устройство S***

Идентификатор на блока

```
----------S----------
```

10a *Условие „Извън обсег“ (OUT) в началото на този ден* (да се остави празно, ако не е зададено условие „Извън обсег“)

```
----------OUT----------
```

10.1 *Период, през който в процепа S на четящото устройство не е била вкарана карта*

Идентификатор на записа
Не е вкарана карта
Показание на километражния брояч на превозното средство в началото на периода

```
  --------------------
⊙▪---
  x xxx xxx km
```

10.2 *Вкарване на карта*

Идентификатор на записа за вкарването на карта
Фамилно име на водача

```
  --------------------
⊙ Фамилно_име_____________
```

	Собствено име на водача Идентификация на картата на водача Краен срок на валидност на картата (ако има такъв) и номер на поколението на картата (GEN 1 или GEN 2) (*) Държава-членка, в която е регистрирано предишното използвано превозно средство, и регистрационен номер на това превозно средство (VRN) Дата и час на изваждане на картата от предишното превозно средство Празен ред Показание на километражния брояч при вкарването на картата, ръчно въвеждане на флага за дейност на водача (M при положителен отговор, празен интервал при отрицателен отговор) Ако през деня, за който е направена разпечатката, не е била вкарвана карта на водач, тогава за блок 10.2 се използва показанието на километражния брояч от последното вкарване на карта преди този ден, за което има данни.	Собствено_име_____ Идентификация_на_картата_____ дд/мм/гггг - GEN 2 Нац./VRN_____ дд/мм/гггг hh:mm x xxx xxx **km** M
10.3	*Дейност* Пиктограма за дейност (A), час на започване, времетраене, статус на екипа водачи (пиктограма за екип, ако той се състои от няколко водача, и празни интервали, ако има само един водач)	A hh:mm hh**h**mm ⊙⊙
10.3a	*Особено условие*. Час на задаване, пиктограма (или комбинация от пиктограми — „pppp“) за особеното условие.	hh:mm ---pppp---
10.4	*Изваждане на картата или край на периода „без карта“* Показание на километражния брояч на превозното средство при изваждането на картата или в края на периода „без карта“ и изминато разстояние от вкарването на картата или от началото на периода „без карта“.	x xxx xxx **km**; x xxx **km**

(*) Номерът на поколението на картата може да бъде отпечатан само от интелигентен тахограф.

11	***Ежедневна справка*** Идентификатор на блока	----------Σ----------
11.1	***Справка от VU за периодите без вкарана карта в процепа на четящото устройство на водача*** Идентификатор на блока	1⊙▬---
11.2	***Справка от VU за периодите без вкарана карта в процепа на четящото устройство на втория водач*** Идентификатор на блока	2⊙▬---
11.3	***Ежедневна справка от VU поотделно за всеки водач*** Идентификатор на записа от данни Фамилно име на водача Собствено име (и презиме) на водача Идентификация на картата на водача	---------- ⊙ Фамилно_име_____ Собствено_име_____ Идентификация_на_картата_____
11.4	*Въвеждане на местоположението, в което започва и/или завършва един дневен период на работа* pi = пиктограма за местоположението при тръгване/пристигане, час, държава (Cou), област (Reg) Показание на километражния брояч	pihh:mm Cou Reg x xxx xxx **km**
11.5	*Въвеждане на местоположението, в което започва и/или завършва един дневен период на работа* и след 3 часа непрекъснато управление на МПС Показание на километражния брояч	⁘ hh:mm x xxx xxx **km**
11.6	*Общо времетраене за всяка дейност (извлечено от определена карта)* Обща продължителност на времето на управление на МПС, изминато разстояние Обща продължителност на времето на работа и на времето на разположение Обща продължителност на почивките и на неизвестни дейности Обща продължителност на дейностите в екип	⊙ hh**h**mm x xxx **km** ⚒ hh**h**mm ⧈ hh**h**mm ⊢ hh**h**mm ? hh**h**mm ⊙⊙ hh**h**mm
11.7	*Общо времетраене за всяка дейност (периоди, през които не е имало карта в четящото устройство на водача)* Обща продължителност на времето на управление на МПС, изминато разстояние Обща продължителност на времето на работа и на времето на разположение Обща продължителност на почивките	⊙ hh**h**mm x xxx **km** ⚒ hh**h**mm ⧈ hh**h**mm ⊢ hh**h**mm

11.8 *Общо времетраене за всяка дейност (периоди, през които не е имало карта в четящото устройство на втория водач)*

Обща продължителност на времето на работа и на времето на разположение

Обща продължителност на почивките

```
* hhhmm   ⧈ hhhmm

ㄴ hhhmm
```

11.9 *Общо времетраене за всяка дейност (и за всеки водач, като се вземат под внимание и двете четящи устройства)*

Обща продължителност на времето на управление на МПС, изминато разстояние

Обща продължителност на времето на работа и на времето на разположение

Обща продължителност на почивките

Обща продължителност на дейностите в екип

```
⊙ hhhmm   x xxx km

* hhhmm   ⧈ hhhmm

ㄴ hhhmm
⊙⊙ hhhmm
```

Ако се изисква разпечатка за текущия ден, обобщената информация за деня се изчислява въз основа на наличните данни към момента на разпечатването.

12 ***Събития и/или неизправности, записани върху карта***

12.1 Идентификатор на блока от данни за 5-те последни „събития и неизправности“, извлечени от картата

```
----------!×▬----------
```

12.2 Идентификатор на блока от данни за всички „събития“, записани в картата

```
----------!▬----------
```

12.3 Идентификатор на блока от данни за всички „неизправности“, записани в картата

```
----------×▬----------
```

12.4 *Запис за събитие и/или неизправност*

Идентификатор на записа

Пиктограма (Pic) за събитие/неизправност, цел (p) на записа, дата и час на началото

Допълнителен код за събитие/неизправност (при необходимост), продължителност

Държава членка, в която е регистрирано превозното средство, и регистрационен номер на превозното средство (VRN), в което е възникнало събитието или неизправността

```
  --------------------
Pic (p) дд/мм/гггг hh:mm

!xx                 hhhmm

🚙 Нац./VRN_____________
```

13 ***Събития и/или неизправности, които са записани или в процес на записване във VU***

13.1 Идентификатор на блока от данни за 5-те последни „събития и неизправности“, извлечени от VU

```
----------!×🚙----------
```

13.2 Идентификатор на блока от данни за всички „събития“, които са записани или в процес на записване във VU

```
----------!🚙----------
```

13.3 Идентификатор на блока от данни за всички „неизправности“, които са записани или в процес на записване във VU

```
----------×🚙----------
```

13.4 *Запис за събитие и/или неизправност*

Идентификатор на записа

Пиктограма за събитие/неизправност, цел (p) на записа, дата и час на началото

Допълнителен код за събитие/неизправност (при необходимост), брой подобни събития през същия ден, продължителност

Идентификация на картите, вкарани в началото или в края на съответното събитие или неизправност (до 4 реда, без повтаряне на номерата на картите)

Ако не е била вкарана карта

Специфични за производителя данни

```
  --------------------
Pic (p) dd/mm/yyyy hh:mm

!xx      (xxx)      hhhmm

Идентификация_на_картата_____
Идентификация_на_картата_____
Идентификация_на_картата_____
Идентификация_на_картата_____
 ▬---
< Literal><ErrorCode>
```

Целта (p) на записа се дава чрез цифров код, който посочва защо е записано събитието или неизправността, в съответствие с елемента `EventFaultRecordPurpose` на данните.

`Literal` е специфичен за производителя на тахографа литерал с максимум 12 символа.

`ErrorCode` е специфичен за производителя на тахографа код за грешка с максимум 12 символа.

14 ***Идентификация на VU***

Идентификатор на блока
Наименование на производителя на VU
Адрес на производителя на VU
Идентификационен номер на VU
Номер на одобрението на VU
Сериен номер на VU
Година на производство на VU
Версия на софтуера на VU и дата на инсталиране

```
----------B-----------
B
Наименование__________________
_
  Адрес_________________

Идентификационен_номер______
  ОдобрN°_____________
  СериенN°_____
  гггг
  V xxxx дд/мм/гггг
```

15 ***Идентификация на датчика***

Идентификатор на блока

```
----------Л-----------
```

15.1 *Запис за „сдвояването“ (pairing)*

Сериен номер на датчика
Номер на одобрението на датчика
Дата на първоначалното сдвояване на датчика

```
Л СериенN°_____
  ОдобрN°_____________
  дд/мм/гггг  hh:mm
```

16 ***Идентификация на GNSS***

Идентификатор на блока

```
----------▚----------
```

16.1 *Запис за свързването*

Сериен номер на външното устройство за GNSS
Номер на одобрението на външното устройство за GNSS
Дата на свързването на външното устройство за GNSS

```
▚ СериенN°_____
  ОдобрN°_____________
  дд/мм/гггг  hh:mm
```

17 ***Данни за калибрирането***

Идентификатор на блока

```
----------T-----------
```

17.1 *Запис за калибрирането*

Идентификатор на записа
Сервиз, извършил калибрирането
Адрес на сервиза
Идентификация на картата за монтаж и настройки
Срок на валидност на картата за монтаж и настройки
Празен ред
Датата на калибрирането + цел на калибрирането
Идентификационен номер на превозното средство (VIN)
Държава членка, в която е регистрирано превозното средство, и регистрационен номер на превозното средство (VRN)
Характеристичен коефициент на превозното средство
Константа на контролния уред за регистриране на данните за движението
Effective circumference of wheel tyres
Размер на монтираните гуми
Настройка на устройството за ограничаване на скоростта
Старо и ново показание на километражния брояч

```
   --------------------
T Име_на_сервиза__________
  Адрес_на_сервиза_______
Идентификация_на_картата_____
  дд/мм/гггг

T дд/мм/гггг  (p)
A VIN_________________
  Нац./VRN___________

w xx xxx Imp/km
k xx xxx Imp/km

l xx xxx mm
● Размер_на_гумите________
S xxx  km/h
x xxx xxx - x xxx xxx km
```

Целта (p) на калибрирането се дава чрез цифров код, който посочва защо са записани тези параметри на калибрирането, в съответствие с елемента `CalibrationPurpose` на данните.

18 ***Сверяване на часовника***

Идентификатор на блока

```
----------◷----------
```

18.1 *Запис за сверяването на часовника*

Идентификатор на записа

Стара дата и час

Нова дата и час

Сервиз, извършил сверяването на часовника

Адрес на сервиза

Идентификация на картата за монтаж и настройки

Срок на валидност на картата за монтаж и настройки

```
  --------------------
!◷ дд/мм/гггг  hh:mm
 ◷ дд/мм/гггг  hh:mm
T Име_на_сервиза_________
  Адрес_на_сервиза______
Идентификация_на_картата_____
  дд/мм/гггг
```

19 ***Последни събития и неизправности, записани във VU***

Идентификатор на блока

Дата и час на последното събитие

Дата и час на последната неизправност

```
----------!×д----------
! дд/мм/гггг  hh:mm
× дд/мм/гггг  hh:mm
```

20 ***Информация относно контрола за превишаване на допустимата скорост***

Идентификатор на блока

Дата и час на последния КОНТРОЛ ЗА ПРЕВИШАВАНЕ НА ДОПУСТИМАТА СКОРОСТ

Дата и час на първото превишаване на допустимата скорост и брой на събитията от такъв характер, записани оттогава

```
----------»»----------
»▫дд/мм/гггг  hh:mm

»»дд/мм/гггг hh:mm (nnn)
```

21 ***Запис за превишаванията на скоростта***

21.1 Идентификатор на блока „Първо превишаване на допустимата скорост след последното калибриране“

```
--------»»T---------
```

21.2 Идентификатор на блока „5 най-сериозни превишавания през последните 365 дни“

```
-------»»(365)------
```

21.3 Идентификатор на блока „Най-сериозното превишаване за всеки от последните 10 дни на възникване на това събитие“

```
-------»»(10)-------
```

21.4 Идентификатор на блока

Дата, час и продължителност

Максимална и средна скорост, брой подобни събития през същия ден

Фамилно име на водача

Собствено име (и презиме) на водача

Идентификация на картата на водача

```
  --------------------
»»дд/мм/гггг hh:mm hhhmm
  xxx km/h xxx km/h(xxx)
◙ Фамилно_име_____________
  Собствено_име_____________
Идентификация_на_картата_____
```

21.5 Ако в даден блок няма запис за превишаване на допустимата скорост

```
»»---
```

22 ***Ръчно въведена информация***

Идентификатор на блока

```
------------------------
▫• ..................
▫  ..................
◷+ ..................
+◷ ..................
◙  ..................
```

22.1 Контролен пункт

22.2 Подпис на контрольора

22.3 От час

22.4 До час

22.5 Подпис на водача

„Ръчно въведена информация“: вмъкнете достатъчно празни редове над всеки ръчно въведен елемент, за да можете да впишете необходимата информация или да поставите подписа си.

23 ***Карти, последно вкарани във VU***

Идентификатор на блока

23.1 Вкарана карта

Идентификатор на записа

Вид карта, поколение, версия, производител (*)

Идентификация на картата

Сериен номер на картата

Дата и час на последното вкарване на картата

```
-------- ⊟■⊙ --------

----
⍑ <gen> <version> <MC>
Идентификация на картата
Сериен № на картата
дд/мм/гггг hh:mm
```

(*) (всичко на един ред)

със

вид на картата: пиктограма, един знак + празен интервал

gen („поколение“): GEN1 или GEN2, 4 знака + празен интервал

version *(„версия“):* до 10 символа

MC: код на производителя, 3 символа

3. СПЕЦИФИКАЦИИ ЗА РАЗПЕЧАТКИТЕ

В настоящата глава се прилагат следните условни обозначения:

N	Отпечатване на блока или на записа с номер N
N	Отпечатване на блока или на записа номер N, повторен толкова пъти, колкото е необходимо
X/Y	Отпечатване на блоковете или на записите X и/или Y, според нуждите, и повторение на операцията толкова пъти, колкото е необходимо

3.1. **Ежедневна разпечатка на данните за дейностите на водача, извлечени от карта**

PRT_008 Ежедневната разпечатка на данните за дейностите на водача, извлечени от карта, трябва да бъде в съответствие със следния формат:

1	Дата и час на отпечатване на документа
2	Тип на разпечатката
3	Идентификация на контрольора (ако е вкарана контролна карта във VU)
3	Идентификация на водача (извлечена от картата, която е обект на разпечатката + GEN)
4	Идентификация на превозното средство (от което е направена разпечатката)
5	Идентификация на VU (от което е направена разпечатката + GEN)
6	Последно калибриране на това бордово устройство
7	Последна проверка, на която е бил подложен инспектираният водач
8	Разграничител на данни за дейностите на водача
8a	Условие „Извън обсег“ в началото на този ден
8.1а/ 8.1б/ 8.1в/ 8.2 / 8.3 / 8.3а/ 8.4	Дейности на водача в хронологичен ред
11	Разграничител за ежедневната справка

11.4	Въведени местоположения в хронологичен ред
11.5	GNSS данни
11.6	Общо времетраене на всяка дейност
12.1	Разграничител на данни за събития или неизправности, извлечени от картата
12.4	Записи за събития или неизправности (за последните 5 събития или неизправности, съхранявани в картата)
13.1	Разграничител на данни за събития или неизправности, извлечени от бордовото устройство
13.4	Записи за събития/неизправности (5-те последни събития или неизправности, които са записани или са в процес на записване в бордовото устройство)
22.1	Контролен пункт
22.2	Подпис на контрольора
22.5	Подпис на водача

3.2. **Ежедневна разпечатка на данните за дейностите на водача, извлечени от бордовото устройство**

PRT_009 Ежедневната разпечатка на данните за дейностите на водача, извлечени от бордовото устройство, трябва да бъде в съответствие със следния формат:

1	Дата и час на отпечатване на документа
2	Тип на разпечатката
3	Идентификация на титуляря на картата (за всички карти, вкарани във VU + GEN)
4	Идентификация на превозното средство (от което е направена разпечатката)
5	Идентификация на VU (от което е направена разпечатката + GEN)
6	Последно калибриране на това бордово устройство
7	Последна проверка на този тахограф
9	Разграничител на данни за дейностите на водача
10	Разграничител за четящото устройство за картата на водача (процеп 1)
10a	Условие „Извън обсег“ в началото на този ден
10.1 / 10.2 / 10.3 /10.3a / 10.4	Дейности в хронологичен ред (четящо устройство на водача)
10	Разграничител за четящото устройство за картата на втория водач (процеп 2)
10a	Условие „Извън обсег“ в началото на този ден
10.1 / 10.2 / 10.3 /10.3a / 10.4	Дейности в хронологичен ред (четящо устройство на втория водач)
11	Разграничител за ежедневната справка
11.1	Справка за периодите без вкарана карта в процепа на четящото устройство на водача
11.4	Въведени местоположения в хронологичен ред
11.5	GNSS данни
11.6	Общо времетраене на всяка дейност
11.2	Справка за периодите без вкарана карта в процепа на четящото устройство на втория водач
11.4	Въведени местоположения в хронологичен ред
11.5	GNSS данни

11.7	Общо времетраене на всяка дейност
11.3	Справка за дейностите на водача, като се вземат под внимание и двете четящи устройства
11.4	Местоположения, въведени от този водач в хронологичен ред
11.5	GNSS данни
11.8	Общо времетраене на всяка дейност на този водач
13.1	Разграничител на данни за събития и неизправности
12.4	Записи за събития/неизправности (5-те последни събития или неизправности, които са записани или са в процес на записване в бордовото устройство)
13.1	Контролен пункт
22.2	Подпис на контрольора
22.3	От час (празно място, където водач без карта посочва периодите, валидни за него)
22.4	До час
22.5	Подпис на водача

3.3. **Разпечатка на данните за събития и неизправности, извлечени от картата**

PRT_010 Ежедневната разпечатка на данните за събития и неизправности, извлечени от картата, трябва да е в съответствие със следния формат:

1	Дата и час на отпечатване на документа
2	Тип на разпечатката
3	Идентификация на контрольора (ако е вкарана контролна карта във VU + GEN)
3	Идентификация на водача (извлечена от картата, която е обект на разпечатката)
4	Идентификация на превозното средство (от което е направена разпечатката)
12.2	Разграничител на данни за събития
12.4	Записи за събития (за всички събития, записани върху картата)
12.3	Разграничител на данни за неизправности
12.4	Записи за неизправности (за всички неизправности, записани върху картата)
22.1	Контролен пункт
22.2	Подпис на контрольора
22.5	Подпис на водача

3.4. **Разпечатка на данните за събития и неизправности, извлечени от бордовото устройство**

PRT_011 Разпечатката на данните за събития и неизправности, извлечени от бордовото устройство, трябва да е в съответствие със следния формат:

1	Дата и час на отпечатване на документа
2	Тип на разпечатката
3	Идентификация на титуляря на картата (за всички карти, вкарани във VU + GEN)
4	Идентификация на превозното средство (от което е направена разпечатката)

13.2	Разграничител на данни за събитията
13.4	Записи за събития (за всички събития, които са записани или са в процес на записване в бордовото устройство)
13.3	Разграничител на данни за неизправности
13.4	Записи за неизправности (за всички неизправности, които са записани или са в процес на записване в бордовото устройство)
22.1	Контролен пункт
22.2	Подпис на контрольора
22.5	Подпис на водача

3.5. **Разпечатка на техническите данни**

PRT_012 Разпечатката на техническите данни трябва да е в съответствие със следния формат:

1	Дата и час на отпечатване на документа
2	Тип на разпечатката
3	Идентификация на титуляря на картата (за всички карти, вкарани във VU + GEN)
4	Идентификация на превозното средство (от което е направена разпечатката)
14	Идентификация на бордовото устройство
15	Идентификация на датчика
15.1	Данни за сдвояването на датчика (всички налични данни в хронологичен ред)
16	Идентификация на GNSS
16.1	Данни за свързването на външното устройство за GNSS (всички налични данни в хронологичен ред)
17	Разграничител на данните от калибрирането
17.1	Записи за калибрирането (всички налични записи в хронологичен ред)
18	Разграничител на данни за сверяването на часовника
18.1	Записи за сверяването на часовника (всички налични записи от сверяването на часовника и от калибрирането)
19	Последни събития и неизправности, записани във VU

3.6. **Разпечатка за превишаванията на скоростта**

PRT_013 Разпечатката за превишаванията на скоростта трябва да е в съответствие със следния формат:

1	Дата и час на отпечатване на документа
2	Тип на разпечатката
3	Идентификация на титуляря на картата (за всички карти, вкарани във VU + GEN)
4	Идентификация на превозното средство (от което е направена разпечатката)
20	Информация относно контрола за превишаване на допустимата скорост
21.1	Идентификатор на данните за превишаване на допустимата скорост
21.4 / 21.5	Първо превишаване на допустимата скорост след последното калибриране

21.2	Идентификатор на данните за превишаване на допустимата скорост
21.4 / 21.5	5 най-сериозни превишавания през последните 365 дни
21.3	Идентификатор на данните за превишаване на допустимата скорост
21.4 / 21.5	Най-сериозното превишаване за всеки от последните 10 дни на възникване на това събитие
22.1	Контролен пункт
22.2	Подпис на контрольора
22.5	Подпис на водача

3.7. **Разпечатка за историята на вкараните карти**

PRT_014 Разпечатката за историята на вкараните карти трябва да е в съответствие със следния формат

1	Дата и час на отпечатване на документа
2	Тип на разпечатката
3	Идентификация на титуляря на картата (за всички карти, вкарани в бордовото устройство)
23	Последни карти, вкарани в бордовото устройство
23.1	Вкарани карти (до 88 записа)
12.3	Разграничител на данни за неизправности

Допълнение 5

ПОКАЗВАНЕ

В настоящото допълнение се прилагат следните условни обозначения за формата:

— символите, които се изписани с **удебелен** шрифт, обозначават обикновен текст, който трябва да се покаже (показват се същите символи, но с нормален шрифт),

— символите с нормален шрифт обозначават променливи (пиктограми или данни), които се заместват при показването с техните съответни стойности:

— дд мм гггг: ден, месец, година,

— hh: часове,

— mm: минути,

— D: пиктограма за времетраене,

— EF: комбинация от пиктограми за събитие или неизправност,

— O: пиктограма за режим на работа.

DIS_001 Тахографът трябва да показва данните в следните формати:

Данни	Формат
Показване по подразбиране	
Местно време	hh:mm
Режим на работа	O
Информация относно водача:	**1** Dhh**h**mm **II**hh**h**mm
Информация относно втория водач:	**2** Dhh**h**mm
Отворено условие „Извън обсег“	**OUT**
Показване на предупреждение	
Надвишаване на времето за непрекъснато управление на МПС	**1** ⊙hh**h**mm **II**hh**h**mm
Събитие или неизправност	EF
Показване на други данни	
Дата по координирано универсално време (UTC) час	**UTC** ⊙ дд/мм/гггг или **UTC** ⊙ дд/мм/гггг hh:mm
Време на непрекъснато управление на МПС и общо време на прекъсване за водача	**1** ⊙hh**h**mm **II**hh**h**mm
Време на непрекъснато управление на МПС и общо време на прекъсване за втория водач	**2** ⊙hh**h**mm **II**hh**h**mm
Общо време на управление на МПС на водача през текущата и предходната седмица	**1** ⊙ **II** hhh**h**mm
Общо време на управление на МПС на втория водач през текущата и предходната седмица	**2** ⊙ **II** hhh**h**mm

Допълнение 6

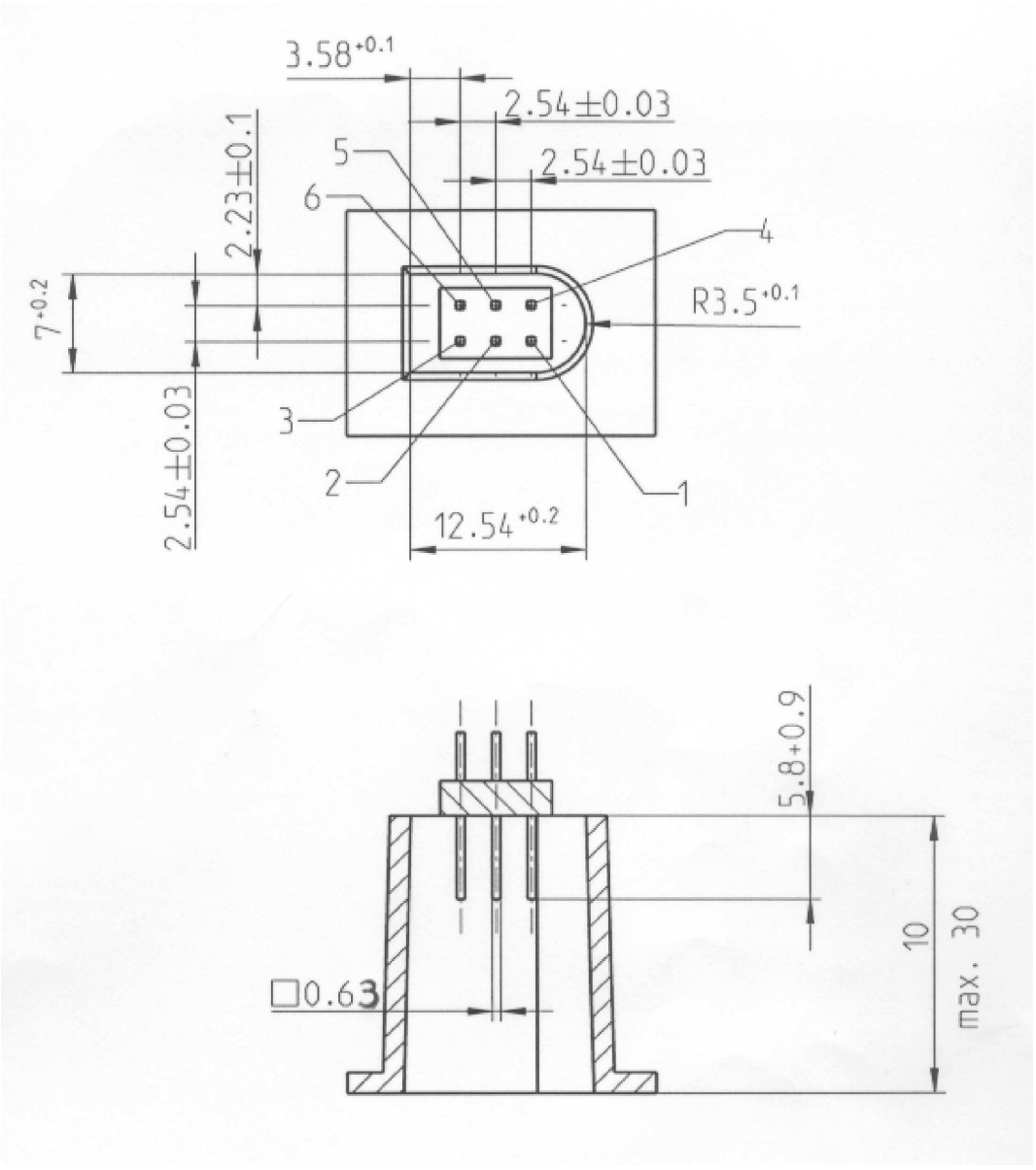
ПРЕДЕН СЪЕДИНИТЕЛ ЗА КАЛИБРИРАНЕ И ИЗТЕГЛЯНЕ НА ДАННИ

СЪДЪРЖАНИЕ

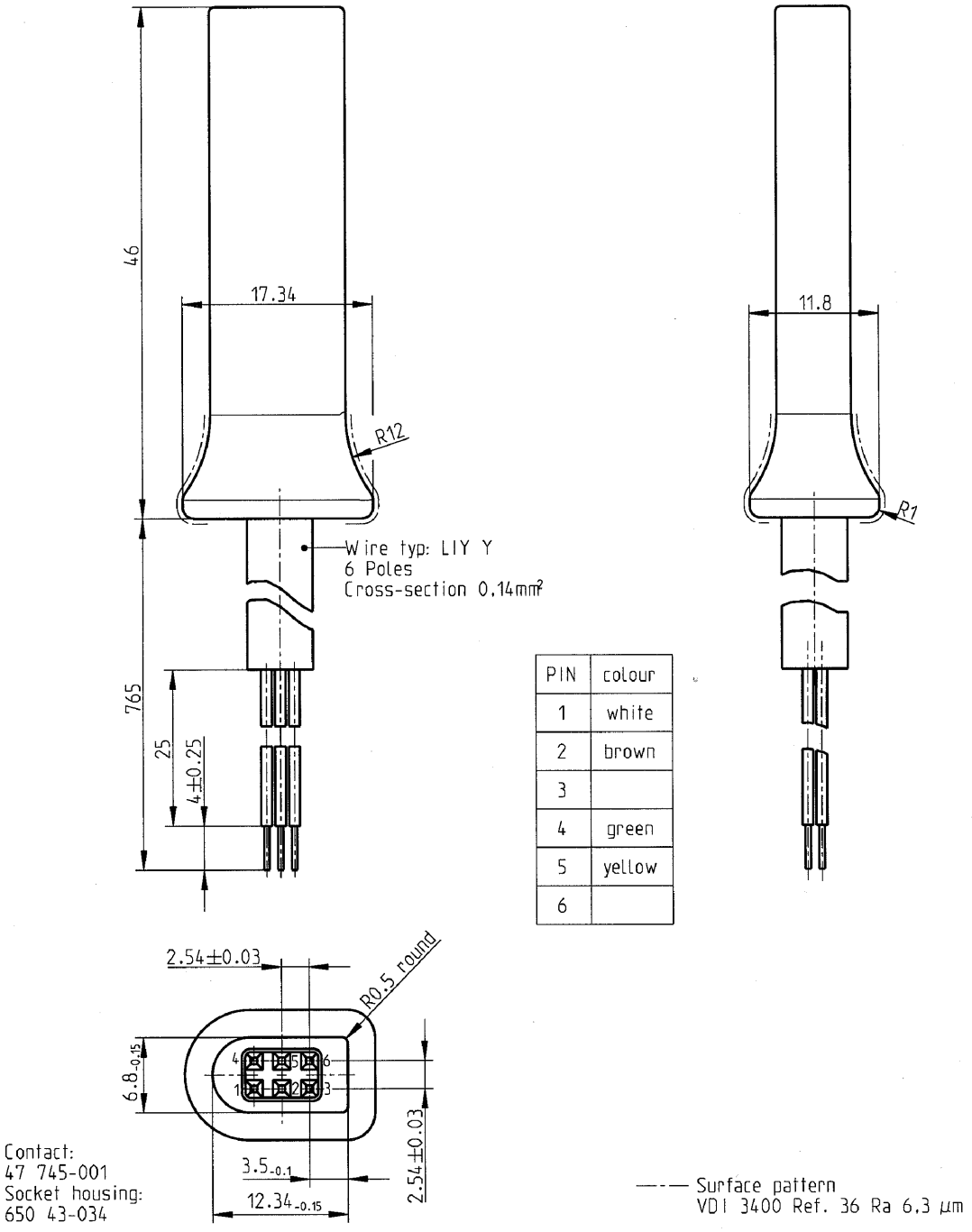
1. ХАРДУЕР

1.1. **Съединител**

INT_001 Съединителят за калибриране/изтегляне на данни трябва да е с шест крачета, да е достъпен върху лицевия панел, без да се налага разкачване на каквато и да е част на тахографа, и да е в съответствие със следния чертеж (всички размери са дадени в милиметри):



На следната схема е показан обичаен контактен съединител с 6 крачета:



1.2. **Разпределение на контактите**

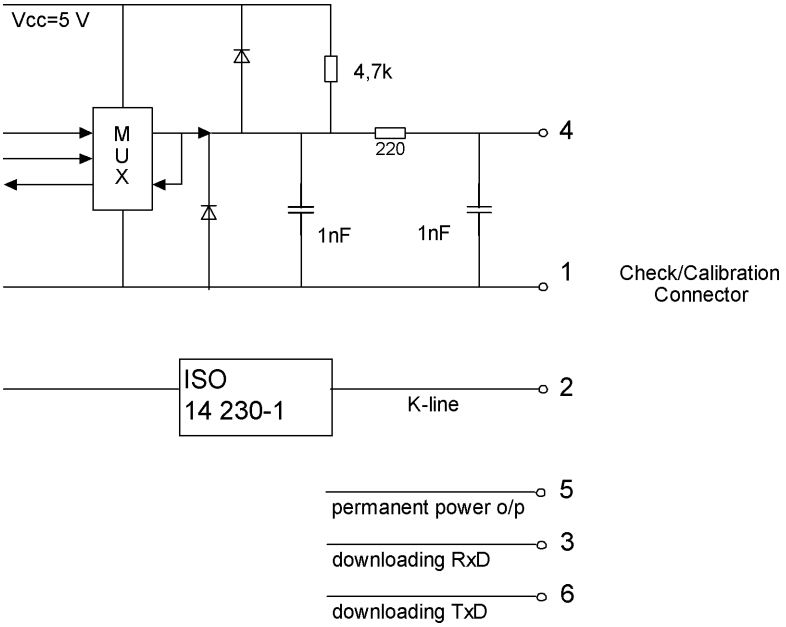
INT_002 Контактите трябва да са разпределени съгласно следната таблица:

Краче	Описание	Забележка
1	Отрицателен полюс на акумулатора	Свързан към отрицателната клема на акумулатора на превозното средство
2	Предаване на данни	Линия K (ISO 14230-1)

Краче	Описание	Забележка
3	RxD — изтегляне на данни	Входящи данни към тахографа
4	Входен/изходен сигнал	Калибриране
5	Постоянна изходяща мощност	Обхватът на напрежението трябва да бъде същият както за електрическото захранване на превозното средство, намален с 3 V, за да се отчете спадът на напрежението през защитните вериги Изход 40 mA
6	TxD — изтегляне на данни	Изходящи данни от тахографа

1.3. **Блоксхема**

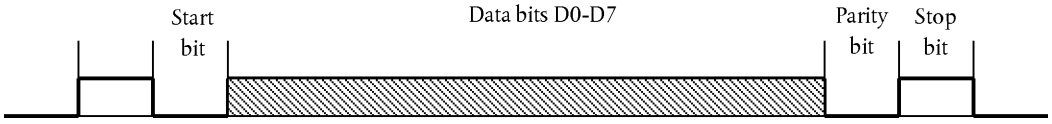
INT_003 Блоксхемата трябва е в съответствие със следното:



2. ИНТЕРФЕЙС ЗА ИЗТЕГЛЯНЕ НА ДАННИ

INT_004 Интерфейсът за изтегляне на данни трябва да е в съответствие със спецификациите RS232.

INT_005 Интерфейсът за изтегляне на данни използва един стартов бит, осем бита за данни (в началото е най-младшият бит), един бит за проверка по четност и един стопов бит.



Организация на байта за данни

Стартов бит: един бит с логическо ниво 0

Битове за данни: предават се, като първи е най-младшият бит

Бит за четност: проверка по четност

Стопов бит: един бит с логическо ниво 1

При предаването на цифрови данни, съставени от повече от един байт, първо се предава най-старшият байт, а най-младшият байт е последен.

INT_006 Скоростта на предаване на данните трябва да може да се регулира от 9 600 bps до 115 200 bps. Предаването на данни се извършва с най-високата възможна скорост, като началната скорост е 9 600 bps.

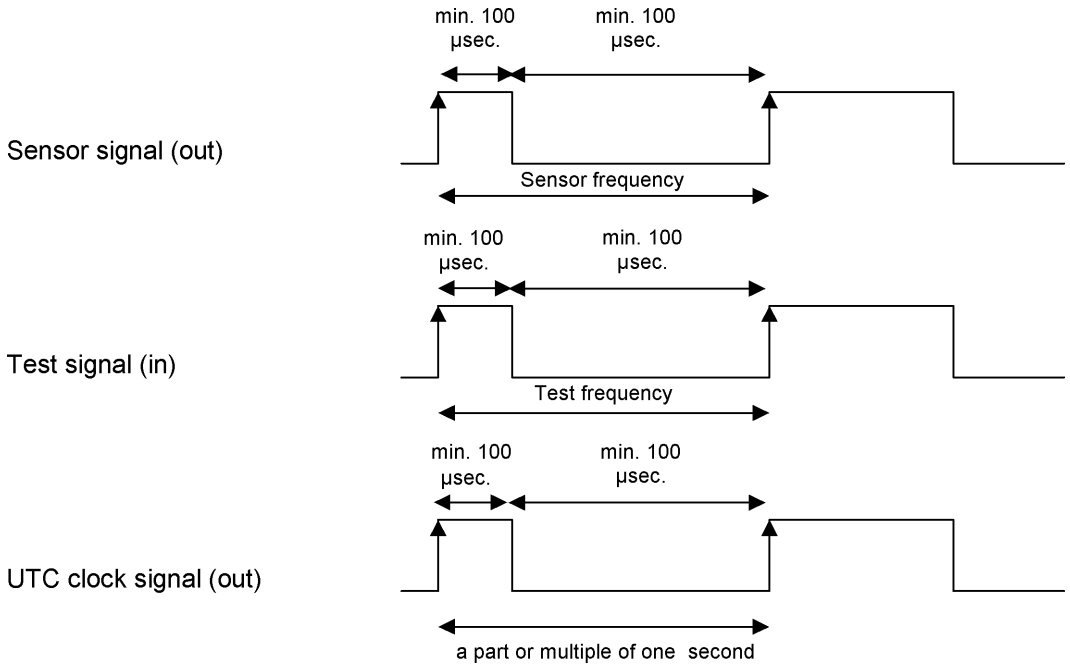
3. ИНТЕРФЕЙС ЗА КАЛИБРИРАНЕ

INT_007 Предаването на данни трябва да е в съответствие с ISO 14 230-1: Пътни превозни средства. Системи за диагностика. Протокол с ключови думи 2000 — част I: физически слой. Първо издание, 1999 г.

INT_008 Входният/изходният сигнал трябва да е в съответствие със следната електрическа спецификация:

Параметър	Минимум	Обичайна стойност	Максимум	Забележка
U_{low} (ниско ниво на входния сигнал)			1,0 V	I = 750 µA
U_{high} (високо ниво на входния сигнал)	4 V			I = 200 µA
Честота			4 kHz	
U_{low} (ниско ниво на изходния сигнал)			1,0 V	I = 1 mA
U_{high} (високо ниво на изходния сигнал)	4 V			I = 1 mA

INT_009 Входният/изходният сигнал трябва да е в съответствие със следните хронограми:



Допълнение 7

ПРОТОКОЛИ ЗА ИЗТЕГЛЯНЕ НА ДАННИ

СЪДЪРЖАНИЕ

1. ВЪВЕДЕНИЕ

В това допълнение са посочени процедурите, които е необходимо да се прилагат за извършване на различните типове изтегляне на данни върху външно запаметяващо устройство, както и протоколите, които трябва да се спазват, за да се осигури правилното прехвърляне на данни и да се гарантира пълната съвместимост на формàта на изтеглените данни с цел всяко контролиращо лице да може да инспектира тези данни, като преди да пристъпи към техния анализ, да може да се увери в тяхната автентичност и цялост.

1.1. **Обхват**

Някои данни могат да бъдат изтеглени върху външно запаметяващо устройство:

— от бордовото устройство чрез специализирано интелигентно устройство (IDE), свързано към това устройство,

— от тахографска карта чрез IDE, оборудвано с интерфейсно устройство за карта (IFD),

— през бордовото устройство от тахографска карта чрез IDE, свързано към устройството.

С цел да се даде възможност за проверка на автентичността и целостта на изтеглените данни, съхранени върху външно запаметяващо устройство, тези данни се придружават от подпис съгласно общите механизми за сигурност от допълнение 11. Данните за идентификацията на изходното оборудване (бордово устройство или карта) и неговите сертификати за сигурност (държава членка и оборудване) също се изтеглят. Проверителят на данните трябва да притежава свой собствен защитен европейски публичен ключ.

DDP_001 Данните, които са изтеглени по време на сесия за изтегляне, трябва да се съхранят в един файл върху външното запаметяващо устройство.

1.2. **Съкращения и означения**

В настоящото допълнение се използват следните съкращения:

AID Идентификатор на приложението

ATR Отговор на инициализиране

CS Байт за контролна сума

DF Специализиран файл

DS_ Диагностична сесия

EF Елементарен файл

ESM Външно запаметяващо устройство

FID Идентификатор на файл

FMT Байт за структура (първи байт на заглавната част на съобщение)

ICC Карта с интегрална схема

IDE Специализирано интелигентно устройство: устройство, което се използва за изтегляне на данни върху ESM (например персонален компютър)

IFD Интерфейсно устройство

KWP Протокол „Keyword 2000“

LEN Байт за дължина (последен байт на заглавната част на съобщение)

PPS Избор на параметрите на протокола

PSO Извършване на операция по сигурността

SID Идентификатор на услуга

SRC Изходен байт

TGT Целеви байт

TLV Стойност за дължината на тага

TREP Параметър на отговор за трансфер

TRTP Параметър на заявка за трансфер

VU Бордово устройство

2. ИЗТЕГЛЯНЕ НА ДАННИ ОТ БОРДОВО УСТРОЙСТВО

2.1. **Процедура за изтегляне на данни**

За да се извърши изтегляне на данни от бордово устройство, потребителят трябва да изпълни следните операции:

— поставя тахографската си карта в процепа за картата на VU (*);

— свързва IDE към съединителя за изтегляне на данни от VU;

— установява връзката между IDE и VU;

— от IDE избира данните, които ще се изтеглят, и изпраща заявката към VU;

— приключва сесията за изтегляне на данни.

2.2. **Протокол за изтегляне на данни**

Структурата на протокола се основава на принципа главно-подчинено устройство, като IDE има функцията на главно устройство, а VU — на подчинено устройство.

Структурата на съобщенията, техните типове и потокът им се основават главно на протокола „Keyword 2000“ (KWP) (ISO 14230-2 Пътни превозни средства. Системи за диагностика. Протокол „Keyword 2000“. Част 2: канален слой).

Приложният слой се основава главно върху актуалния проект за стандарт ISO 14229-1 (Пътни превозни средства. Системи за диагностика. Част 1: услуги за диагностика, версия 6 от 22 февруари 2001 г.).

2.2.1 *Структура на съобщението*

DDP_002 Всички разменени съобщения между IDE и VU се характеризират със структура от три части:

— заглавна част, съставена от байт за структура (FMT), целеви байт (TGT), изходен байт (SRC) и евентуално байт за дължина (LEN);

— поле за данни, съдържащо байт за идентификатор на услуга (SID) и променлив брой байтове за информация, които могат да включат един незадължителен байт за диагностична сесия (DS_) или един незадължителен байт за параметър за трансфер (TRTP или TREP);

— контролна сума, съставена от байт за контролна сума (CS).

Заглавна част				Поле за данни					Контролна сума
FMT	TGT	SRC	LEN	SID	DATA	…	…	…	CS
4 байта				255 байта максимум					1 байт

(*) Поставянето на картата активира съответните права за достъп до функцията за изтегляне на данни и до данните. Трябва да е възможно обаче изтеглянето на данни от карта на водач, вкарана в един от процепите на VU, когато в другия процеп не е поставена друга карта.

Байтовете TGT и SRC представляват физическите адреси на получателя и изпращача на съобщението. Те приемат стойностите F0 Hex за IDE и EE Hex за VU.

Байтът LEN е дължината на полето за данни.

Байтът за контролна сума е серия от суми по 8 бита по модул 256, които представляват всички байтове на съобщението с изключение на самата CS.

Байтовете FMT, SID, DS_, TRTP и TREP са определени по-нататък в този документ.

DDP_003 Ако дължината на данните, които трябва да се пренесат от съобщението, надхвърля свободното пространство в полето за данни, изпращането на това съобщение става под формата на няколко подсъобщения. Всяко подсъобщение съдържа заглавна част, същите SID, TREP и брояч на подсъобщения от 2 байта, който посочва номера на подсъобщението в рамките на цялото съобщение. С цел проверка за грешки и евентуално прекратяване на обмена на данни IDE потвърждава получаването на всяко подсъобщение. IDE може да приеме подсъобщение, да поиска повторното му предаване и да поиска от VU да възобнови или да прекрати предаването.

DDP_004 Ако полето за данни на последното подсъобщение съдържа точно 255 байта, е необходимо да се прибави едно последно подсъобщение, което съдържа празно поле за данни (с изключение на SID TREP и брояча на подсъобщения), за да покаже края на съобщението.

Пример:

Заглавна част	SID	TREP	Съобщение	CS
4 байта	Дължина, по-голяма от 255 байта			

Ще бъде предадено като:

Заглавна част	SID	TREP	00	01	Подсъобщение 1	CS
4 байта	255 байта					

Заглавна част	SID	TREP	00	02	Подсъобщение 2	CS
4 байта	255 байта					

…

Заглавна част	SID	TREP	xx	yy	Подсъобщение n	CS
4 байта	По-малка от 255 байта					

или като:

Заглавна част	SID	TREP	00	01	Подсъоб-щение 1	CS
4 байта	255 байта					

Заглавна част	SID	TREP	00	02	Подсъоб-щение 2	CS
4 байта	255 байта					

…

Заглавна част	SID	TREP	xx	yy	Подсъобщение n	CS
4 байта	255 байта					

Заглавна част	SID	TREP	xx	yy + 1	CS
4 байта	4 байта				

2.2.2 *Типове съобщения*

Протоколът за връзка за изтегляне на данни между VU и IDE изисква обмен на 8 различни типа съобщения.

Следващата таблицата обобщава тези съобщения.

Структура на съобщението	4 байта максимум Заглавна част				255 байта максимум Данни			1 байт Контролна сума
IDE -> <- VU	FMT	TGT	SRC	LEN	SID	DS_/TRTP	DATA	CS
Start Communication Request	81	EE	F0		81			E0
Positive Response Start Communication	80	F0	EE	03	C1		EA, 8F	9B
Start Diagnostic Session Request	80	EE	F0	02	10	81		F1
Positive Response Start Diagnostic	80	F0	EE	02	50	81		31
Link Control Service Verify Baud Rate (stage 1)								
9 600 Bd	80	EE	F0	04	87		01,01, 01	EC
19 200 Bd	80	EE	F0	04	87		01,01, 02	ED
38 400 Bd	80	EE	F0	04	87		01,01, 03	EE
57 600 Bd	80	EE	F0	04	87		01,01, 04	EF
115 200 Bd	80	EE	F0	04	87		01,01, 05	F0
Positive Response Verify Baud Rate	80	F0	EE	02	C7		01	28
Transition Baud Rate (stage 2)	80	EE	F0	03	87		02,03	ED
Request Upload	80	EE	F0	0A	35		00,00, 00,00, 00,FF,FF, FF,FF	99
Positive Response Request Upload	80	F0	EE	03	75		00,FF	D5

Структура на съобщението	4 байта максимум Заглавна част				255 байта максимум Данни			1 байт Контролна сума
IDE -> <- VU	FMT	TGT	SRC	LEN	SID	DS_/TRTP	DATA	CS
Transfer Data Request								
Overview	80	EE	F0	02	36	01		97
Activities	80	EE	F0	06	36	02	Date	CS
Events & Faults	80	EE	F0	02	36	03		99
Detailed Speed	80	EE	F0	02	36	04		9A
Technical Data	80	EE	F0	02	36	05		9B
Card download	80	EE	F0	02	36	06	Slot	CS
Positive Response Transfer Data	80	F0	EE	Len	76	TREP	Data	CS
Request Transfer Exit	80	EE	F0	01	37			96
Positive Response Request Transfer Exit	80	F0	EE	01	77			D6
Stop Communication Request	80	EE	F0	01	82			E1
Positive Response Stop Communication	80	F0	EE	01	C2			21
Acknowledge sub message	80	EE	F0	Len	83		Data	CS
Negative responses								
General reject	80	F0	EE	03	7F	Sid Req	10	CS
Service not supported	80	F0	EE	03	7F	Sid Req	11	CS
Sub function not supported	80	F0	EE	03	7F	Sid Req	12	CS
Incorrect Message Length	80	F0	EE	03	7F	Sid Req	13	CS
Conditions not correct or Request sequence error	80	F0	EE	03	7F	Sid Req	22	CS
Request out of range	80	F0	EE	03	7F	Sid Req	31	CS
Upload not accepted	80	F0	EE	03	7F	Sid Req	50	CS
Response pending	80	F0	EE	03	7F	Sid Req	78	CS
Data not available	80	F0	EE	03	7F	Sid Req	FA	CS

Забележки:

— Sid Req = the Sid на съответната заявка.

— TREP = the TRTP на съответната заявка.

— Черните полета означава, че нищо не е предадено.

— Терминът „upload“ [„качване на данни“] (от IDE) се използва за съвместимостта със стандарта ISO 14229. Този термин притежава същото значение като „download“ [„изтегляне на данни“] (от VU).

— В тази таблица не са показани потенциални броячи за подсъобщения от 2 байта.

— Процеп е номерът на процепа — или 1 (карта в процепа за водача), или 2 (карта в процепа за втория водач).

— Ако процепът не е посочен, VU избира процеп 1, ако картата е поставена в този процеп, а процеп 2 — само ако този процеп е специално избран от потребителя.

2.2.2.1 Start Communication Request (SID 81)

DDP_005 Това съобщение се подава от IDE за установяване на връзка с VU. Началната връзка се извършва винаги със скорост от 9 600 бода (до момента, когато тази скорост за предаване на данни се промени с помощта на съответните услуги за контрол на връзките).

2.2.2.2 Positive Response Start Communication (SID C1)

DDP_006 VU изпраща това съобщение, за да отговори положително на start communication request. То съдържа двата ключови байта 'EA' и '8F', които указват, че съответното устройство поддържа протокол със заглавна част, включително целевата и изходната информация и информацията за дължината.

2.2.2.3 Start Diagnostic Session Request (SID 10)

DDP_007 IDE изпраща съобщение за Start Diagnostic Session request с цел заявяване на нова диагностична сесия с VU. Подфункцията „default session" (81 Hex) указва, че ще започне стандартна диагностична сесия.

2.2.2.4 Positive Response Start Diagnostic (SID 50)

DDP_008 VU изпраща съобщение Positive Response Start Diagnostic, за да отговори положително на Diagnostic Session Request.

2.2.2.5 Link Control Service (SID 87)

DDP_052 Link Control Service се използва от IDE, за да започне промяна в скоростта за предаване на данни. Тази операция включва два етапа. През първия етап IDE предлага промяна в скоростта за предаване на данни, като посочва нова скорост. При получаване на положително съобщение от VU IDE изпраща потвърждение на промяната в скоростта за предаване на данни до VU (втори етап). Тогава IDE преминава към новата скорост за предаване на данни. След получаване на потвърждението VU преминава към новата скорост за предаване на данни.

2.2.2.6 Link Control Positive Response (SID C7)

DDP_053 Link Control Positive Response се подава от VU, за да се отговори положително на Link Control Service request (първи етап). Трябва да се отбележи, че на заявката за потвърждение не се дава никакъв отговор (втори етап).

2.2.2.7 Request Upload (SID 35)

DDP_009 IDE изпраща съобщение за Request Upload, за да посочи на VU, че заявява изпълнение на операция по изтегляне на данни. За да се изпълнят изискванията на стандарта ISO 14229, се включват данни относно адреса, размера и характеристиките на формàта на заявените данни. Тъй като тази информация не е известна на IDE преди изтегляне на данните, адресът в паметта се нулира, формàтът се декриптира и декомпресира и размерът на паметта се определя на максимума.

2.2.2.8 Positive Response Request Upload (SID 75)

DDP_010 VU изпраща съобщение Positive Response Request Upload, за да съобщи на IDE, че е готов да изтегли данните. За да се изпълнят изискванията на стандарт ISO 14229, положителното съобщение за отговор съдържа данни, които показват на IDE, че следващите съобщения Positive Response Transfer Data ще съдържат максимум 00FF hex байта.

2.2.2.9 Transfer Data Request (SID 36)

DDP_011 IDE изпраща Transfer Data Request, за да уточни на VU вида на данните, които трябва да се изтеглят. Transfer Request Parameter (TRTP) на определен байт показва типа трансфер.

Съществуват шест типа трансфер на данни:

— Overview (TRTP 01),

— Activities of a specified date (TRTP 02),

— Events and faults (TRTP 03),

— Detailed speed (TRTP 04),

— Technical data (TRTP 05),

— Card download (TRTP 06).

DDP_054 За IDE е задължително да заяви overview data transfer (TRTP 01) по време на сесия за изтегляне на данни, защото единствено това гарантира, че сертификатите на VU се регистрират в изтегления файл (и по този начин позволява проверката на електронния подпис).

Във втория случай (TRTP 02) съобщението Transfer Data Request съдържа указание за календарния ден (формат `TimeReal`), чиито данни трябва да се изтеглят.

2.2.2.10 Positive Response Transfer Data (SID 76)

DDP_012 VU изпраща Positive Response Transfer Data в отговор на Transfer Data Request. Съобщението съдържа заявените данни с Transfer Response Parameter (TREP), съответстващ на TRTP на заявката.

DDP055 В първия случай (TREP 01) VU ще изпрати данни, предназначени да помогнат на потребителя на IDE при избора на данните, които иска да изтегли. Информацията, която се съдържа в това съобщение, е:

— сертификати за сигурност,

— идентификация на превозното средство,

— актуалната дата и час на VU,

— най-ранната и най-късната дата за изтегляне на данните (данни от VU),

— указване за наличието на карти в VU,

— предишни изтеглени данни към превозвач,

— блокировки от страна на превозвача,

— предишни проверки.

2.2.2.11 Request Transfer Exit (SID 37)

DDP_013 IDE изпраща съобщение Request Transfer Exit, за да информира VU, че сесията за изтегляне на данни е приключена.

2.2.2.12 Positive Response Request Transfer Exit (SID 77)

DDP_014 VU изпраща съобщение Positive Response Request Transfer Exit, за да потвърди получаването на Request Transfer Exit.

2.2.2.13 Stop Communication Request (SID 82)

DDP_015 IDE изпраща съобщение Stop Communication Request с цел преустановяване на връзката с VU.

2.2.2.14 Positive Response Stop Communication (SID C2)

DDP_016 VU изпраща съобщение Positive Response Stop Communication, за да потвърди получаването на Stop Communication Request.

2.2.2.15 Acknowledge Sub Message (SID 83)

DDP_017 IDE изпраща Acknowledge Sub Message с цел потвърждение получаването на различните части от съобщението, изпратени под формата на подсъобщения. Полето за данни съдържа SID, получен от VU, както и следния код от 2 байта:

— MsgC + 1 потвърждава правилното получаване на подсъобщение номер MsgC.

Заявка за изпращане на следващото подсъобщение, адресирано от IDE до VU.

— MsgC посочва появяването на проблем, който засяга получаването на подсъобщение номер MsgC.

Заявка за повторно изпращане на подсъобщение, адресирано от IDE до VU.

— FFFF заявява прекъсване на съобщението.

IDE може да използва това, за да сложи край на предаването на съобщението от VU поради каквато и да е причина.

Възможно е да се потвърди последното подсъобщение от съобщение (байт LEN < 255), като се използва някой от тези кодове.

Отговорите на VU, които ще са съставени от няколко подсъобщения, са:

— Positive Response Transfer Data (SID 76)

2.2.2.16 Negative Response (SID 7F)

DDP_018 VU изпраща съобщение Negative Response в отговор на съобщенията по-горе, ако не е в състояние да удовлетвори заявката. Полетата за данни на съобщението съдържат SID на отговора (7F), SID на заявката и код, който уточнява причината за отрицателния отговор. Налични са следните кодове:

— 10 — общо отхвърляне

Действието не може да се изпълни по причина, която не се разглежда по-нататък.

— 11 — услугата не се поддържа

SID на заявката не се разбира.

— 12 — подфункцията не се поддържа

DS_ или TRTP на заявката не се разбира или предаването на подсъобщения е приключило.

— 13 — неправилна дължина на съобщение

Дължината на полученото съобщение е грешна.

— 22 — неправилни условия или грешка, която засяга последователността на заявяването

Заявената услуга не е активна или последователността на съобщенията за заявката е неправилна.

— 31 — недопустимост на заявката

Записването (полето за данни) на параметъра на заявката не е валидно.

— 50 — качването на данни не е прието

Заявката не може да се изпълни (VU се използва в несвойствен режим на работа или има някаква вътрешна неизправност на VU).

— 78 — изчакване на отговор

Заявеното действие не може да приключи в определеното време и VU няма готовност да приеме друга заявка.

— Данни FA, които не са на разположение

Обектът от данни на заявка за трансфер на данни не е достъпен в VU (например не е поставена карта, …).

2.2.3 *Поток на съобщенията*

При нормална процедура за изтегляне на данни потокът на съобщенията обикновено е следният:

IDE		VU
Start Communication Request	⇨ ⇦	Positive Response
Start Diagnostic Service Request	⇨ ⇦	Positive Response
Request Upload	⇨ ⇦	Positive Response

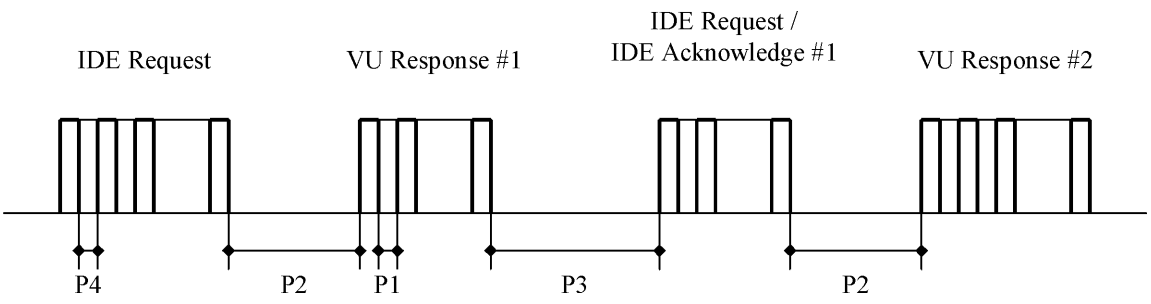
IDE		VU
Transfer Data Request Overview	⇨	
	⇦	Positive Response
Transfer Data Request #2	⇨	
	⇦	Positive Response #1
Acknowledge Sub Message #1	⇨	
	⇦	Positive Response #2
Acknowledge Sub Message #2	⇨	
	⇦	Positive Response #m
Acknowledge Sub Message #m	⇨	
	⇦	Positive Response (Data Field<255 Bytes)
Acknowledge Sub Message (optional)	⇨	
…		
Transfer Data Request #n	⇨	
	⇦	Positive Response
Request Transfer Exit	⇨	
	⇦	Positive Response
Stop Communication Request	⇨	
	⇦	Positive Response

2.2.4 *Синхронизация*

DDP_019 При нормални условия на работа се прилагат следните параметри за синхронизация, илюстрирани на следната фигура:

Фигура 1

Поток на съобщенията, синхронизация



където:

P1 = междубайтово време за отговора на VU,

P2 = времето между края на заявка на IDE и началото на отговор на VU или между края на потвърждаване от IDE и начало на следващ отговор от VU,

P3 = времето между края на отговор на VU и началото на нова заявка на IDE, между края на отговор на VU и началото на потвърждаване от IDE или между края на заявка от IDE и началото на нова заявка от IDE, ако VU не даде отговор,

P4 = междубайтово време за заявка на IDE,

P5 = разширена стойност на P3 за изтегляне на данни от карти.

В следващата таблица са показани разрешените стойности за параметрите за синхронизация (разширен набор от параметри за синхронизация KWP, използвани в случай на физическо адресиране за по-бърза връзка).

Синхронизация Параметър	Долна граница Стойност (в ms)	Горна граница Стойност (в ms)
P1	0	20
P2	20	1 000 (*)
P3	10	5 000
P4	5	20
P5	10	20 минути

(*) ако VU отговори с Negative Response, съдържащ код със значение „request correctly received, response pending“ („правилно получена заявка, очаква се отговор“), тази стойност се разширява до същата горна стойност на P3.

2.2.5 *Обработка на грешки*

Ако се появи грешка по време на обмена на съобщения, схемата за поток на съобщенията се променя в зависимост от устройството, което е открило грешката, и от съобщението, което е породило тази грешка.

На фигури 2 и 3 са показани процедурите за обработване на грешки, които се прилагат съответно за VU и IDE.

2.2.5.1 Start Communication phase

DDP_020 Ако IDE открие грешка по време на Start Communication phase, както на ниво синхронизация, така и на ниво последователност на битовете, тогава то изчаква за период от P3 min, преди да изпрати отново заявката.

DDP_021 Ако VU открие грешка в последователността, която идва от IDE, то не изпраща никакъв отговор и изчаква друго съобщение Start Communication Request в рамките на период от P3 max.

2.2.5.2 Communication phase

Могат да се определят две различни процедури за обработване на грешки:

1. **VU открива грешка в предаването от IDE**

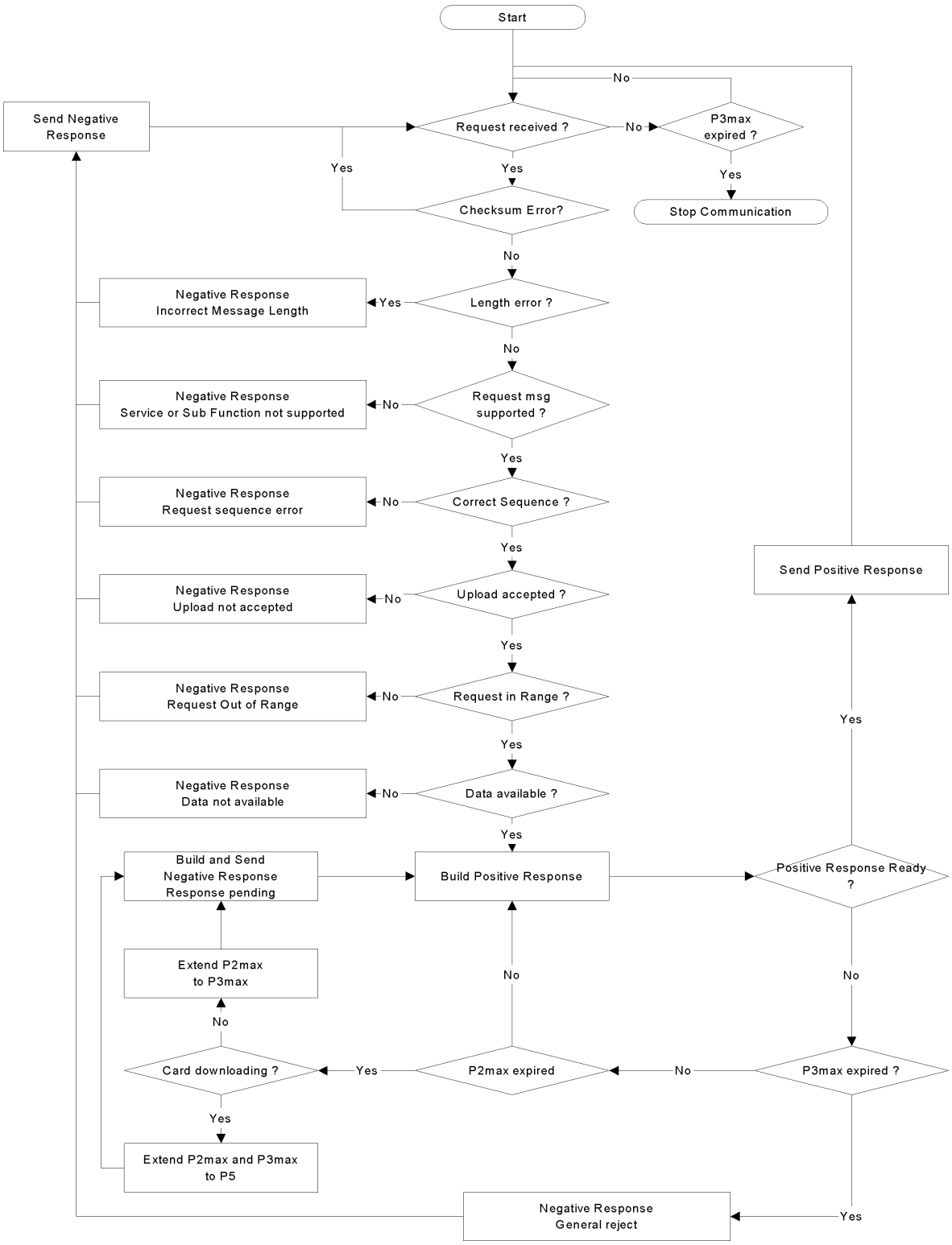
DDP_022 VU извършва анализ на всяко получено съобщение, за да открие евентуална грешка по синхронизирането, структурата на байтовете (например нарушения, които засягат началните битове и битовете за край) или грешки във връзка с кадрите (приемане на грешен брой байтове, грешен байт за контролна сума).

DDP_023 Ако VU открие една от горепосочените грешки, то не изпраща никакъв отговор и не взема под внимание полученото съобщение.

DDP_024 VU може да открие други грешки, които засягат структурата или съдържанието на полученото съобщение (например съобщението не се поддържа) даже и ако съобщението отговаря на изискванията за дължина и контролна сума; в такъв случай VU трябва да отговори на IDE със съобщение Negative Response, което указва характера на грешката.

Фигура 2

Обработка на грешки в VU



2. **IDE открива грешка при предаването от VU**

DDP_025 IDE извършва анализ на всяко получено съобщение, за да открие евентуална грешка по синхронизирането, структурата на байтовете (например нарушения, които засягат началните битове и битовете за край) или грешки във връзка с кадрите (приемане на грешен брой байтове, грешен байт за контролна сума).

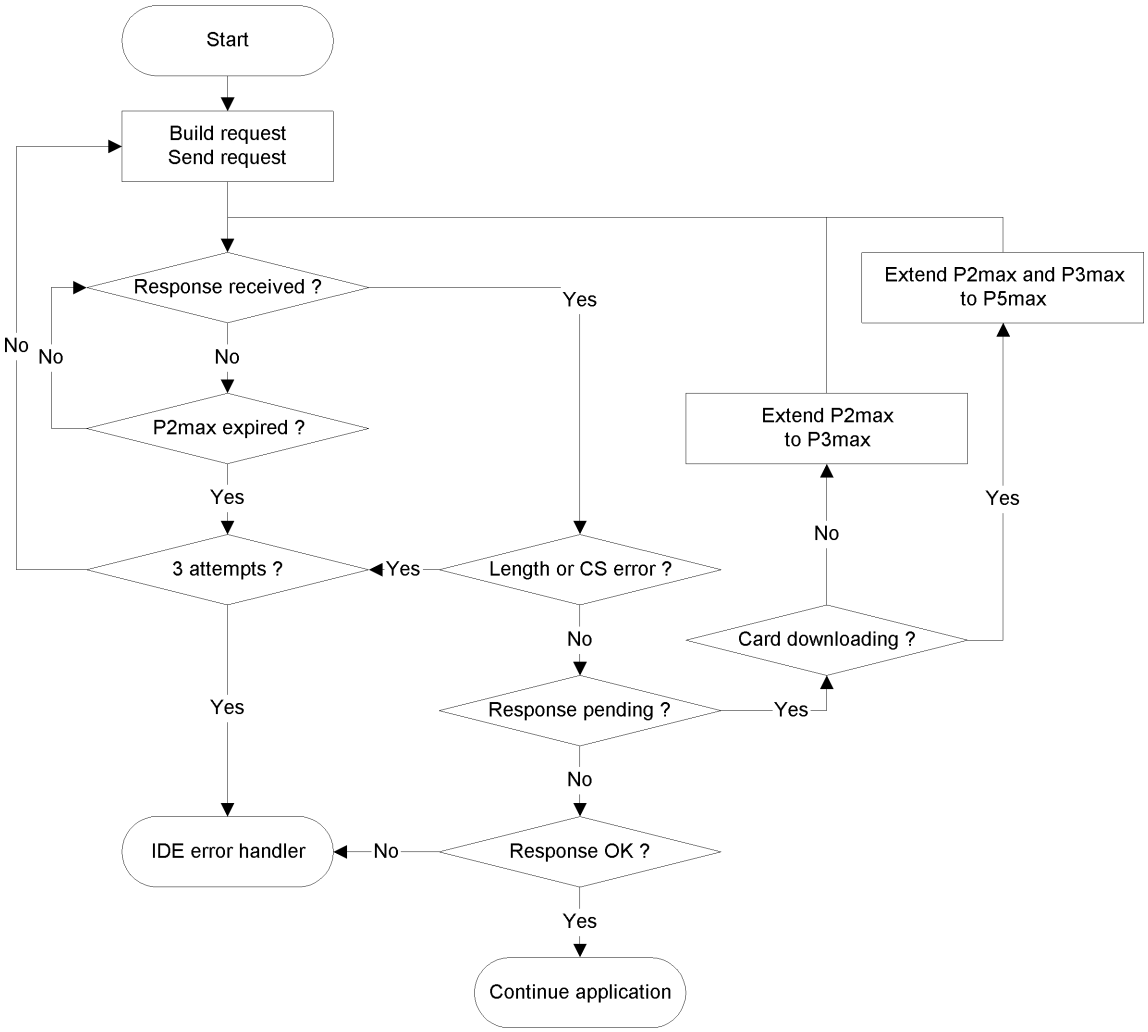
DDP_026 IDE открива грешки при последователността, като например погрешно увеличение на брояча на подсъобщения в последователно получени съобщения.

DDP_027 Ако IDE открие грешка или ако VU не му изпрати никакъв отговор в срок от максимум P2, съобщението за заявка ще бъде отново изпратено общо най-много три пъти. За целите на това откриване на грешки всяко потвърждаване за подсъобщение ще се разглежда като заявка до VU.

DDP_028 IDE трябва да изчака в продължение най-малко на P3min, преди започване на предаване на данни; времето за изчакване се измерва от последната поява на бит за край след откриване на съответната грешка.

Фигура 3

Обработка на грешки на ниво на IDE



2.2.6 *Съдържание на съобщенията за отговор*

В този параграф е определено съдържанието на полетата за данни на различните положителни съобщения за отговор.

Елементите от данни са определени в допълнение 1 (Речник на данните).

Забележка: при изтеглените данни от поколение 2 всеки елемент от данни от най-високо ниво е представен от масив записи дори ако съдържа само един запис. Масивът записи започва със заглавна част, която съдържа типа, размера и броя записи. Масивите записи имат наименованието„…RecordArray“ (със заглавна част) в следващите таблици.

2.2.6.1 Positive Response Transfer Data Overview

DDP_029 Полето за данни на съобщението „Positive Response Transfer Data Overview“ трябва да дава данните по-долу по следния ред по SID 76 Hex, TREP 01 Hex и съответните критерии за разделяне и прекъсване на подсъобщенията:

Структура на данните от поколение 1

Елемент от данни	Коментар
MemberStateCertificate VUCertificate	Сертификати за сигурност на VU
VehicleIdentificationNumber VehicleRegistrationIdentification	Идентификация на превозното средство
CurrentDateTime	Актуална дата и час на VU
VuDownloadablePeriod	Период за изтегляне на данни
CardSlotsStatus	Тип карти, поставени в VU
VuDownloadActivityData	Предишни изтеглени данни от VU
VuCompanyLocksData	Всички съхранени блокировки от страна на превозвача. Ако тази част е празна, се изпраща само noOfLocks = 0
VuControlActivityData	Всички съхранени в VU контролни записи. Ако тази част е празна, се изпраща само noOfControls = 0
Signature	RSA подпис на всички данни (освен сертификатите), започвайки от VehicleIdentificationNumber до последния байт на последния VuControlActivityData

Структура на данните от поколение 2

Елемент от данни	Коментар
MemberStateCertificateRecordArray	Сертификат на държава членка
VUCertificateRecordArray	Сертификат за VU
VehicleIdentificationNumberRecordArray	Идентификация на превозното средство
VehicleRegistrationNumberRecordArray	Регистрационен номер на превозното средство
CurrentDateTimeRecordArray	Актуална дата и час на VU
VuDownloadablePeriodRecordArray	Период за изтегляне на данни
CardSlotsStatusRecordArray	Тип карти, вкарани в VU
VuDownloadActivityDataRecordArray	Предишни изтеглени данни от VU
VuCompanyLocksRecordArray	Всички съхранени блокировки от страна на превозвача. Ако тази част е празна, се изпраща заглавна част на масив с noOfRecords = 0
VuControlActivityRecordArray	Всички съхранени в VU контролни записи. Ако тази част е празна, се изпраща заглавна част на масив с noOfRecords = 0
SignatureRecordArray	ECC подпис на всички предходни данни освен сертификатите

2.2.6.2 Positive Response Transfer Data Activities

DDP_030 Полето за данни на съобщението„Positive Response Transfer Data Activities“ трябва да дава данните по-долу по следния ред по SID 76 Hex, TREP 02 Hex и съответните критерии за разделяне и преброяване на подсъобщенията:

Структура на данните от поколение 1

Елемент от данни	Коментар
TimeReal	Дата на деня, за който са изтеглени данни
OdometerValueMidnight	Километражен брояч в края на деня, за който са изтеглени данни
VuCardIWData	Данни за циклите на поставяне и изваждане на картите. — Ако тази част не съдържа данни, се изпраща само noOfVuCardIWRecords = 0. — Когато VuCardIWRecord обхваща период, който започва преди 00:00 ч. (поставяне на картата в предходния ден) или приключва след 24:00 ч. (изваждане на картата на следващия ден), този елемент от данни се появява цялостно в записите за двата съответни дни
VuActivityDailyData	Статус на процепите в 00:00 ч. и промени на дейността, записани за деня, за който са изтеглени данни
VuPlaceDailyWorkPeriodData	Данни във връзка с местоположенията, записани за деня, за който са изтеглени данни. Ако тази част е празна, се изпраща само noOfPlaceRecords = 0
VuSpecificConditionData	Данни във връзка със специфични условия, записани за деня, за който са изтеглени данни. Ако тази част е празна, се изпраща само noOfSpecificConditionRecords = 0
Signature	RSA подпис на всички данни, започвайки от TimeReal до последния байт на последния запис за специфично условие

Структура на данните от поколение 2

Елемент от данни	Коментар
DateOfDayDownloadedRecordArray	Дата на деня, за който са изтеглени данни
OdometerValueMidnightRecordArray	Километражен брояч в края на деня, за който са изтеглени данни
VuCardIWRecordArray	Данни за циклите на поставяне и изваждане на картите. — Ако тази част не съдържа налични данни, се изпраща заглавна част на масив с noOfRecords = 0. — Когато VuCardIWRecord обхваща период, който започва преди 00:00 ч. (поставяне на картата в предходния ден) или приключва след 24:00 ч. (изваждане на картата на следващия ден), този елемент от данни се появява цялостно в записите за двата съответни дни.
VuActivityDailyRecordArray	Статус на процепите в 00:00 ч. и промени на дейността, записани за деня, за който са изтеглени данни
VuPlaceDailyWorkPeriodRecordArray	Данни във връзка с местоположенията, записани за деня, за който са изтеглени данни. Ако тази част е празна, се изпраща заглавна част на масив с noOfRecords = 0
VuGNSSCDRecordArray	Местоположения по GNSS на превозното средство, ако времето за непрекъснато управление на водача достигне число, кратно на три часа. Ако тази част е празна, се изпраща заглавна част на масив с noOfRecords = 0
VuSpecificConditionRecordArray	Данни във връзка със специфични условия, записани за деня, за който са изтеглени данни. Ако тази част е празна, се изпраща заглавна част на масив с noOfRecords = 0
SignatureRecordArray	ECC подпис на всички предходни данни

2.2.6.3 Positive Response Transfer Data Events and Faults

DDP_031 Полето за данни на съобщението „Positive Response Transfer Data Events and Faults“ трябва да дава данните по-долу по следния ред по SID 76 Hex, TREP 03 Hex и съответните критерии за разделяне и прекъсване на подсъобщенията:

Структура на данните от поколение 1

Елемент от данни	Коментар
VuFaultData	Всички записани или текущи неизправности в VU. Ако тази част е празна, се изпраща само noOfVuFaults = 0
VuEventData	Всички записани или текущи събития в VU (освен превишаването на скоростта). Ако тази част е празна, се изпраща само noOfVuEvents = 0
VuOverSpeedingControlData	Данни във връзка с последната проверка за превишаване на скоростта (стойност по подразбиране, ако няма данни)
VuOverSpeedingEventData	Всички събития „превишаване на скоростта“, записани в VU. Ако тази част е празна, се изпраща само noOfVuOverSpeedingEvents = 0
VuTimeAdjustmentData	Всички събития „сверяване на часовника“, записани в VU (извън рамките на пълно калибриране). Ако тази част е празна, се изпраща само noOfVuTimeAdjRecords = 0
Signature	RSA подпис на всички данни, започвайки от noOfVuFaults до последния байт на последния запис за сверяване на часовника

Структура на данните от поколение 2

Елемент от данни	Коментар
VuFaultRecordArray	Всички записани или текущи неизправности в VU. Ако тази част е празна, се изпраща заглавна част на масив с noOfRecords = 0
VuEventRecordArray	Всички записани или текущи събития в VU (освен превишаването на скоростта). Ако тази част е празна, се изпраща заглавна част на масив с noOfRecords = 0
VuOverSpeedingControlDataRecordArray	Данни във връзка с последната проверка за превишаване на скоростта (стойност по подразбиране, ако няма данни)
VuOverSpeedingEventRecordArray	Всички събития „превишаване на скоростта“, записани в VU. Ако тази част е празна, се изпраща заглавна част на масив с noOfRecords = 0
VuTimeAdjustmentRecordArray	Всички събития „сверяване на часовника“, записани в VU (извън рамките на пълно калибриране). Ако тази част е празна, се изпраща заглавна част на масив с noOfRecords = 0
VuTimeAdjustmentGNSSRecordArray	
SignatureRecordArray	ECC подпис на всички предходни данни

2.2.6.4 Positive Response Transfer Data Detailed Speed

DDP_032 Полето за данни на съобщението „Positive Response Transfer Data Detailed Speed“ трябва да дава данните по-долу по следния ред по SID 76 Hex, TREP 04 Hex и съответните критерии за разделяне и преброяване на подсъобщенията:

Структура на данните от поколение 1

Елемент от данни	Коментар
VuDetailedSpeedData	Всички подробни данни за скоростта в VU (един блок с данни за скоростта на минута, през която превозното средство е в движение) 60 стойности на скоростта на минута (една на секунда)
Signature	RSA подпис на всички данни, започвайки от noOfSpeedBlocks до последния байт на последния блок данни за скоростта

Структура на данните от поколение 2

Елемент от данни	Коментар
VuDetailedSpeedBlockRecordArray	Всички подробни данни за скоростта в VU (един блок с данни за скоростта на минута, през която превозното средство е в движение) 60 стойности на скоростта на минута (една на секунда)
SignatureRecordArray	ECC подпис на всички предходни данни

2.2.6.5 Positive Response Transfer Data Technical Data

DDP_033 Полето за данни на съобщението „Positive Response Transfer Data Technical Data“ трябва да дава данните по-долу по следния ред по SID 76 Hex, TREP 05 Hex и съответните критерии за разделяне и преброяване на подсъобщенията:

Структура на данните от поколение 1

Елемент от данни	Коментар
VuIdentification	
SensorPaired	
VuCalibrationData	Всички записи за калибриране, съхранени в VU
Signature	RSA подпис на всички данни, започвайки от vuManufacturerName до последния байт на последния VuCalibrationRecord

Структура на данните от поколение 2

Елемент от данни	Коментар
VuIdentificationRecordArray	
VuSensorPairedRecordArray	Всички сдвоявания с датчика за движение (MS), съхранени в VU
VuSensorExternalGNSSCoupledRecordArray	Всички свързвания с външното устройство за GNSS, съхранени в VU
VuCalibrationRecordArray	Всички записи за калибриране, съхранени в VU
VuCardRecordArray	Всички данни за поставяне на карти, съхранени в VU
VuITSConsentRecordArray	
VuPowerSupplyInterruptionRecordArray	
SignatureRecordArray	ECC подпис на всички предходни данни

2.3. **Съхранение на файлове върху ESM**

DDP_034 Ако дадена сесия за изтегляне на данни е включвала прехвърляне на данни от VU, IDE съхранява в един-единствен физически файл всички данни, получени от VU по време на тази сесия за изтегляне на данни в рамките на съобщенията Positive Response Transfer Data. Съхранените данни изключват заглавните части на съобщенията, броячите на подсъобщения, празните подсъобщения и контролните суми, но включват SID и TREP (на първото подсъобщение, при положение че има няколко подсъобщения).

3. ПРОТОКОЛ ЗА ИЗТЕГЛЯНЕ НА ДАННИ ОТ ТАХОГРАФСКИТЕ КАРТИ

3.1. **Обхват**

В настоящия параграф е описано директното изтегляне на данни от тахографска карта към IDE. IDE не е част от сигурната среда; ето защо не се извършва удостоверяване между картата и IDE.

3.2. **Определения**

Сесия за изтегляне на данни: всеки път, когато се извършва изтегляне на данни от ICC. Тази сесия обхваща цялата процедура от инициализацията на ICC чрез IFD до дезактивирането на ICC (изваждане на картата или следващо инициализиране).

Подписан файл за данни: файл от ICC. Този файл се прехвърля като обикновен текст към IFD. Върху ICC файлът се хешира и подписва, а подписът се прехвърля към IFD.

3.3. **Изтегляне на данни от карта**

DDP_035 Изтеглянето на данни от тахографска карта съдържа следните операции:

— изтегляне на общата информация на картата в EFs ICC и IC. Тази информация е незадължителна и не е защитена с електронен подпис;

— изтегляне на EFs Card_Certificate (или CardSignCertificate) и CA_Certificate. Тази информация не е защитена с електронен подпис.

Тези файлове трябва задължително да се изтеглят за всяка сесия за изтегляне на данни;

— изтегляне на другите данни от приложение EFs (в рамките на Tachograph DF и Tachograph_G2 DF, ако е уместно) освен EF Card_Download. Тази информация е защитена с електронен подпис;

— задължително е да се изтеглят поне EFs Application_Identification и ID за всяка сесия за изтегляне на данни.

— Когато се извършва изтегляне на данни от карта на водач, е необходимо също да се изтеглят следните EFs:

- Events_Data,
- Faults_Data,
- Driver_Activity_Data,
- Vehicles_Used,
- Places,
- GNSS_Places (if relevant),
- Control_Activity_Data,
- Specific_Conditions;

— когато се извършва изтегляне на данни от карта на водач, трябва да се актуализира датата на LastCardDownload в EF Card_Download;

— когато се извършва изтегляне на данни от карта за монтаж и настройки, е необходимо да се инициализира броячът за калибриране в EF Card_Download;

— когато се изтеглят данни от карта за монтаж и настройки, не трябва да се изтеглят данните от EF Sensor_Installation_Data.

3.3.1 *Последователност при инициализиране*

DDP_036 IDE трябва да започне последователността, както следва:

Карта	Посока	IDE/IFD	Значение/Забележки
	⇦	Инициализация на хардуера	
ATR	⇨		

Възможно е да се използва PPS, за да премине към по-висока скорост за предаване на данни, при условие че ICC я поддържа.

3.3.2 *Последователност за неподписани файлове с данни*

DDP_037 Последователността за изтегляне на данни от EFs ICC, IC, Card_Certificate (или CardSignCertificate) и CA_Certificate е, както следва:

Карта	Посока	IDE/IFD	Значение/Забележки
	⇦	**Select File**	Изберете идентификаторите на файлове
OK	⇨		
	⇦	**Read Binary**	Ако файлът съдържа повече данни от капацитета на буферната памет на четящото устройство или картата, командата трябва да се повтори, докато целият файл се прочете.
Данни от файла OK	⇨	Съхранение на данните върху ESM	Съгласно **3.4** Data storage format

Забележка 1: преди да се избере Card_Certificate (или CardSignCertificate) EF, трябва да се избере тахографското приложение (избор от страна на AID).

Забележка 2: изборът и прочитането на файл може да се извършат и в една стъпка, като се използва командата Read Binary с кратък EF идентификатор.

3.3.3 *Последователност за подписани файлове с данни*

DDP_038 Трябва да се използва следната последователност за всеки от следните файлове, от които трябва да се изтеглят данните с техния подпис:

Карта	Посока	IDE/IFD	Значение/Забележки
	⇦	**Select File**	
OK	⇨		
	⇦	**Perform Hash of File**	Позволява да се изчисли хеш-стойността по отношение на съдържанието на избрания файл, като се използва хеш-алгоритъмът, посочен в допълнение 11. Това не е команда ISO.
Изчислява се Hash of File и временно се съхранява хеш-стойността			
OK	⇨		
	⇦	**Read Binary**	Ако файлът съдържа повече данни от капацитета на буферната памет на четящото устройство или картата, командата трябва да се повтори, докато целият файл се прочете.
Данни от файла **OK**	⇨	Получените данни се съхраняват върху ESM	Съгласно **3.4** Data storage format
	⇦	**PSO: Compute Digital Signature**	
Изпълнение на операция за сигурност „Compute Digital Signature“, като се използва временно съхранената хеш-стойност			
Подпис **OK**	⇨	Добавяне на данни към тези, които са съхранени преди това върху ESM	Съгласно **3.4** Data storage format

Забележка: изборът и прочитането на файл могат да се извършат и в една стъпка, като се използва командата Read Binary с кратък EF идентификатор. В този случай може да се избере и прочете EF, преди да се приложи командата Perform Hash of File.

3.3.4 *Последователност за инициализиране на брояча за калибриране*

DDP_039 Последователността на инициализиране на брояча `NoOfCalibrationsSinceDownload` в EF `Card_Download` в карта за монтаж и настройки е следната:

Карта	Посока	IDE/IFD	Значение/Забележки
	⇦	**Select File** EF Card_Download	Изберете идентификаторите на файлове
OK	⇨		

Карта	Посока	IDE/IFD	Значение/Забележки
	⇦	**Update Binary** NoOfCalibrationsSince-Download = '00 00'	
Инициализира броя на изтеглянията на данни от картата			
OK	⇨		

Забележка: изборът и актуализацията на файл могат да се извършат и в една стъпка, като се използва командата Update Binary с кратък EF идентификатор.

3.4. Формат за съхранение на данните

3.4.1 *Въведение*

DDP_040 Изтеглените данни трябва да се съхраняват при следните условия:

— съхранението на данните трябва се извършва прозрачно. Това означава, че при съхранението трябва да се запазят редът на байтовете и редът на битовете в рамките на байта, които се прехвърлят от картата;

— всички файлове на картата, от която са изтеглени данни в рамките на една сесия за изтегляне на данни, се съхраняват в един файл на ESM.

3.4.2 *Формат на файловете*

DDP_041 Форматът на файловете представлява съединяване на няколко обекта TLV.

DDP_042 Тагът за EF трябва да е FID плюс допълнението„00“.

DDP_043 Тагът на EF подпис трябва да е FID на файла плюс допълнението„01“.

DDP_044 Дължината е стойност от два байта. Стойността определя броя на байтовете в полето за стойност. Стойността„FF FF“ в полето за дължина се запазва за по-нататъшна употреба.

DDP_045 Когато не е изтеглен файл, не се запазва никаква информация за файла (без таг и без дължина нула).

DDP_046 Всеки подпис трябва да бъде съхранен под формата на обект TLV веднага след обекта TLV, който съдържа данните на файла.

Определение	Значение	Дължина
FID (2 байта) || „00“	Таг за EF (FID)	3 байта
FID (2 байта) || „01“	Таг за подпис EF(FID)	3 байта
xx xx	Дължина на полето за стойността	2 байта

Пример за данни в изтеглен файл върху ESM:

Таг	Дължина	Стойност
00 02 00	00 11	Данни от EF ICC
C1 00 00	00 C2	Данни от EF Card_Certificate
		...
05 05 00	0A 2E	Данни от EF Vehicles_Used
05 05 01	00 80	Подпис на EF Vehicles_Used

4. ИЗТЕГЛЯНЕ НА ДАННИ ОТ ТАХОГРАФСКА КАРТА ЧРЕЗ БОРДОВО УСТРОЙСТВО

DDP_047 VU трябва да позволява изтеглянето на съдържанието на карта на водач, поставена в свързано IDE.

DDP_048 IDE трябва да изпрати съобщение „Transfer Data Request Card Download“ до VU, за да се започне този режим (вж. 2.2.2.9).

DDP_049 Тогава VU трябва да извърши цялостното изтегляне на данни от картата, файл по файл, в съответствие с протокола за изтегляне на данни от карта, определен в параграф 3, както и да изпрати към IDE всички данни, които са получени от картата в съответния файлов формат TLV (вж. 3.4.2) и са капсулирани в съобщение „Positive Response Transfer Data“.

DDP_050 IDE трябва да извлече данните от картата от съобщението „Positive Response Transfer Data“ (като премахне всички заглавни части, SID, TREP, броячи на подсъобщения и контролни суми) и да ги запише в един физически файл, както е описано в параграф 2.3.

DDP_051 След това, в зависимост от случая, VU трябва да извърши актуализиране на файла `Control_Activity_Data` или `Card_Download` на картата на водач.

Допълнение 8

ПРОТОКОЛ ЗА КАЛИБРИРАНЕ

СЪДЪРЖАНИЕ

1. ВЪВЕДЕНИЕ

В това допълнение са разгледани начините на обмен на данни между бордово устройство и изпитвателно оборудване посредством линията K, която представлява част от интерфейса за калибриране, описан в допълнение 6. В настоящото допълнение е описан също контролът на линията за входни/изходни сигнали на съединителя за калибриране.

Установяването на връзките по линия K е дадено в раздел 4 „Communication Services“.

В настоящото допълнение е използвана концепцията за „диагностични сесии“ за определяне на обхвата на контрола на линията K при различни условия. Сесията по подразбиране е „StandardDiagnosticSession“, при която е възможно всички данни да се прочетат от бордово устройство, но никакви данни не могат да бъдат записани върху него.

Избирането на диагностична сесия е описано в раздел 5 „Management Services“.

Настоящото допълнение е от значение за двете поколения бордови устройства и карти за монтаж и настройки в съответствие с изискванията към оперативната съвместимост по този регламент.

CPR_001 „ECUProgrammingSession“ дава възможност да се въведат данните в бордовото устройство. Освен това, когато се въвеждат данни за калибриране, бордовото устройство трябва да е в режим на работа „КАЛИБРИРАНЕ“.

Трансферът на данни по линията K е описан в раздел 6 „Data Transmission Services“. Форматите на прехвърлените данни са дадени подробно в раздел 8 „dataRecords formats“.

CPR_002 „ECUAdjustmentSession“ дава възможност да се избере режима на работа за линията за входни/изходни сигнали за калибриране чрез интерфейса на линията K. Контролът на линията за входни/изходни сигнали за калибриране е описан в раздел 7 „Control of Test Pulses — Input/Output Control functional unit“.

CPR_003 В настоящия документ адресът на изпитвателното оборудване се посочва като „tt“. Въпреки че е възможно да има предпочитани адреси за изпитвателното оборудване, бордовото устройство трябва да отговаря правилно на всеки адрес на изпитвателно оборудване. Физическият адрес на бордовото устройство е 0xEE.

2. ПОНЯТИЯ, ОПРЕДЕЛЕНИЯ И СПРАВОЧНИ МАТЕРИАЛИ

Протоколите, съобщенията и кодовете за грешка се основават главно на проект на стандарт ISO 14229-1 (Пътни превозни средства. Системи за диагностика. Част 1: услуги за диагностика, версия 6 от 22 февруари 2001 г.).

Кодирането на байтове и други шестнадесетични стойности се използват за идентификаторите на услуги, служебните заявки и отговори и стандартните параметри.

„Изпитвателно оборудване“ е оборудването, което се използва за въвеждане на данни за програмиране/калибриране в бордовото устройство.

Понятията „клиент“ и „сървър“ се отнасят съответно за изпитвателното оборудване и бордовото устройство.

Понятието UCE е „електронен блок за управление“ и се отнася за бордовото устройство.

Справочни материали:

ISO 14230-2: Пътни превозни средства. Системи за диагностика. Протокол „Keyword 2000“. Част 2: канален слой).

Първо издание: 1999 г.

Превозни средства — Диагностика.

3. ПРЕГЛЕД НА УСЛУГИТЕ

3.1. **Налични услуги**

В следващата таблица са представени услугите, които са налични в тахографа и са определени в настоящия документ.

CPR_004 В тази таблица е посочено кои са услугите на разположение по време на активна диагностична сесия.

— В **първата колона** са дадени наличните услуги.

— Във **втората колона** е посочен номерът на раздела в настоящото допълнение, където са представени допълнителни данни за услугата.

— В **третата колона** са указани стойностите за идентификаторите на услугите за съобщенията за заявка.

— В **четвъртата колона** са дадени услугите на **„StandardDiagnosticSession“ (SD)**, които трябва да се изпълняват във всяко бордово устройство.

— В **петата колона** са уточнени услугите на **„ECUAdjustmentSession“ (ECUAS)**, които трябва да се изпълняват, за да се даде възможност за контрол на линията за входни/изходни сигнали от предния панел на съединителя за калибриране на бордовото устройство.

— В **шестата колона** са посочени услугите на **„ECUProgrammingSession“ (ECUPS)**, които трябва да се изпълняват, за да се даде възможност за програмиране на параметрите в бордовото устройство.

Таблица 1

Обобщаваща таблица за стойностите на идентификаторите на услуги

			Диагностични сесии		
Наименование на диагностичната услуга	Раздел №	Стойности за съобщенията за заявка за SId	SD	ECUAS	ECUPS
StartCommunication	4.1	81	■	■	■
StopCommunication	4.2	82	■		
TesterPresent	4.3	3E	■	■	■
StartDiagnosticSession	5.1	10	■	■	■
SecurityAccess	5.2	27	■	■	■
ReadDataByIdentifier	6.1	22	■	■	■
WriteDataByIdentifier	6.2	2E			■
InputOutputControlByIdentifier	7.1	2F		■	

■ Този символ указва, че услугата е задължителна в тази диагностична сесия.

Няма символ, който да посочва, че съответната услуга не е разрешена в тази диагностична сесия.

3.2. **Кодове за отговор**

Кодовете за отговор са определени за всяка услуга.

4. СЪОБЩИТЕЛНИ УСЛУГИ

Някои услуги са необходими за установяване и поддържане на връзката. Те не се появяват в приложния слой. В следващата таблица са посочени наличните услуги:

Таблица 2

Съобщителни услуги

Наименование на услугата	Описание
StartCommunication	Клиентът заявява започване на съобщителна сесия със сървъра(ите).
StopCommunication	Клиентът заявява прекъсване на текущата съобщителна сесия.
TesterPresent	Клиентът указва на сървъра, че е все още на линия.

CPR_005 Услугата StartCommunication се използва за започване на връзка. Изпълнението на всяка услуга предполага установяване на връзка и избор на параметри на връзката, подходящи за желания режим.

4.1. **Услуга StartCommunication**

CPR_006 При получаване на примитив за указване StartCommunication бордовото устройство проверява дали заявената съобщителна връзка може да се осъществи при дадените условия. Валидните условия за осъществяване на съобщителна връзка са описани в документ ISO 14230-2.

CPR_007 След това бордовото устройство трябва да изпълни всички необходими действия за осъществяване на съобщителната връзка и да изпрати примитив за отговор StartCommunication с избраните параметри за положителен отговор.

CPR_008 Ако едно вече инициализирано бордово устройство (и влязло в диагностична сесия) получи нова заявка за StartCommunication (например поради повторно стартиране при грешка в изпитвателното оборудване), тази заявка трябва да бъде приета и устройството да бъде реинициализирано.

CPR_009 Ако по една или друга причина осъществяването на съобщителната връзка се окаже невъзможно, бордовото устройство трябва да продължи да работи по същия начин, както непосредствено преди опита за осъществяване на съобщителна връзка.

CPR_010 Съобщението за заявка за StartCommunication трябва да се адресира физически.

CPR_011 Инициализирането на бордовото устройство за услугите се осъществява чрез „бързо инициализиране“:

— има време на активност/неактивност преди всяко действие;

— след това изпитвателното оборудване изпраща конфигурация за инициализиране;

— цялата информация за установяване на връзка се съдържа в отговора на бордовото устройство.

CPR_012 След приключване на инициализирането:

— стойностите, които са определени за всички съобщителни параметри, са описани в таблица 4 в зависимост от ключовите байтове;

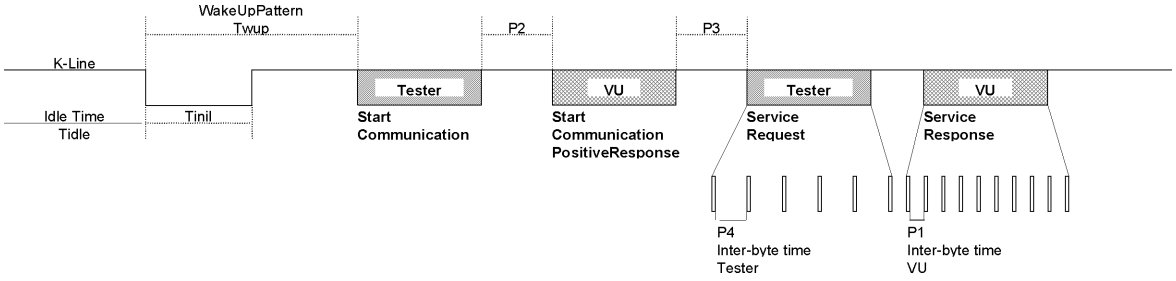
— бордовото устройство изчаква първата заявка от изпитвателното оборудване;

— бордовото устройство работи в диагностичен режим по подразбиране, тоест в StandardDiagnostic-Session;

— линията за входни/изходни сигнали за калибриране се намира в състояние по подразбиране, тоест е дезактивирана.

CPR_014 Скоростта за предаване на данни по линията K трябва да е 10 400 бода.

CPR_016 Бързата инициализация се задейства от изпитвателното оборудване, изпращащо сигнал за активиране (Wup) по линията K след период на неактивност на линията K, последван от времеви период Tinil. Изпитвателното оборудване изпраща първия бит на услугата StartCommunicationService след времеви период Twup, последван от първия заден фронт на импулса.



CPR_017 Стойностите за синхронизация за бързата инициализация и връзките по принцип са подробно описани в следващите таблици. Що се отнася до времето на неактивност, има различни възможности:

— Първо предаване на данни след включване под напрежение — Tidle = 300 ms.

— След приключване на услугата StopCommunication — Tidle = 3 min.

— След прекъсване на връзката поради превишаване на определеното време P3 max — Tidle = 0.

Таблица 3

Стойности за синхронизация, определени за бързата инициализация

Параметър		Минимална стойност	Максимална стойност
Tinil	25 ± 1 ms	24 ms	26 ms
Twup	50 ± 1 ms	49 ms	51 ms

Таблица 4

Стойности за синхронизация за връзките

Синхронизация Параметър	Описание на параметъра	Допустими минимални стойности (ms)	Допустими максимални стойности (ms)
		Минимални	Максимални
P1	Междубайтово време за отговора на бордовото устройство	0	20
P2	Време между една заявка от изпитвателното оборудване и един или два отговора от бордовото устройство	25	250
P3	Време между края на отговорите на бордовото устройство и началото на нова заявка, изпратена от изпитвателното оборудване	55	5 000
P4	Междубайтово време за заявка, изпратена от изпитвателното оборудване	5	20

CPR_018 Форматът на съобщенията за бързата инициализация е подробно описан в следващите таблици. (ЗАБЕЛЕЖКА: Hex means hexadecimal)

Таблица 5

Съобщение за заявка за StartCommunication

Байт #	Наименование на параметъра	Стойност hex.	Мнемоничен код
#1	Байт за структура — физическо адресиране	81	FMT
#2	Целеви байт за адреса	EE	TGT
#3	Изходен байт за адреса	tt	SRC
#4	**Идентификатор на заявка за услугата StartCommunication**	**81**	**SCR**
#5	Контролна сума	00-FF	CS

Таблица 6

Съобщение за положителен отговор за StartCommunication

Байт #	Наименование на параметъра	Стойност hex.	Мнемоничен код
#1	Байт за структура — физическо адресиране	80	FMT
#2	Целеви байт за адреса	tt	TGT
#3	Изходен байт за адреса	EE	SRC
#4	Допълнителен байт за дължина	03	LEN
#5	**Идентификатор на положителен отговор за услугата StartCommunication**	**C1**	**SCRPR**
#6	Ключов байт 1	EA	KB1
#7	Ключов байт 2	8F	KB2
#8	Контролна сума	00-FF	CS

CPR_019 Няма отрицателен отговор на съобщението за заявка за StartCommunication. Поради липса на съобщение за положителен отговор за изпращане, бордовото устройство не се инициализира, никакви данни не се предават и то остава в режим на нормална работа.

4.2. **Услуга StopCommunication**

4.2.1 *Описание на съобщенията*

Целта на тази услуга е да се прекрати съобщителната сесия.

CPR_020 При получаване на примитив за указване StopCommunication бордовото устройство трябва да провери дали актуалните условия позволяват да се прекрати тази връзка. В такъв случай бордовото устройство трябва да извърши всички необходими операции, за да прекрати връзката.

CPR_021 Ако е възможно прекратяване на връзката, бордовото устройство трябва да изпрати примитив за отговор StopCommunication с избраните параметри за положителен отговор, преди да прекрати връзката.

CPR_022 Ако по една или друга причина се окаже невъзможно прекратяването на връзката, бордовото устройство трябва да изпрати примитив за отговор StopCommunication с избрания параметър за отрицателен отговор.

CPR_023 Ако бордовото устройство установи надвишаване на времетраенето P3max, връзката се прекратява без примитив за отговор.

4.2.2 *Формат на съобщенията*

CPR_024 Форматите на съобщенията за примитивите на StopCommunication са подробно описани в следващите таблици.

Таблица 7

Съобщение за заявка за StopCommunication

Байт #	Наименование на параметъра	Стойност hex.	Мнемоничен код
#1	Байт за структура — физическо адресиране	80	FMT
#2	Целеви байт за адреса	EE	TGT
#3	Изходен байт за адреса	tt	SRC
#4	Допълнителен байт за дължина	01	LEN
#5	**Идентификатор на заявка за услугата StopCommunication**	**82**	**SPR**
#6	Контролна сума	00-FF	CS

Таблица 8

Съобщение за положителен отговор за StopCommunication

Байт #	Наименование на параметъра	Стойност hex.	Мнемоничен код
#1	Байт за структура — физическо адресиране	80	FMT
#2	Целеви байт за адреса	tt	TGT
#3	Изходен байт за адреса	EE	SRC
#4	Допълнителен байт за дължина	01	LEN
#5	**Идентификатор на положителен отговор за услугата StopCommunication**	**C2**	**SPRPR**
#6	Контролна сума	00-FF	CS

Таблица 9

Съобщение за отрицателен отговор за StopCommunication

Байт #	Наименование на параметъра	Шестнайсетична стойност	Мнемоничен код
#1	Байт за структура — физическо адресиране	80	FMT
#2	Целеви байт за адреса	tt	TGT
#3	Изходен байт за адреса	EE	SRC
#4	Допълнителен байт за дължина	03	LEN
#5	**Идентификатор на отрицателен отговор за услугата**	**7F**	**NR**
#6	Идентификация на заявка за услугата StopCommunication	82	SPR
#7	responseCode = generalReject	10	RC_GR
#8	Контролна сума	00-FF	CS

4.2.3 *Определяне на параметрите*

Тази услуга не налага определяне на параметри.

4.3. **Услуга TesterPresent**

4.3.1 *Описание на съобщенията*

Услугата TesterPresent се използва от изпитвателното оборудване, за да укаже на сървъра, че все още е на разположение, с цел да се попречи на автоматичното връщане на сървъра към режим на нормална работа и да се избегне евентуалното прекъсване на връзката. Изпращана периодично, тази услуга поддържа активна диагностичната сесия/връзката, като нулира брояча P3 при всяка заявка за тази услуга.

4.3.2 *Формат на съобщенията*

CPR_079 Форматите на съобщенията за примитивите за TesterPresent са подробно описани в следващите таблици.

Таблица 10

Съобщение за заявка за TesterPresent

Байт #	Наименование на параметъра	Шестнайсетична стойност	Мнемоничен код
#1	Байт за структура — физическо адресиране	80	FMT
#2	Целеви байт за адреса	EE	TGT
#3	Изходен байт за адреса	tt	SRC
#4	Допълнителен байт за дължина	02	LEN
#5	**Идентификатор на заявка за услугата TesterPresent**	**3E**	**TP**

Байт #	Наименование на параметъра	Шестнайсетична стойност	Мнемоничен код
#6	Подфункция = responseRequired = [да	01	RESPREQ_Y
	не]	02	RESPREQ_NO
#7	Контролна сума	00-FF	CS

CPR_080 Ако за параметъра responseRequired е зададено„да“, сървърът ще отговори с последващо съобщение за положителен отговор. Ако е зададено „не“, сървърът не изпраща отговор.

Таблица 11

Съобщение за положителен отговор за TesterPresent

Байт #	Наименование на параметъра	Шестнайсетична стойност.	Мнемоничен код
#1	Байт за структура — физическо адресиране	80	FMT
#2	Целеви байт за адреса	tt	TGT
#3	Изходен байт за адреса	EE	SRC
#4	Допълнителен байт за дължина	01	LEN
#5	**Идентификатор на положителен отговор за услугата TesterPresent**	**7E**	**TPPR**
#6	Контролна сума	00-FF	CS

CPR_081 Услугата трябва да поддържа следните кодове за отрицателен отговор:

Таблица 12

Съобщение за отрицателен отговор за TesterPresent

Байт #	Наименование на параметъра	Шестнайсетична стойност	Мнемоничен код
#1	Байт за структура — физическо адресиране	80	FMT
#2	Целеви байт за адреса	tt	TGT
#3	Изходен байт за адреса	EE	SRC
#4	Допълнителен байт за дължина	03	LEN
#5	**Идентификатор на отрицателен отговор за услугата**	**7F**	**NR**
#6	Идентификация на заявка за услугата TesterPresent	3E	TP

Байт #	Наименование на параметъра		Шестнайсетична стойност	Мнемоничен код
#7	responseCode =	[SubFunctionNotSupported-InvalidFormat	12	RC_SFNS_IF
		incorrectMessageLength]	13	RC_IML
#8	Контролна сума		00-FF	CS

5. УСЛУГИ ЗА УПРАВЛЕНИЕ

В следващата таблица са посочени наличните услуги:

Таблица 13

Услуги за управление

Наименование на услугата	Описание
StartDiagnosticSession	Клиентът заявява започване на диагностична сесия с бордовото устройство.
SecurityAccess	Клиентът заявява достъп до функции, които са запазени за оторизирани потребители.

5.1. **Услуга StartDiagnosticSession**

5.1.1 *Описание на съобщенията*

CPR_025 Услугата StartDiagnosticSession позволява активиране на различни диагностични сесии в сървъра. Диагностичната сесия дава възможност за специфичен набор от услуги в съответствие с таблица 17. Сесията може да позволи извършването на специфични услуги на производителя на превозното средство, които не са част от настоящия документ. Правилата за тяхното извършване трябва да отговарят на следните изисквания:

— винаги има само една активна диагностична сесия в бордовото устройство;

— бордовото устройство винаги започва StandardDiagnosticSession, когато е включен под напрежение. Ако няма започната друга диагностична сесия, StandardDiagnosticSession остава активна, докато бордовото устройство е включено към захранване;

— ако една вече започната диагностична сесия е заявена от изпитвателното оборудване, бордовото устройство изпраща съобщение за положителен отговор;

— когато изпитвателното оборудване заяви нова диагностична сесия, бордовото устройство първо изпраща съобщение за положителен отговор за StartDiagnosticSession, преди да се започне новата сесия в бордовото устройство. Ако бордовото устройство не може да започне заявената нова диагностична сесия, той изпраща съобщение за отрицателен отговор на StartDiagnosticSession и текущата сесия продължава.

CPR_026 Диагностична сесия започва само ако е била установена връзка между клиента и бордовото устройство.

CPR_027 Параметрите за синхронизация, определени в таблица 4, се активират след успешно изпълнение на StartDiagnosticSession с параметъра diagnosticSession, за който е зададено „StandardDiagnosticSession“ в съобщението за заявка, ако преди това е била активна друга диагностична сесия.

5.1.2 *Формат на съобщенията*

CPR_028 Форматите на съобщенията за примитивите StartDiagnosticSession са подробно описани в следващите таблици.

Таблица 14

Съобщение за заявка за StartDiagnosticSession

Байт #	Наименование на параметъра	Шестнайсетична стойност	Мнемоничен код
#1	Байт за структура — физическо адресиране	80	FMT
#2	Целеви байт за адреса	EE	TGT
#3	Изходен байт за адреса	tt	SRC
#4	Допълнителен байт за дължина	02	LEN
#5	**Идентификатор на заявка за услугата Start-DiagnosticSession**	**10**	**STDS**
#6	diagnosticSession = [една стойност от таблица 17]	xx	DS_…
#7	Контролна сума	00-FF	CS

Таблица 15

Съобщение за положителен отговор за StartDiagnosticSession

Байт #	Наименование на параметъра	Шестнайсетична стойност	Мнемоничен код
#1	Байт за структура — физическо адресиране	80	FMT
#2	Целеви байт за адреса	tt	TGT
#3	Байт за изходен адрес	EE	SRC
#4	Допълнителен байт за дължина	02	LEN
#5	**Идентификатор на положителен отговор за услугата StartDiagnosticSession**	**50**	**STDSPR**
#6	diagnosticSession = [същата стойност като байт #6 таблица 14]	xx	DS_…
#7	Контролна сума	00-FF	CS

Таблица 16

Съобщение за отрицателен отговор за StartDiagnosticSession

Байт #	Наименование на параметъра	Шестнайсетична стойност	Мнемоничен код
#1	Байт за структура — физическо адресиране	80	FMT
#2	Байт за целеви адрес	tt	TGT

Байт #	Наименование на параметъра	Шестнайсетична стойност	Мнемоничен код
#3	Байт за изходен адрес	EE	SRC
#4	Допълнителен байт за дължина	03	LEN
#5	**Идентификатор на отрицателен отговор за услугата**	**7F**	**NR**
#6	Идентификатор на заявка за услугата StartDiagnosticSession	10	STDS
#7	ResponseCode = [subFunctionNotSupported (а)	12	RC_SFNS
	incorrectMessageLength (б)	13	RC_IML
	conditionsNotCorrect (в)	22	RC_CNC
#8	Контролна сума	00-FF	CS

(а) Въведената стойност в байт #6 на съобщението за заявка не се поддържа, тоест не е в таблица 17.
(б) Дължината на съобщението е грешна.
(в) Критериите за заявка за StartDiagnosticSession не са изпълнени.

5.1.3 *Определяне на параметрите*

CPR_029 Параметърът ***diagnosticSession (DS_)*** се използва от услугата StartDiagnosticSession за избор на специален режим на сървъра(ите). Следващите диагностични сесии са посочени в настоящия документ:

Таблица 17

Определяне на стойностите на diagnosticSession

Hex	Описание	Мнемоничен код
81	**StandardDiagnosticSession** Тази диагностична сесия дава възможност за всички услуги, посочени в **таблица 1, колона 4, „SD“**. Тези услуги позволяват четенето на данни от сървър (бордово устройство). Тази диагностична сесия е активна след успешна инициализация между клиент (изпитвателно оборудване) и сървър (бордово устройство). Възможно е тази диагностична сесия да бъде заменена от други други диагностични сесии, посочени в този раздел.	**SD**
85	**ECUProgrammingSession** Тази диагностична сесия дава възможност за всички услуги, посочени в **таблица 1, колона 6, „ECUPS“**. Тези услуги поддържат програмирането на паметта на сървър (бордово устройство). Възможно е тази сесия да бъде заменена от други други диагностични сесии, посочени в този раздел.	**ECUPS**
87	**ECUAdjustmentSession** Тази диагностична сесия дава възможност за всички услуги, посочени в **таблица 1, колона 5, „ECUAS“**. Тези услуги поддържат контрола на входните/изходните данни на сървър (бордово устройство). Възможно е тази диагностична сесия да бъде заменена от други други диагностични сесии, посочени в този раздел.	**ECUAS**

5.2. **Услуга SecurityAccess**

Записването на данните за калибрирането не е възможно, освен ако бордовото устройство работи в режим КАЛИБРИРАНЕ. Освен вкарването на валидна карта за монтаж и настройки в бордовото устройство е необходимо да се въведе съответният PIN в устройството, преди да се получи достъп до режима КАЛИБРИРАНЕ.

Когато бордовото устройство е в режим КАЛИБРИРАНЕ или КОНТРОЛ, достъпът до входно-изходната линия за калибриране е също възможен.

Услугата SecurityAccess позволява въвеждане на PIN и посочване на изпитвателното оборудване дали бордовото устройство работи в режим КАЛИБРИРАНЕ.

Допустимо е да се използват други методи за въвеждане на PIN.

5.2.1 *Описание на съобщенията*

Услугата SecurityAccess се състои от съобщение „requestSeed“ на SecurityAccess, евентуално последвано от съобщението „sendKey“ на SecurityAccess. Услугата SecurityAccess трябва да се изпълни след услугата StartDiagnosticSession.

CPR_033 Изпитвателното оборудване трябва да използва съобщение „requestSeed“ на SecurityAccess, за да провери дали бордовото устройство е в готовност да приеме PIN.

CPR_034 Ако бордовото устройство е вече в режим КАЛИБРИРАНЕ, то трябва да отговори на заявката чрез изпращане на инициализация с начална стойност от 0x0000, като използва положителен отговор на услугата SecurityAccess.

CPR_035 Ако бордовото устройство е готово да приеме PIN за проверка чрез карта за монтаж и настройки, то трябва да отговори на заявката чрез изпращане на инициализация с начална стойност, по-голяма от 0x0000, като използва положителен отговор на услугата SecurityAccess.

CPR_036 Ако бордовото устройство не е готово да приеме PIN от изпитвателното оборудване, защото вкараната карта за монтаж и настройки не е валидна или защото не е вкарана карта, или защото бордовото устройство изчаква PIN по друг начин, то трябва да отговори на заявката с отрицателен отговор, придружен от код за отговор conditionsNotCorrectOrRequestSequenceError.

CPR_037 Тогава евентуално изпитвателното оборудване трябва да използва съобщение „sendKey“ на SecurityAccess, за да предаде PIN на бордовото устройство. За управление на времето, необходимо за извършване на процеса по удостоверяване на картата, бордовото устройство трябва да използва кода за отрицателен отговор requestCorrectlyReceived-ResponsePending, за да удължи времето за отговор. Максималното време за отговор не трябва обаче да надхвърля 5 минути. След като бъде изпълнена заявената услуга, бордовото устройство изпраща съобщение за положителен или отрицателен отговор с код за отговор, който е различен от кода по-горе. Кодът за отрицателен отговор requestCorrectlyReceived-ResponsePending може да се повторя от бордовото устройство, докато заявената услуга бъде изпълнена, а съобщението за краен отговор — изпратено.

CPR_038 Бордовото устройство трябва да отговори на тази заявка, като използва положителен отговор на SecurityAccess само когато работи в режим КАЛИБРИРАНЕ.

CPR_039 В следващите случаи бордовото устройство трябва да отговори на тази заявка с отрицателен отговор, придружен от един от следните кодове за отговор:

— не се поддържа subFunctionNot: невалиден формат за параметъра subfunction (accessType);

— conditionsNotCorrectOrRequestSequenceError: бордовото устройство не е готово за приемане на PIN;

— invalidKey: невалиден PIN и броят на опитите за проверка на PIN не е надхвърлен;

— exceededNumberOfAttempts: невалиден PIN и броят на опитите за проверка на PIN е надхвърлен;

— generalReject: правилен PIN, но неуспешно взаимно удостоверяване с картата за монтаж и настройки.

5.2.2 *Формат на съобщенията — SecurityAccess — requestSeed*

CPR_040 Форматите на съобщенията за примитивите на „requestSeed“ на SecurityAccess са подробно описани в следващите таблици.

Таблица 18

Заявка за SecurityAccess — съобщение за requestSeed

Байт #	Наименование на параметъра	Шестнайсетична стойност	Мнемоничен код
#1	Байт за структура — физическо адресиране	80	FMT
#2	Байт за целевия адрес	EE	TGT
#3	Байт за изходен адрес	tt	SRC
#4	Допълнителен байт за дължина	02	LEN
#5	**Идентификатор на заявка за услугата SecurityAccess**	**27**	**SA**
#6	accessType — requestSeed	7D	AT_RSD
#7	Контролна сума	00-FF	CS

Таблица 19

SecurityAccess — съобщение за положителен отговор за requestSeed

Байт #	Наименование на параметъра	Шестнайсетична стойност	Мнемоничен код
#1	Байт за структура — физическо адресиране	80	FMT
#2	Байт за целевия адрес	tt	TGT
#3	Байт за изходния адрес	EE	SRC
#4	Допълнителен байт за дължина	04	LEN
#5	**Идентификатор на положителен отговор за услугата SecurityAccess**	**67**	**SAPR**
#6	accessType — requestSeed	7D	AT_RSD
#7	Инициализация от високо ниво	00-FF	SEEDH
#8	Инициализация от ниско ниво	00-FF	SEEDL
#9	Контролна сума	00-FF	CS

Таблица 20

Съобщение за отрицателен отговор за SecurityAccess

Байт #	Наименование на параметъра	Шестнайсетична стойност	Мнемоничен код
#1	Байт за структура — физическо адресиране	80	FMT
#2	Байт за целевия адрес	tt	TGT
#3	Байт за изходния адрес	EE	SRC

Байт #	Наименование на параметъра	Шестнайсетична стойност	Мнемоничен код
#4	Допълнителен байт за дължина	03	LEN
#5	**Идентификатор на отрицателен отговор за услугата**	**7F**	**NR**
#6	Идентификатор на заявка за услугата SecurityAccess	27	SA
#7	responseCode = [conditionsNotCorrectOrRequestSequenceError incorrectMessageLength]	22 13	RC_CNC RC_IML
#8	Контролна сума	00-FF	CS

5.2.3 *Формат на съобщенията — SecurityAccess — sendKey*

CPR_041 Форматите на съобщенията за примитивите на „sendKey“ на SecurityAccess са подробно описани в следващите таблици.

Таблица 21

Заявка за SecurityAccess — съобщение за sendKey

Байт #	Наименование на параметъра	Шестнайсетична стойност	Мнемоничен код
#1	Байт за структура — физическо адресиране	80	FMT
#2	Байт за целевия адрес	EE	TGT
#3	Байт за изходния адрес	tt	SRC
#4	Допълнителен байт за дължина	m+2	LEN
#5	**Идентификатор на заявка за услугата SecurityAccess**	**27**	**SA**
#6	accessType — sendKey	7E	AT_SK
#7 до #m +6	Key #1 (High) … Key #m (ниска, стойността на m трябва да бъде в интервала между 4 и 8)	xx … xx	KEY
#m+7	Контролна сума	00-FF	CS

Таблица 22

SecurityAccess — съобщение за положителен отговор за sendKey

Байт #	Наименование на параметъра	Шестнайсетична стойност	Мнемоничен код
#1	Байт за структура — физическо адресиране	80	FMT
#2	Байт за целевия адрес	tt	TGT
#3	Байт за изходния адрес	EE	SRC

Байт #	Наименование на параметъра	Шестнайсетична стойност	Мнемоничен код
#4	Допълнителен байт за дължина	02	LEN
#5	**Идентификатор на положителен отговор за услугата SecurityAccess**	**67**	**SAPR**
#6	accessType — sendKey	7E	AT_SK
#7	Контролна сума	00-FF	CS

Таблица 23

Съобщение за отрицателен отговор за SecurityAccess

Байт #	Наименование на параметъра		Шестнайсетична стойност	Мнемоничен код
#1	Байт за структура — физическо адресиране		80	FMT
#2	Байт за целевия адрес		tt	TGT
#3	Байт за изходния адрес		EE	SRC
#4	Допълнителен байт за дължина		03	LEN
#5	**Идентификатор на отрицателен отговор за услугата**		**7F**	**NR**
#6	Идентификатор на заявка за услугата SecurityAccess		27	SA
#7	ResponseCode =	[generalReject	10	RC_GR
		subFunctionNotSupported	12	RC_SFNS
		incorrectMessageLength	13	RC_IML
		conditionsNotCorrectOrRequestSequenceError	22	RC_CNC
		invalidKey	35	RC_IK
		exceededNumberOfAttempts	36	RC_ENA
		requestCorrectlyReceived-ResponsePending]	78	RC_RCR_RP
#8	Контролна сума		00-FF	CS

6. УСЛУГИ ЗА ПРЕДАВАНЕ НА ДАННИ

В следващата таблица са посочени наличните услуги:

Таблица 24

Услуги за предаване на данни

Наименование на услугата	Описание
ReadDataByIdentifier	Клиентът заявява предаването на актуалната стойност на запис с достъп от recordDataIdentifier.
WriteDataByIdentifier	Клиентът заявява запаметяване на запис, до който recordDataIdentifier е имал достъп.

6.1. **Услуга ReadDataByIdentifier**

6.1.1 *Описание на съобщенията*

CPR_050 Услугата ReadDataByIdentifier се използва от клиента, за да заяви извличането на стойности, които са записани на сървър. Данните се идентифицират от recordDataIdentifier. Производителят на бордовото устройство има задължение да следи за изпълнението на условията на сървъра по време на извършването на тази услуга.

6.1.2 *Формат на съобщенията*

CPR_051 Форматите на съобщенията за примитивите на ReadDataByIdentifier са подробно описани в следващите таблици.

Таблица 25

Съобщение за заявка за ReadDataByIdentifier

Байт #	Наименование на параметъра	Шестнайсетична стойност	Мнемоничен код
#1	Байт за структура — физическо адресиране	80	FMT
#2	Байт за целевия адрес	EE	TGT
#3	Байт за изходния адрес	tt	SRC
#4	Допълнителен байт за дължина	03	LEN
#5	**Идентификатор на заявка за услугата ReadDataByIdentifier**	**22**	**RDBI**
#6 до #7	recordDataIdentifier = [стойност от таблица 28]	xxxx	RDI_…
#8	Контролна сума	00-FF	CS

Таблица 26

Съобщение за положителен отговор за ReadDataByIdentifier

Байт #	Наименование на параметъра	Шестнайсетична стойност	Мнемоничен код
#1	Байт за структура — физическо адресиране	80	FMT
#2	Байт за целевия адрес	tt	TGT
#3	Байт за изходния адрес	EE	SRC
#4	Допълнителен байт за дължина	m + 3	LEN
#5	**Идентификатор на положителен отговор за услугата ReadDataByIdentifier**	**62**	**RDBIPR**
#6 и #7	recordDataIdentifier = [същата стойност като байтовете #6 и #7 таблица 25]	xxxx	RDI_…
#8 до #m + 7	dataRecord[] = [data#1 : data#m]	xx : xx	DREC_DATA1 : DREC_DATAm
#m + 8	Контролна сума	00-FF	CS

Таблица 27

Съобщение за отрицателен отговор за ReadDataByIdentifier

Байт #	Наименование на параметъра		Шестнайсетична стойност	Мнемоничен код
#1	Байт за структура — физическо адресиране		80	FMT
#2	Байт за целевия адрес		tt	TGT
#3	Байт за изходния адрес		EE	SRC
#4	Допълнителен байт за дължина		03	LEN
#5	**Идентификатор на отрицателен отговор за услугата**		**7F**	**NR**
#6	Идентификатор на заявка за услугата ReadDataByIdentifier		22	RDBI
#7	ResponseCode=	[requestOutOfRange	31	RC_ROOR
		incorrectMessageLength	13	RC_IML
		conditionsNotCorrect]	22	RC_CNC
#8	Контролна сума		00-FF	CS

6.1.3 *Определяне на параметрите*

CPR_052 Параметърът ***recordDataIdentifier (RDI_)*** в съобщението за заявка за ReadDataByIdentifier идентифицира запис на данни.

CPR_053 Определените с настоящия документ стойности на recordDataIdentifier са показани в таблицата по-долу.

Таблицата за recordDataIdentifier се състои от четири колони и няколко реда.

— **Първата колона (Hex.)** указва „Hex Value.“ (шестнайсетична стойност), присвоявана на recordDataIdentifier, посочен в третата колона.

— **Втората колона (елемент от данни)** показва елемента на данни от допълнение 1, на който се основава recordDataIdentifier (понякога е необходимо преобразуване на кода).

— **Третата колона (описание)** указва наименованието на съответния recordDataIdentifier.

— **Четвъртата колона (мнемоничен код)** показва мнемоничния код, свързан с този recordDataIdentifier.

Таблица 28

Определяне на стойностите на recordDataIdentifier

Hex	Елемент от данни	Наименование на recordDataIdentifier (вж. формàта в раздел 8.2)	Мнемоничен код
F90B	`CurrentDateTime`	TimeDate	RDI_TD
F912	`HighResOdometer`	HighResolutionTotalVehicleDistance	RDI_HRTVD
F918	`K-ConstantOfRecordingEquipment`	Kfactor	RDI_KF

Hex	Елемент от данни	Наименование на recordDataIdentifier (вж. формàта в раздел 8.2)	Мнемоничен код
F91C	L-TyreCircumference	LfactorTyreCircumference	RDI_LF
F91D	W-VehicleCharacteristicConstant	WvehicleCharacteristicFactor	RDI_WVCF
F921	TyreSize	TyreSize	RDI_TS
F922	nextCalibrationDate	NextCalibrationDate	RDI_NCD
F92C	SpeedAuthorised	SpeedAuthorised	RDI_SA
F97D	vehicleRegistrationNation	RegisteringMemberState	RDI_RMS
F97E	VehicleRegistrationNumber	VehicleRegistrationNumber	RDI_ VRN
F190	VehicleIdentificationNumber	VIN	RDI_ VIN

CPR_054 Параметърът ***dataRecord (DREC_)*** е използван от съобщението за положителен отговор на ReadDataByIdentifier, за да подаде на клиента (изпитвателното оборудване) стойността от записа на данни, идентифицирана от recordDataIdentifier. Форматите на данни са посочени в раздел 8. Други dataRecords, включително входящите данни в бордовото устройство, вътрешните и изходните данни, могат да се получат по избор от потребителя, но те не са определени в настоящия документ.

6.2. **Услуга WriteDataByIdentifier**

6.2.1 *Описание на съобщенията*

CPR_056 Клиентът използва услугата WriteDataByIdentifier, за да запише стойностите от записи на данни върху сървър. Данните се идентифицират от recordDataIdentifier. Производителят на бордовото устройство има задължение да следи за изпълнението на условията на сървъра по време на извършването на тази услуга. За актуализация на параметрите, изброени в таблица 28, бордовото устройство трябва да е в режим КАЛИБРИРАНЕ.

6.2.2 *Формат на съобщенията*

CPR_057 Форматите на съобщенията за примитивите на WriteDataByIdentifier са подробно описани в следващите таблици.

Таблица 29

Съобщение за заявка за WriteDataByIdentifier

Байт #	Наименование на параметъра	Шестнайсетична стойност	Мнемоничен код
#1	Байт за структура — физическо адресиране	80	FMT
#2	Байт за целевия адрес	EE	TGT
#3	Байт за изходния адрес	tt	SRC
#4	Допълнителен байт за дължина	m + 3	LEN
#5	**Идентификатор на заявка за услугата WriteDataByIdentifier**	**2E**	**WDBI**
#6 до #7	recordDataIdentifier = [стойност от таблица 28]	xxxx	RDI_…

Байт #	Наименование на параметъра	Шестнайсетична стойност	Мнемоничен код
#8 до m + 7	dataRecord[] = [data#1 : data#m]	xx : xx	DREC_DATA1 : DREC_DATAm
#m + 8	Контролна сума	00-FF	CS

Таблица 30

Съобщение за положителен отговор за WriteDataByIdentifier

Байт #	Наименование на параметъра	Шестнайсетична стойност	Мнемоничен код
#1	Байт за структура — физическо адресиране	80	FMT
#2	Байт за целевия адрес	tt	TGT
#3	Байт за изходния адрес	EE	SRC
#4	Допълнителен байт за дължина	03	LEN
#5	**Идентификатор на положителен отговор за услугата WriteDataByIdentifier**	**6E**	**WDBIPR**
#6 до #7	recordDataIdentifier = [същата стойност като байтовете #6 и #7 таблица 29]	xxxx	RDI_…
#8	Контролна сума	00-FF	CS

Таблица 31

Съобщение за отрицателен отговор за WriteDataByIdentifier

Байт #	Наименование на параметъра	Шестнайсетична стойност	Мнемоничен код
#1	Байт за структура — физическо адресиране	80	FMT
#2	Байт за целевия адрес	tt	TGT
#3	Байт за изходния адрес	EE	SRC
#4	Допълнителен байт за дължина	03	LEN
#5	**Идентификатор на отрицателен отговор за услугата**	**7F**	**NR**
#6	Идентификатор на заявка за услугата WriteDataByIdentifier	2E	WDBI

Байт #	Наименование на параметъра		Шестнайсетична стойност	Мнемоничен код
#7	ResponseCode=	[requestOutOfRange	31	RC_ROOR
		incorrectMessageLength	13	RC_IML
		conditionsNotCorrect]	22	RC_CNC
#8	Контролна сума		00-FF	CS

6.2.3 *Определяне на параметрите*

Параметърът ***recordDataIdentifier (RDI_)*** е определен таблица 28.

Параметърът ***dataRecord (DREC_)*** се използва от съобщението за заявка на WriteDataByIdentifier, за да осигури стойностите на записа от данни, идентифициран от recordDataIdentifier, на сървъра (бордовото устройство). Форматите на данни са посочени в раздел 8.

7. КОНТРОЛ НА ИЗПИТВАТЕЛНИТЕ ИМПУЛСИ — ФУНКЦИОНАЛЕН БЛОК ЗА КОНТРОЛ НА ВХОДНИТЕ/ИЗХОДНИТЕ ДАННИ

В следващата таблица са посочени наличните услуги:

Таблица 32

Функционален блок за контрол на входните/изходните данни

Наименование на услугата	Описание
InputOutputControlByIdentifier	Клиентът заявява извършване на контрол на определени входни/изходни данни на сървъра

7.1. Услуга InputOutputControlByIdentifier

7.1.1 *Описание на съобщенията*

Връзката, която се осъществява посредством фронтално разположения съединител, позволява контрола или следенето на изпитвателните импулси с помощта на съответно изпитвателно оборудване

CPR_058 Възможно е да се конфигурира тази линия за входни/изходни сигнали за калибриране с команда по линията K, като се използва услугата InputOutputControlByIdentifier за избора на необходимата входна или изходна функция за линията. Съществуват следните състояния по линията:

— дезактивирана,

— speedSignalInput, когато линията за входния/изходния сигнал за калибриране се използва за въвеждане на сигнал за скорост (изпитвателен сигнал), който замества сигнала за скорост на датчика за движение, като тази функция не съществува в режим КОНТРОЛ,

— realTimeSpeedSignalOutputSensor, когато линията за входни/изходни сигнали за калибриране се използва за извеждане на сигнала за скорост на датчика за движение,

— RTCOutput, когато линията за входни/изходни сигнали за калибриране се използва за извеждане на сигнала на часовника, работещ по координираното универсално време, като тази функция не съществува в режим КОНТРОЛ.

CPR_059 За да бъде в състояние да конфигурира състоянието на линията, бордовото устройство трябва да е започнало сесия за настройка и да работи в режим КАЛИБРИРАНЕ или КОНТРОЛ. Когато бордовото устройство е в режим КАЛИБРИРАНЕ, могат да се изберат четирите състояние на линията (дезактивирана, speedSignalInput, realTimeSpeedSignalOutputSensor и RTCOutput). Когато бордовото устройство е в режим КОНТРОЛ, могат да се изберат само двете състояние на линията (дезактивирана и realTimeSpeedSignalOutputSensor). При приключване на сесия за настройка или излизане от режим КАЛИБРИРАНЕ или КОНТРОЛ, бордовото устройство трябва да осигури линията за входни/изходни сигнали за калибриране да се е върнала в дезактивирано състояние (по подразбиране).

CPR_060 В случай на получаване на импулси за скорост по линията за входния сигнал за моментната скорост на бордовото устройство, при положение че линията за входни/изходни сигнали работи в режим на въвеждане на данни, тази линия трябва да премине в режим на извеждане на данни или да се върне в своето дезактивирано състояние.

CPR_061 Последователността на операциите е следната:

— установяване на връзки чрез услугата StartCommunication,

— влизане в сесия за настройка чрез услугата StartDiagnosticSession и преминаване в режим на работа КАЛИБРИРАНЕ ИЛИ КОНТРОЛ (редът на изпълнение на тези две операции е без значение),

— промяна на състоянието на изхода чрез услугата InputOutputControlBydentifier.

7.1.2 *Формат на съобщенията*

CPR_062 Форматите на съобщенията за примитивите на InputOutputControlByIdentifier са подробно описани в следващите таблици.

Таблица 33

Съобщение за заявка за InputOutputControlByIdentifier

Байт #	Наименование на параметъра	Шестнайсетична стойност	Мнемоничен код
#1	Байт за структура — физическо адресиране	80	FMT
#2	Байт за целевия адрес	EE	TGT
#3	Байт за изходния адрес	tt	SRC
#4	Допълнителен байт за дължина	xx	LEN
#5	**Идентификатор на заявка за InputOutputControlByIdentifier**	**2F**	**IOCBI**
#6 и #7	InputOutputIdentifier = [CalibrationInputOutput]	F960	IOI_CIO
#8 или	ControlOptionRecord = [		COR_…
#8 до #9	inputOutputControlParameter — една стойност от таблица 36	xx	IOCP_…
	controlState — една стойност от таблица 37 (вж. забележката по-долу)]	xx	CS_…
#9 или #10	Контролна сума	00-FF	CS

Забележка: параметърът controlState се появява само в някои случаи (вж. 7.1.3).

Таблица 34

Съобщение за положителен отговор за InputOutputControlByIdentifier

Байт #	Наименование на параметъра	Шестнайсетична стойност	Мнемоничен код
#1	Байт за структура — физическо адресиране	80	FMT
#2	Байт за целевия адрес	tt	TGT

Байт #	Наименование на параметъра	Шестнайсетична стойност	Мнемоничен код
#3	Байт за изходния адрес	EE	SRC
#4	Допълнителен байт за дължина	xx	LEN
#5	**Идентификатор на положителен отговор за inputOutputControlByIdentifier**	**6F**	**IOCBIPR**
#6 и #7	inputOutputIdentifier = [CalibrationInputOutput]	F960	IOI_CIO
#8 или #8 до #9	controlStatusRecord = [		CSR_
	inputOutputControlParameter (същата стойност като байт #8 таблица 33)	xx	IOCP_…
	controlState (същата стойност като байт #9 таблица 33)] (ако е приложимо)	xx	CS_…
#9 или #10	Контролна сума	00-FF	CS

Таблица 35

Съобщение за отрицателен отговор за InputOutputControlByIdentifier

Байт #	Наименование на параметъра	Шестнайсетична стойност	Мнемоничен код
#1	Байт за структура — физическо адресиране	80	FMT
#2	Байт за целевия адрес	tt	TGT
#3	Байт за изходния адрес	EE	SRC
#4	Допълнителен байт за дължина	03	LEN
#5	**Идентификатор на отрицателен отговор за услугата**	**7F**	**NR**
#6	Идентификатор на заявка за inputOutputControlByIdentifier	2F	IOCBI
#7	responseCode=[		
	incorrectMessageLength	13	RC_IML
	conditionsNotCorrect	22	RC_CNC
	requestOutOfRange	31	RC_ROOR
	deviceControlLimitsExceeded]	7A	RC_DCLE
#8	Контролна сума	00-FF	CS

7.1.3 *Определяне на параметрите*

CPR_064 Параметърът ***inputOutputControlParameter (IOCP_)*** е определен в следващата таблица.

Таблица 36

Определяне на стойностите на inputOutputControlParameter

Hex	Описание	Мнемоничен код
00	**ReturnControlToECU** Тази стойност трябва да посочва на сървъра (бордовото устройство), че изпитвателното оборудване не управлява повече линията за входни/изходни сигнали за калибриране.	RCTECU
01	**ResetToDefault** Тази стойност трябва да посочва на сървъра (бордовото устройство), че трябва да върне линията за входни/изходни сигнали за калибриране към състоянието ѝ по подразбиране.	RTD
03	**ShortTermAdjustment** Тази стойност трябва да посочва на сървъра (бордовото устройство), че трябва да настрои линията за входни/изходни сигнали за калибриране към стойността, включена в параметъра controlState.	STA

CPR_065 Параметърът ***controlState*** се появява само когато inputOutputControlParameter е конфигуриран като ShortTermAdjustment и е определен в следващата таблица:

Таблица 37

Определяне на стойностите на controlState

Режим	Шестнайсетична стойност	Описание
Дезактивиран	00	Дезактивирана линия за вход/изход (по подразбиране)
Активиран	01	Активирана линия за вход/изход за калибриране като speedSignalInput
Активиран	02	Активирана линия за вход/изход за калибриране като realTimeSpeedSignalOutputSensor
Активиран	03	Активирана линия за вход/изход за калибриране като RTCOutput

8. ФОРМАТИ НА DATARECORDS

В настоящия раздел са изложени подробно:

— общите правила, които трябва да се прилагат към диапазоните от параметри, предавани от бордовото устройство към изпитвателното оборудване,

— форматите, които трябва да се използват за прехвърлените данни чрез услугите за предаване на данни, изложени в раздел 6.

CPR_067 Всички идентифицирани параметри трябва да се поддържат от бордовото устройство.

CPR_068 Данните, предавани от бордовото устройство към изпитвателното оборудване в отговор на съобщение за заявка, трябва да са измерими (тоест актуалната стойност на заявения параметър е такава, каквато е измерена или наблюдавана от бордовото устройство).

8.1. **Диапазони от предавани параметри**

CPR_069 Таблица 38 определя използваните диапазони за определяне валидността на даден предаван параметър.

CPR_070 Стойностите от диапазона „индикатор за грешка“ позволяват на бордовото устройство да посочи веднага, че към съответния момент не са налице валидни данни за параметъра поради някакъв вид грешка в тахографа.

CPR_071 Стойностите от диапазона „не е наличен“ позволяват на бордовото устройство да изпрати съобщение, съдържащо параметър, който не е наличен или не се поддържа в този модул. Стойностите от диапазона „Незаявен“ позволяват на устройството да предаде командно съобщение и да идентифицира параметрите, за които не се очаква отговор от получаващото устройство.

CPR_072 Когато неизправност в даден компонент попречи на предаването на валидни данни за даден параметър, е целесъобразно да се използва индикаторът за грешка, така както е описан в таблица 38, вместо данните за този параметър. Въпреки това, ако измерените или изчислените данни показват валидна стойност, която обаче надвишава определения за този параметър диапазон, индикаторът за грешка не трябва да бъде използван. В този случай следва да се предадат данните, като се използва подходящата минимална или максимална стойност на параметъра.

Таблица 38

Диапазони на dataRecords

Наименование на диапазона	1 байт (шестнайсетична ст-т)	2 байта (шестнайсетична ст-т)	4 байта (стойност hex.)	ASCII
Валиден сигнал	00 до FA	0000 до FAFF	00000000 до FAFFFFFF	1 до 254
Специфичен за даден параметър индикатор	FB	FB00 до FBFF	FB000000 до FBFFFFFF	Няма
Диапазон, запазен за бъдещите битове на индикатора	FC до FD	FC00 до FDFF	FC000000 до FDFFFFFF	Няма
Индикатор за грешка	FE	FE00 до FEFF	FE000000 до FEFFFFFF	0
Не е наличен или незаявен	FF	FF00 до FFFF	FF000000 до FFFFFFFF	FF

CPR_073 За параметрите, кодирани в ASCII, символът ASCII „*“ се запазва като разграничител.

8.2. **Формати на dataRecords**

В таблица 39 до таблица 42 са изложени подробно форматите, които трябва да се използват чрез услугите ReadDataByIdentifier и WriteDataByIdentifier.

CPR_074 Таблица 39 указва дължината, разделителната способност и оперативния диапазон на всеки параметър, идентифициран от своя recordDataIdentifier:

Таблица 39

Формат на dataRecords

Наименование на параметъра	Дължина на данните (байтове)	Разделителна способност	Оперативен диапазон
TimeDate	8	Вж. подробна информация в таблица 40	
HighResolutionTotalVehicleDistance	4	усилване 5 m/bit, отместване 0 m	0 до + 21 055 406 km
Kfactor	2	усилване 0,001 imp/m/bit, отместване 0	0 до 64,255 imp/m
LfactorTyreCircumference	2	усилване 0,125 10^{-3} m/bit, отместване 0	0 до + 8,031 m
WvehicleCharacteristicFactor	2	усилване 0,001 imp/m/bit, отместване 0	0 до 64,255 imp/m
TyreSize	15	ASCII	ASCII

Наименование на параметъра	Дължина на данните (байтове)	Разделителна способност	Оперативен диапазон
NextCalibrationDate	3	Вж. подробна информация в таблица 41	
SpeedAuthorised	2	усилване 1/256 km/h/bit, отместване 0	0 до 250,996 km/h
RegisteringMemberState	3	ASCII	ASCII
VehicleRegistrationNumber	14	Вж. подробна информация в таблица 42	
VIN	17	ASCII	ASCII

CPR_075 Таблица 40 показва подробно форматите на различните байтове на параметъра TimeDate:

Таблица 40

Подробна структура на TimeDate (стойност на recordDataIdentifier # F90B)

Байт	Определяне на параметрите	Разделителна способност	Оперативен диапазон
1	Секунди	усилване 0,25 s/bit, отместване 0 секунди	0 до 59,75 s
2	Минути	усилване 1 min/bit, отместване 0 минути	0 до 59 минути
3	Часове	усилване 1 h/bit, отместване 0 часа	0 до 23 ч
4	Месец	усилване 1 month/bit, отместване 0 месеца	1 до 12 месеца
5	Ден	усилване 0,25 дена/bit, отместване 0 дена (вж. забележката по-долу таблица 41)	0,25 до 31,75 дена
6	Година	усилване 1 година/bit, отместване + 1985 година (вж. забележката по-долу таблица 41)	1985 до 2235 година
7	Корекция на минути спрямо местното време	усилване 1 min/bit, отместване – 125 min	– 59 до 59 минути
8	Поправка на часове спрямо местното време	усилване 1 h/bit, отместване – 125 h	– 23 до + 23 ч

CPR_076 Таблица 41 показва подробно форматите на различните байтове на параметъра NextCalibrationDate:

Таблица 41

Подробен формат на NextCalibrationDate (стойност на recordDataIdentifier # F922)

Байт	Определяне на параметрите	Разделителна способност	Оперативен диапазон
1	Месец	усилване 1 месец/bit, отместване 0 месеца	1 до 12 месеца
2	Ден	усилване 0,25 дена/bit, отместване 0 дена (вж. забележката по-долу)	0,25 до 31,75 дена
3	Година	усилване 1 година/bit, отместване + 1985 година (вж. забележката по-долу)	1985 до 2235 година

ЗАБЕЛЕЖКА относно използването на параметъра„Ден“:

1) Стойност 0 за датата е нулева. Стойностите 1, 2, 3 и 4 се използват, за да идентифицират първия ден от месеца; стойностите 5, 6, 7 и 8 указват втория ден на месеца и т.н.

2) Този параметър не влияе, нито променя параметъра за часовете по-горе.

ЗАБЕЛЕЖКА относно използването на байта на параметъра„година“:

Стойност 0 за годината отговаря на година 1985; стойност от 1 отговаря на година 1986 и т.н.

CPR_078 Таблица 42 показва подробно форматите на различните байтове на параметъра VehicleRegistration-Number:

Таблица 42

Подробен формат на VehicleRegistrationNumber (стойност на recordDataIdentifier # F97E)

Байт	Определяне на параметрите	Разделителна способност	Оперативен диапазон
1	Кодова страница (както е определена в допълнение 1)	ASCII	от 01 до 0A
2 — 14	Регистрационен номер на превозното средство (както е определен в допълнение 1)	ASCII	ASCII

Допълнение 9

МИНИМАЛНО ИЗИСКВАНИ ИЗПИТВАНИЯ ЗА ОДОБРЕНИЕ НА ТИПА

СЪДЪРЖАНИЕ

1. ВЪВЕДЕНИЕ

1.1. **Одобряване на типа**

ЕО одобряването на типа на уреди за регистриране на данните за движението (или на техен компонент), или съответно на тахографска карта, се основава на:

— **сертифициране за сигурност**, въз основа на спецификациите на Общите критерии, при цел за състояние на сигурност на системата, което да е в пълно съответствие с допълнение 10 към настоящото приложение (подлежи на допълване/изменение),

— **сертифициране за функционалност**, извършвано от компетентния орган на съответната държава членка, удостоверяващо че изпитваното устройство отговаря на изискванията в настоящото приложение по отношение на изпълняваните функции, на точността на измерванията и на характеристиките на околната среда,

— **сертифициране за оперативна съвместимост**, извършвано от компетентния орган, удостоверяващо че уредът за регистриране на данните за движението (или тахографската карта) е изцяло оперативно съвместим съответно с необходимите модели тахографска карта (или уред за регистриране на данните за движението) (виж глава 8 от настоящото приложение).

В настоящото допълнение е уточнено кои изпитвания трябва да бъдат проведени като минимум от компетентния орган на дадена държава членка в рамките на функционалните изпитвания, както и кои изпитвания трябва да бъдат проведени като минимум от компетентния орган в рамките на изпитванията за оперативна съвместимост. Не са включени допълнителни уточнения нито за процедурите за провеждането на тези изпитвания, нито за типа на изпитванията.

Също така, в настоящото допълнение не са разгледани и аспектите на сертифицирането за сигурност. Ако по време на процеса за оценяване и сертифициране на сигурността са извършени някои изпитвания, изисквани за одобряването на типа, не е необходимо те да бъдат провеждани повторно. В такъв случай могат да бъдат инспектирани само резултатите от тези изпитания за сигурност. С информативна цел в настоящото допълнение са отбелязани със звездичка („*“) изискванията, за които се очаква да бъдат проведени изпитвания при сертифицирането за сигурност (или съответно изискванията, тясно свързани с такива изпитвания).

Номерираните изисквания са свързани със съдържанието на настоящото приложение, а останалите изисквания са свързани с другите допълнения (например PIC_001 е свързано с Допълнение 3 „Пиктограми“).

В настоящото допълнение са разгледани поотделно одобряването на типа на датчика за движение, на бордовото устройство и на външното устройство за GNSS, в качеството им на компоненти на уредите за регистриране на данните за движението. За всеки компонент се издава негов отделен сертификат за одобрение, в който се посочват другите съвместими компоненти. Функционалното изпитване на датчика за движение (или на външното устройство за GNSS) се прави заедно с бордовото устройство, и обратно.

Не се изисква оперативна съвместимост между всеки модел датчик за движение (респективно всеки модел външно устройство за GNSS) и всеки модел бордово устройство. В подобни случаи одобрението на типа на датчик за движение (респективно на външно устройство за GNSS) може да бъде дадено само в комбинация с одобрение на типа на съответното бордово устройство и обратно.

1.2. **Позовавания**

В настоящото допълнение се използват позовавания на следните стандарти:

IEC 60068-2-1: Изпитване на въздействия на околната среда — Част 2-1: Изпитвания — Изпитване A: Студ

IEC 60068-2-2: Основни процедури за изпитване на въздействия на околната среда; Част 2: Изпитвания; Изпитване B: Суха топлина (синусоидални).

IEC 60068-2-6: Изпитване на въздействия на околната среда — Част 2: Изпитвания — Изпитване Fc:: Вибрации

IEC 60068-2-14: Изпитания на въздействия на околната среда; Част 2-14: Изпитвания; Изпитване N: Промени на температурата

IEC 60068-2-27: Изпитания на въздействия на околната среда. Част 2: Изпитвания. Изпитване Ea и указания: Удар

IEC 60068-2-30: Изпитване на въздействия на околната среда — Част 2-30: Изпитвания — Изпитване Db: Влажна топлина, циклично (цикъл 12 + 12 часа)

IEC 60068-2-64: Изпитване на въздействия на околната среда — Част 2-64: Изпитвания — Изпитване Fh: Вибрации, широколентови случайни, и указания

IEC 60068-2-78: Изпитване на въздействия на околната среда — Част 2-78: Изпитвания — ИзпитванеCab: Влажна топлина, постоянен режим

ISO 16750-3 Механични натоварвания (2012-12)

ISO 16750-4 Климатични натоварвания (2010-04)

ISO 20653: Пътни превозни средства. Степен на защита (IP код). Защита на електрическото оборудване срещу чужди обекти, вода и достъп

ISO 10605:2008 + Техническа поправка:2010 + AMD1:2014 Пътни превозни средства. Методи за изпитване на електрически смущения, предизвикани от електростатичен разряд

ISO 7637-1:2002 + AMD1: 2008 Пътни превозни средства. Електрически смущения от електропроводящите устройства и свързването. Част 1: Определения и общи съображения.

ISO 7637-2 Пътни превозни средства. Електрически смущения от електропроводящите устройства и свързването. Част 2: Разпространение на смущения от преходни процеси само по захранващите линии.

ISO 7637-3 Пътни превозни средства. Електрически смущения от електропроводящите устройства и свързването. Част 3: Прехвърляне на смущения от преходни процеси чрез капацитивно и индуктивно свързване по линии, различни от захранващите линии.

ISO/IEC 7816-1 Идентификационни карти. Карти с интегрална(и) схема(и) с контакти. Част 1: Физични характеристики.

ISO/IEC 7816-2 Информационни технологии. Идентификационни карти. Карти с интегрална(и) схема(и) с контакти. Част 2: Размери и разположение на контактите.

ISO/IEC 7816-3 Информационни технологии. Идентификационни карти. Карти с интегрална(и) схема(и) с контакти. Част 3: Електронни сигнали и протоколи за предаване.

ISO/IEC 10373-1:2006 + AMD1:2012 Идентификационни карти. Методи за изпитване. Част 1: Общи характеристики

ISO/IEC 10373-3:2010 + Technical Corrigendum:2013 Идентификационни карти. Методи за изпитване. Част 3: Карти с интегрална(и) схема(и) с контакти и съответни интерфейсни устройства

ISO 16844-3:2004, Cor 1:2006 Пътни превозни средства. Тахографски системи. Част 3: Интерфейс на датчика за движение (към бордови устройства).

ISO 16844-4 Пътни превозни средства. Тахографски системи. Част 4: Интерфейс на CAN мрежа

ISO 16844-6 Пътни превозни средства. Тахографски системи. Част 6: Диагностика

ISO 16844-7 Пътни превозни средства. Тахографски системи. Част 7: Параметри

ISO 534 Хартия и картон. Определяне на дебелина, плътност и специфичен обем

Правило № 10 на ИКЕ на ООН Единни условия относно одобряването на превозни средства по отношение на електромагнитната съвместимост (Икономическа комисия за Европа на Организацията на обединените нации)

2. ФУНКЦИОНАЛНИ ИЗПИТВАНИЯ НА БОРДОВОТО УСТРОЙСТВО

№	Изпитване	Описание	Съответни изисквания
1	**Административен преглед**		
1.1	Документация	Коректност на документацията	
1.2	Резултати от изпитване, проведено от производителя	Резултати от изпитване при интегриране, проведено от производителя Писмени демонстрации.	88, 89,91
2	**Визуално инспектиране**		
2.1	Съответствие с документацията		
2.2	Идентификация/маркировки		224 до 226
2.3	Материали		219 до 223
2.4	Херметизация		398, 401 до 405
2.5	Външни интерфейси		
3	**Функционални изпитвания**		
3.1	Осигурявани функции		03, 04, 05, 07, 382,
3.2	Режими на работа		09 до 11*, 132, 133
3.3	Права за достъп до функции и данни		12* 13*, 382, 383, 386 до 389
3.4	Следене на вкарването и изваждането на картите		15, 16, 17, 18, 19*, 20*, 132
3.5	Измерване на скорост и разстояние		21 до 31
3.6	Измерване на време (изпитване, провеждано при 20 °C)		38 до 43
3.7	Следене на дейностите на водача		44 до 53, 132
3.8	Следене на състоянието при управление на МПС		54, 55, 132

№	Изпитване	Описание	Съответни изисквания
3.9	Ръчно въвеждани данни		56 до 62
3.10	Управление на фирмените блокировки за информация на превозвачи		63 до 68
3.11	Следене на контролните дейности		69, 70
3.12	Установяване на събития и/или неизправности		71 до 88, 132
3.13	Данни за идентифициране на уредите		93*, 94*, 97, 100
3.14	Данни за вкарването и изваждането на картата на водач		102* до 104*
3.15	Данни за дейностите на водача		105* до 107*
3.16	Данни за места и местоположения		108* до 112*
3.17	Данни от километражния брояч		113* до 115*
3.18	Подробни данни за скоростта		116*
3.19	Данни за събития		117*
3.20	Данни за неизправности		118*
3.21	Данни за калибриране		119* до 121*
3.22	Данни за сверяване на часовника		124*, 125*
3.23	Данни за контролните дейности		126*, 127*
3.24	Данни за фирмени блокировки за информация на превозвачи		128*
3.25	Изтегляне на данни за дейностите		129*
3.26	Данни за специфични условия		130*, 131*
3.27	Записване и запаметяване върху тахографските карти		134, 135, 136*, 137*, 139*, 140, 141 142, 143, 144*, 145*, 146*, 147, 148
3.28	Показване върху дисплея		90, 132, 149 до 166, PIC_001, DIS_001
3.29	Разпечатване		90, 132, 167 до 179, PIC_001, PRT_001 до PRT_014
3.30	Предупреждаване		132, 180 до 189, PIC_001

№	Изпитване	Описание	Съответни изисквания
3.31	Изтегляне на данни към външни носители		90, 132, 190 до 194
3.32	Връзка от разстояние за извършване на насочени пътни проверки		195 до 197
3.33	Данни, прехвърляни към допълнителни външни устройства		198, 199
3.34	Калибриране		202 до 206*, 383, 384, 386 до 391
3.35	Крайпътна проверка на калибрирането		207 до 209
3.36	Сверяване на часовника		210 до 212*
3.37	Отсъствие на смущения от страна на допълнителните функции		06, 425
3.38	Интерфейс на датчика на движение		02, 122
3.39	Външно устройство за GNSS		03, 123
3.40	Да се провери дали бордовото устройство открива, записва и съхранява събитието(та) и/или неизправността(ите), определени от производителя на бордовото устройство, когато съответно свързан с него датчик за движение реагира на магнитни полета, смущаващи установяването на движението на превозното средство.		217
3.41	Криптографска поредица (cypher suite) и стандартизирани домейн параметри		CSM_48, CSM_50
4	**Изпитания за въздействията на околната среда**		
4.1	Температура	Проверява се функционалността чрез следните изпитвания: Изпитване съгласно ISO 16750-4, глава 5.1.1.2: Изпитване за работа при ниска температура (72 часа при – 20 °C) Това изпитване е с позоваване на IEC 60068-2-1: Изпитване на въздействия на околната среда — Част 2-1: Изпитвания. Изпитване A: Студ Изпитване съгласно ISO 16750-4: Глава 5.1.2.2 Изпитване за работа при висока температура (72 часа при 70 °C) Това изпитване е с позоваване на IEC 60068-2-2: Основни процедури за изпитване на въздействия на околната среда; Част 2: Изпитвания; Изпитвания B: Суха топлина Изпитване съгласно ISO 16750-4: Глава 5.3.2: Бърза промяна на температурата при зададена продължителност на прехода (– 20 °C/70 °C, 20 цикъла, време на задържане при всяка от температурите 2 часа) Възможно е да се проведат намален набор изпитвания (измежду посочените в раздел 3 на настоящата таблица) съответно при ниските температури, високите температури и температурните цикли	213

№	Изпитване	Описание	Съответни изисквания
4.2	Влажност	Проверява се, че бордовото устройство може да понесе циклично изпитване на топлина във влажна среда съгласно IEC 60068-2-30, изпитване Db, със шест цикъла по 24 часа, като във всеки от тях температурата се изменя от + 25 °C до + 55 °C и относителната влажност е съответно 97 % при + 25 °C и 93 % при + 55 °C	214
4.3	Механични въздействия	1. Синусоидални вибрации. Проверява се, че бордовото устройство може да понесе синусоидни вибрации със следните характеристики: постоянно изместване, при честота между 5 и 11 Hz: максимум 10 mm постоянно ускорение, при честота между 11 и 300 Hz: 5 g Съответствието с това изискване с проверява чрез изпитване Fc по IEC 60068-2-6, с минимално времетраене на изпитването 3 × 12 часа (по 12 часа на координатна ос) Стандартът ISO 16750-3 не изисква да се провежда изпитване със синусоидални вибрации за устройства, намиращи се в отделна кабина на превозното средство (decoupled vehicle cab). 2. Случайни вибрации: Изпитване съгласно ISO 16750-3: Глава 4.1.2.8 Изпитване VIII: Търговски превозни средства (commercial vehicles) с отделна кабина Изпитване за случайни вибрации (Random vibration test), 10…2 000 Hz, вертикално средноквадратично отклонение 21,3 m/s^2, надлъжно средноквадратично отклонение 11,8 m/s^2, напречно средноквадратично отпклонение 13,1 m/s^2, 3 оси, по 32 часа за ос, включително температурен цикъл – 20…70 °C. Това изпитване е с позоваване на IEC 60068-2-64: Изпитване на въздействия на околната среда — Част 2-64: Изпитвания. Изпитване Fh: Вибрации, широколентови случайни, и указания 3. Удари: механичен удар с ускорение 3g, полусинусоидален, съгласно ISO 16750. Гореописаните изпитвания се извършват върху различни мостри на изпитваните съоръжения.	219
4.4	Защита срещу вода и чужди тела	Изпитване съгласно ISO 20653: Пътни превозни средства. Степен на защита (IP код). Защита на електрическото оборудване срещу чужди обекти, вода и достъп (запазване на характеристиките); Минимално допустима стойност IP 40	220, 221
4.5	Защита срещу пренапрежения	Проверява се, че бордовото устройство може да понесе захранващо напрежение както следва: при варианти за напрежение 24 V: 34 V при + 40 °C в продължение на 1 час при варианти за 12 V: 17 V при + 40 °C в продължение на 1 час (ISO 16750-2)	216
4.6	Защита срещу обратна полярност	Проверява се, че бордовото устройство може да издържи на размяна на полюсите на своето електрическо захранване (ISO 16750-2)	216

№	Изпитване	Описание	Съответни изисквания
4.7	Защита срещу къси съединения	Проверява се, че входно/изходните сигнали са защитени срещу къси съединения към захранването и към масата (ISO 16750-2)	216
5	**Изпитание за електромагнитна съвместимост (ЕМС)**		
5.1	Излъчени емисии и чувствителност към тях	Съответствие с Правило № 10 на ИКЕ на ООН	218
5.2	Електростатичен разряд	Съответствие със стандарт ISO 10605:2008 + Техническа поправка:2010 + AMD1:2014: +/– 4 kV за контактен разряд и +/– 8 kV за разряд през въздух	218
5.3	Чувствителност към преходни процеси по проводниците на захранването	При варианти за напрежение 24 V: съответствие със стандарт ISO 7637-2 + Правило № 10 на ИКЕ на ООН, Преработка 3: импулс 1a: Vs = – 450 V, Ri = 50 Ω импулс 2a: Vs = + 37 V, Ri = 2 Ω импулс 2b: Vs = + 20 V, Ri = 0,05 Ω импулс 3 a: Vs = – 150 V, Ri = 50 Ω импулс 3b: Vs = + 150 V, Ri = 50 Ω импулс 4: Vs = – 16 V, Va = – 12 V, t6 = 100 ms импулс 5: Vs = + 120 V, Ri = 2,2 Ω, td = 250 ms При варианти за напрежение 12 V: съответствие със стандарт ISO 7637-1 + Правило № 10 на ИКЕ на ООН, Поправка 3: импулс 1: Vs = – 75 V, Ri = 10 Ω импулс 2 a: Vs = + 37 V, Ri = 2 Ω импулс 2b: Vs = + 10 V, Ri = 0,05 Ω импулс 3 a: Vs = – 112 V, Ri = 50 Ω импулс 3b: Vs = + 75 V, Ri = 50 Ω импулс 4: Vs = – 6 V, Va = – 5 V, t6 = 100 ms импулс 5: Vs = + 65 V, Ri = 2,2 Ω, td = 250 ms Импулс 5 се изпитва само за бордови устройства, предвидени за монтиране на превозни средства, които не разполагат с устройство за обща външна защита срещу повишено напрежение вследствие разкачане на акумулаторната батерия при зареждащ я алтернатор (protection against load dump) За примерни стойности на повишено напрежение вследствие разкачане на акумулаторната батерия при зареждащ я алтернатор, виж стандарт ISO 16750-2, 4-то издание, глава 4.6.4.	218

3. ФУНКЦИОНАЛНИ ИЗПИТВАНИЯ НА ДАТЧИКА ЗА ДВИЖЕНИЕ

№	Изпитване	Описание	Съответни изисквания
1.	**Административен преглед**		
1.1	Документация	Коректност на документацията	

№	Изпитване	Описание	Съответни изисквания
2.	**Визуално инспектиране**		
2.1.	Съответствие с документацията		
2.2.	Идентификация/маркировки		225, 226,
2.3	Материали		219 до 223
2.4.	Херметизация		398, 401 до 405
3.	**Функционални изпитвания**		
3.1	Данни за идентифициране на датчика		95 до 97*
3.2	Сдвояване датчик за движение — бордово устройство		122*, 204
3.3	Установяване на движение Точност на измерване на движението		30 до 35
3.4	Интерфейс към бордовото устройство		02
3.5	Проверява се дали датчикът за движение е защитен срещу въздействието на постоянно магнитно поле. Като алтернативна възможност се проверява дали датчикът за движение реагира по такъв начин на постоянни магнитни полета, смущаващи установяването на движение на превозното средство, че свързано с него бордово устройство да може да открива, записва и съхранява данни за неизправности във функционирането на датчика		217
4.	**Изпитания за въздействията на околната среда**		
4.1	Работна температура	Проверява се функционалността (както е дефинирана за изпитване № 3.3) за температурния обхват [– 40 °C; + 135 °C] чрез: изпитване Ad по IEC 60068-2-1, с продължителност на изпитването 96 часа при минималната температура To_{min}, изпитване Bd по IEC 60068-2-2, с продължителност на изпитването 96 часа при максимална температура To_{max} Изпитване съгласно ISO 16750-4: Глава 5.1.1.2 Изпитване за работа при ниска температура (24 часа при – 40 °C) Това изпитване е с позоваване на IEC 60068-2-1: Изпитване на въздействия на околната среда — Част 2-1: Изпитвания. Изпитване A: Студ, IEC 68-2-2 изпитване Bd, с продължителност на изпитването 96 часа при минималната температура – 40 °C. Изпитване съгласно ISO 16750-4: Глава 5.1.2.2 Изпитване за работа при висока температура (96 часа при 135 °C) Това изпитване е с позоваване на IEC 60068-2-2: Основни процедури за изпитване на въздействия на околната среда; Част 2: Изпитвания; Изпитвания B: Суха топлина	213

№	Изпитване	Описание	Съответни изисквания
4.2	Температурни цикли	Изпитване съгласно ISO 16750-4: Глава 5.3.2: Бърза промяна на температурата при зададена продължителност на прехода (– 40 °C/135 °C, 20 цикъла, време на задържане при всяка от температурите 30 минути) IEC 60068-2-14: Изпитания на въздействия на околната среда; Част 2-14: Изпитвания; Изпитване N: Промени на температурата	213
4.3	Влажностни цикли	Проверява се функционалността (както е дефинирана в изпитване № 3.3) чрез изпитване Db по IEC 60068-2-30, със шест цикъла по 24 часа, с промяна на температурата при всеки от циклите от + 25 °C до + 55 °C и относителна влажност съответно 97 % при + 25 °C и 93 % при + 55 °C	214
4.4	Вибрации	ISO 16750-3: Глава 4.1.2.6: Изпитване VI: Търговско превозно средство (commercial vehicle), двигател, скоростна кутия Смесен режим на изпитване за вибрации, включително а) Изпитване със синусоидални вибрации, 20…520 Hz, 11.4 … 120 m/s², <= 0,5 октави/минута б) Изпитване за случайни вибрации, 10…2 000 Hz, среднноквадратична стойност на ускорението (RMS) 177 m/s² по 94 часа на координатна ос, включително с температурен цикъл – 20…70 °C) Това изпитване е с позоваване на IEC 60068-2-80: Изпитване на въздействия на околната среда — Част 2-80: Изпитвания — Изпитване Fi: Вибрации — Смесен режим на изпитване	219
4.5	Механичен удар	ISO 16750-3: Глава 4.2.3: Изпитване VI: Изпитване за устройства, намиращи се във или върху скоростната кутия полусинусоидален удар, ускорение по съгласуване в интервала 3 000…15 000 m/s², времетраене на удара по съгласуване, но по-малко от 1 ms, брой на ударите: по съгласуване Това изпитване е с позоваване на IEC 60068-2-27: Изпитания на въздействия на околната среда. Част 2: Изпитвания. Изпитване Ea и указания: Удар	219
4.6	Защита срещу вода и чужди тела	Изпитване съгласно ISO 20653: Пътни превозни средства. Степен на защита (IP код). Защита на електрическото оборудване срещу чужди обекти, вода и достъп (Целева стойност IP 64)	220, 221
4.7	Защита срещу обратна полярност	Проверява се, че датчикът може да понесе размяна на полюсите на своето електрическо захранване	216
4.8	Защита срещу къси съединения	Проверява се, че входно/изходните сигнали са защитени срещу къси съединения към захранването и към масата	216

№	Изпитване	Описание	Съответни изисквания
5.	**Изпитание за електромагнитна съвместимост**		
5.1	Излъчени емисии и чувствителност към тях	Проверява се съответствието с Правило № 10 на ИКЕ на ООН	218
5.2	Електростатичен разряд	Съответствие със стандарт ISO 10605:2008 + Техническа поправка:2010 + AMD1:2014: +/– 4 kV за контактен разряд и +/– 8 kV за разряд през въздух	218
5.3	Възприемчивост към преходни процеси, разпространяващи се по линиите за данни	При варианти за напрежение 24 V: съответствие със стандарт ISO 7637-2 + Правило № 10 на ИКЕ на ООН, Преработка 3: импулс 1 a: Vs= – 450 V, Ri=50 Ω импулс 2 a: Vs= + 37 V, Ri=2 Ω импулс 2b: Vs= + 20 V, Ri=0,05 Ω импулс 3 a: Vs= – 150 V, Ri=50 Ω импулс 3b: Vs= + 150 V, Ri=50 Ω импулс 4: Vs = – 16 V, Va = – 12 V, t6 = 100 ms импулс 5: Vs = + 120 V, Ri = 2,2 Ω, td = 250 ms При варианти за напрежение 12 V: съответствие със стандарт ISO 7637-1 + Правило № 10 на ИКЕ на ООН, Преработка 3: импулс 1: Vs=– 75 V, Ri=10 Ω импулс 2a: Vs = + 37 V, Ri = 2 Ω импулс 2b: Vs = + 10 V, Ri = 0,05 Ω импулс 3a: Vs = – 112 V, Ri=50 Ω импулс 3b: Vs = + 75 V, Ri=50 Ω импулс 4: Vs = – 6 V, Va = – 5 V, t6 = 100 ms импулс 5: Vs = + 65 V, Ri = 2,2 Ω, td = 250 ms Импулс 5 се изпитва само за бордови устройства, предвидени за монтиране на превозни средства, които не разполагат с устройство за обща външна защита срещу повишено напрежение вследствие разкачане на акумулаторната батерия при зареждащ я алтернатор (protection against load dump) За примерни стойности на повишено напрежение вследствие разкачане на акумулаторната батерия при зареждащ я алтернатор виж стандарт ISO 16750-2, 4-то издание, глава 4.6.4.	218

4. ФУНКЦИОНАЛНИ ИЗПИТВАНИЯ НА ТАХОГРАФСКИТЕ КАРТИ

Изпитванията съгласно настоящия раздел 4,

№ 5 „Изпитване за спазване на протоколи“

№ 6 „Структура на картата“ и

№ 7 „Функционални изпитвания“

могат да бъдат извършвани от оценителя или сертификатора по време на процеса на сертифициране за сигурност по Общите критерии (Common Criteria security certification process) на модула с чипа.

Изпитванията с номера 2.3 и 4.2 са същите. Това са механичните изпитвания за комбинацията от тялото на картата и модула с чипа. Ако някой от тези компоненти (тялото на картата, модула с чипа) е променен, тези изпитвания са необходими.

№	Изпитване	Описание	Съответни изисквания
1.	**Административен преглед**		
1.1	Документация	Коректност на документацията	
2	**Тяло на картата**		
2.1	Оформление на отпечатването	Проверява се дали всички елементи за защита и видими данни са правилно отпечатани на картата и дали са в съответствие. [Обозначител] Приложение 1B, глава 4.1 „Видими данни“, 227) Лицевата страна трябва да съдържа: думите „карта на водач“ или „контролна карта“ или „карта за монтаж и настройки“ или „карта на превозвач“, отпечатани с главни букви на официалния(ите) език (езици) на държавата членка, която е издала картата, според типа карта. [Наименование на държавата членка] Приложение 1B, глава 4.1 „Видими данни“, 228 Лицевата страна трябва да съдържа: наименованието на държавата членка, която издава картата (незадължително); [Знак] Приложение 1B, глава 4.1 „Видими данни“, 229) Лицевата страна трябва да съдържа: отличителния знак на държавата членка, издала картата, отпечатан в бяло на син фон в правоъгълник и ограден с 12 жълти звезди. [Изброяване] Приложение 1B, глава 4.1 „Видими данни“, 232) Обратната страна трябва да съдържа: легенда на номерата, указани на лицевата страна на картата. [Цвят] Приложение 1B, глава 4.1 „Видими данни“, 234) Цветът на фона при отпечатването на тахографските карти трябва да бъде както следва: — карта на водач: бял, — карта за монтаж и настройки: червен, — контролна карта: син, — карта на превозвач: жълт.	227 до 229, 232, 234 до 236

№	Изпитване	Описание	Съответни изисквания
		[Сигурност] Приложение 1B, глава 4.1 „Видими данни“, 235) Тахографските карти трябва да имат следните елементи на защита на тялото на картата срещу подправяне и фалшифициране: — фон със защитни характеристики, включващ мотиви с плетеници (гилоши) от тънки линии и ирисов печат, — поне една двуцветна линия с микропечат.	
		[Маркировки] Приложение 1B, глава 4.1 „Видими данни“, 236) Държавите членки могат да добавят цветове или маркировки, като например национални символи и елементи за сигурност.	
		[Маркировка за одобрение] Тахографските карти трябва да съдържат маркировка за одобрение. Маркировката за одобрение се състои от: — правоъгълник, в който е разположена буквата „e“, последвана от отличителен номер или буква на страната, която е издала одобрението, — номер на одобрението, съответстващ на номера на удостоверението за одобряване на тахографската карта, разположен в непосредствена близост до посочения правоъгълник.	
2.2	Механични изпитвания	[Размер на картата] Тахографските карти трябва да съответстват на стандарта ISO/IEC 7810, Идентификационни карти. Физични характеристики, [5] Големина на картата, [5.1] Размер на картата, [5.1.1] Размери на картата и допуски, карта тип ID-1 Неизползвана карта	240, 243 ISO/IEC 7810
		[Ръбове на картата] Тахографските карти трябва да съответстват на стандарта ISO/IEC 7810, Идентификационни карти. Физични характеристики, [5] Големина на картата, [5.1] Размер на картата, [5.1.2] Ръбове на картата	

№	Изпитване	Описание	Съответни изисквания
		[Конструкция на картата] Тахографските карти трябва да съответстват на стандарта ISO/IEC 7810, Идентификационни карти. Физични характеристики, [6] Конструкция на картата	
		[Материали, от които се състои картата] Тахографските карти трябва да съответстват на стандарта ISO/IEC 7810, Идентификационни карти. Физични характеристики, [7] Материали, от които се състои картата	
		[Коравина на огъване] Тахографските карти трябва да съответстват на стандарта ISO/IEC 7810, Идентификационни карти. Физични характеристики, [8] Характеристики на картата, [8.1] Коравина на огъване	
		[Токсичност] Тахографските карти трябва да съответстват на стандарта ISO/IEC 7810, Идентификационни карти. Физични характеристики, [8] Характеристики на картата [8.3] Токсичност	
		[Устойчивост на химикали] Тахографските карти трябва да съответстват на стандарта ISO/IEC 7810, Идентификационни карти. Физични характеристики, [8] Характеристики на картата, [8.4] Устойчивост на химикали	
		[Устойчивост на картата] Тахографските карти трябва да съответстват на стандарта ISO/IEC 7810, Идентификационни карти. Физични характеристики, [8] Характеристики на картата, [8.5] Устойчивост на размерите на картата и температурно и влажностно измятане	

№	Изпитване	Описание	Съответни изисквания
		[Светлина] Тахографските карти трябва да съответстват на стандарта ISO/IEC 7810, Идентификационни карти. Физични характеристики, [8] Характеристики на картата, [8.6] Светлина	
		[Дълготрайност] Приложение 1B, глава 4.4, „Спецификации във връзка с околната среда и електрически спецификации“, 241) Тахографските карти трябва да могат да функционират правилно през период от пет години, ако се използват в рамките на спецификациите във връзка с околната среда и електрическите спецификации.	
		[Якост на разслояване] Тахографските карти трябва да съответстват на стандарта ISO/IEC 7810, Идентификационни карти. Физични характеристики, [8] Характеристики на картата, [8.8] Якост на разслояване	
		[Прилепване или блокиране] Тахографските карти трябва да съответстват на стандарта ISO/IEC 7810, Идентификационни карти. Физични характеристики, [8] Характеристики на картата, [8.9] Прилепване или блокиране	
		[Измятане] Тахографските карти трябва да съответстват на стандарта ISO/IEC 7810, Идентификационни карти. Физични характеристики, [8] Характеристики на картата, [8.11] Общо измятане на картата	
		[Устойчивост на топлина] Тахографските карти трябва да съответстват на стандарта ISO/IEC 7810, Идентификационни карти. Физични характеристики, [8] Характеристики на картата, [8.12] Устойчивост на топлина	

№	Изпитване	Описание	Съответни изисквания
		[Деформации на повърхността] Тахографските карти трябва да съответстват на стандарта ISO/IEC 7810, Идентификационни карти. Физични характеристики, [8] Характеристики на картата, [8.13] Деформации на повърхността	
		[Замърсяване] Тахографските карти трябва да съответстват на стандарта ISO/IEC 7810, Идентификационни карти. Физични характеристики, [8] Характеристики на картата, [8.14] Замърсяване и взаимодействие на компонентите на картата	
2.3	Механични изпитвания с вграден модул с чип	[Огъване] Тахографските карти трябва да съответстват на стандарта ISO/IEC 7810:2003/Amd. 1:2009, Идентификационни карти. Физични характеристики, Изменение 1: Критерии за карти, съдържащи интегрални схеми [9.2] Динамично напрежение на огъване Общ брой цикли на огъване: 4 000.	ISO/IEC 7810
		[Усукване] Тахографските карти трябва да съответстват на стандарта ISO/IEC 7810:2003/Amd. 1:2009, Идентификационни карти. Физични характеристики, Изменение 1: Критерии за карти, съдържащи интегрални схеми [9.3] Динамично напрежение на усукване Общ брой цикли на усукване: 4 000.	
3	**Модул**		
3.1	Модул	Модулът е корпусът на чипа и контактната повърхност. [Повърхностен профил] Тахографските карти трябва да съответстват на стандарта ISO/IEC 7816-1:2011, Идентификационни карти. Карти с интегрална(и) схема(и). Част 1: Карти с контакти. Физични характеристики [4.2] Повърхностен профил на контактите	ISO/IEC 7816

№	Изпитване	Описание	Съответни изисквания
		[Механична якост] Тахографските карти трябва да съответстват на стандарта ISO/IEC 7816-1:2011, Идентификационни карти. Карти с интегрална(и) схема(и). Част 1: Карти с контакти. Физични характеристики [4.3] Механична якост (на карта и контакти)	
		[Електрическо съпротивление] Тахографските карти трябва да съответстват на стандарта ISO/IEC 7816-1:2011, Идентификационни карти. Карти с интегрална(и) схема(и). Част 1: Карти с контакти. Физични характеристики [4.4] Електрическо съпротивление (на контактите)	
		[Размери] Тахографските карти трябва да съответстват на стандарта ISO/IEC 7816-2:2007, Идентификационни карти. Карти с интегрална(и) схема(и). Част 2: Карти с контакти. Размери и разположение на контактите [3] Размери на контактите	
		[Разположение] Тахографските карти трябва да съответстват на стандарта ISO/IEC 7816-2:2007, Идентификационни карти. Карти с интегрална(и) схема(и). Част 2: Карти с контакти. Размери и разположение на контактите [4] Брой и разположение на контактите При модулите със шест контакти, настоящото изискване за изпитване не се отнася за контакти „C4“ и „C8“.	
4	**Чип**		
4.1	Чип	[Работна температура] Чипът на тахографската карта трябва да може да функционира при околна температура в интервала между – 25 °C и + 85 °C.	241 до 244 Правило № 10 на ИКЕ на ООН ISO/IEC 7810 ISO/IEC 10373

№	Изпитване	Описание	Съответни изисквания
		[Температура и влажност] Приложение 1B, глава 4.4, „Спецификации във връзка с околната среда и електрически спецификации“, 241) Тахографските карти трябва да могат да функционират правилно при всички климатични условия, които нормално се наблюдават на територията на Общността, и в минимален температурен интервал от – 25 °C до + 70 °C, с краткотрайни и редки върхови стойности до + 85 °C, като „краткотрайни и редки“ означава продължителност под 4 часа и не повече от 100 пъти по време на живота на картата. Тахографските карти се подлагат в последователни стъпки на следните температури и влажности в посоченото време. След всяка стъпка тахографските карти се изпитват за електрическа функционалност. 1. Температура – 20 °C в продължение на 2 часа. 2. Температура +/– 0 °C в продължение на 2 часа. 3. Температура + 20 °C и 50 % относителна влажност в продължение на 2 часа. 4. Температура + 50 °C и 50 % относителна влажност в продължение на 2 часа. 5. Температура + 70 °C и 50 % относителна влажност в продължение на 2 часа. Температурата се увеличава с прекъсвания до + 85 °C и 50 % относителна влажност в продължение на 60 минути. 6. Температура 70 °C и 85 % относителна влажност в продължение на 2 часа. Температурата се увеличава с прекъсвания до + 85 °C и 85 % относителна влажност в продължение на 30 минути.	
		[Влажност] Приложение 1B, глава 4.4, „Спецификации във връзка с околната среда и електрически спецификации“, 242) Тахографските карти трябва да могат да функционират правилно при интервал на влажността от 10 % до 90 %.	
		[Електромагнитна съвместимост — EMC] Приложение 1B, глава 4.4 „Спецификации във връзка с околната среда и електрически спецификации“, 244) При функционирането си тахографските карти трябва да са в съответствие с Правило № 10 на ИКЕ на ООН по отношение на електромагнитната съвместимост.	

№	Изпитване	Описание	Съответни изисквания
		[Статично електричество] Приложение 1B, глава 4.4 „Спецификации във връзка с околната среда и електрически спецификации“, 244) При функционирането си тахографските карти трябва да бъдат защитени срещу електростатични разряди. Тахографските карти трябва да съответстват на стандарта ISO/IEC 7810:2003/Amd. 1:2009, Идентификационни карти. Физични характеристики, Изменение 1: Критерии за карти, съдържащи интегрални схеми [9.4] Статично електричество [9.4.1] Контактни карти с интегрална(и) схема(и) Изпитвателно напрежение: 4 000 V	
		[Рентгенови лъчи] Тахографските карти трябва да съответстват на стандарта ISO/IEC 7810:2003/Amd. 1:2009, Идентификационни карти. Физични характеристики, Изменение 1: Критерии за карти, съдържащи интегрални схеми [9.1] Рентгенови лъчи	
		[Ултравиолетова светлина] ISO/IEC 10373-1:2006, Идентификационни карти. Методи за изпитване. Част 1: Общи характеристики [5.11] Ултравиолетова светлина	
		[Триролково изпитване — 3-wheel] Тахографските карти трябва да съответстват на стандарта ISO/IEC 10373-1:2006/Amd. Идентификационни карти. Методи за изпитване. Част 1: Общи характеристики, Изменение 1 [5.22] ICC — Механична якост: Триролково изпитване за карти с интегрална(и) схема(и) с контакти	
		[„Обвивка“ на чипа — Wrapping] Тахографските карти трябва да съответстват на стандарта MasterCard CQM V2.03:2013 [11.1.3] R-L3-14-8: Изпитване за издържливостта на закрепването на чипа към тялото на картата чрез огъване на картата (wrapping test robustness) [13.2.1.32] TM-422: Механична надеждност: Изпитване на опаковката	

№	Изпитване	Описание	Съответни изисквания
4.2	Механични изпитвания на модула с чипа, вграден в тялото на картата -> също като в точка 2.3	[Огъване] Тахографските карти трябва да съответстват на стандарта ISO/IEC 7810:2003/Amd. 1:2009, Идентификационни карти. Физични характеристики, Изменение 1: Критерии за карти, съдържащи интегрални схеми [9.2] Динамично напрежение на огъване Общ брой цикли на огъване: 4 000. [Усукване] Тахографските карти трябва да съответстват на стандарта ISO/IEC 7810:2003/Amd. 1:2009, Идентификационни карти. Физични характеристики, Изменение 1: Критерии за карти, съдържащи интегрални схеми [9.3] Динамично напрежение на усукване Общ брой цикли на усукване: 4 000.	ISO/IEC 7810
5	**Изпитвания за спазване на протоколи**		
5.1	Отговор на инициализиране (ATR)	Проверява се съответствието на ATR	ISO/IEC 7816-3 TCS_14, TCS_17, TCS_18
5.2	T=0	Проверява се съответствието на протокола T = 0	ISO/IEC 7816-3 TCS_11, TCS_12, TCS_13, TCS_15
5.3	Избор на типа протокол (PTS)	Проверява се съответствието на командата PTS, като се преминава към T = 1от T = 0	ISO/IEC 7816-3 TCS_12, TCS_19, TCS_20, TCS_21
5.4	T=1	Проверява се съответствието на протокола T = 1	ISO/IEC 7816-3 TCS_11, TCS_13, TCS_16
6	**Структура на картата**		
6.1		Проверява се съответствието на записаната на картата структура на файловете, като се проверява наличието на задължителните файлове на картата, както и условията за достъп до тях	TCS_22 до TCS_28 TCS_140 до TCS_179
7	**Функционални изпитвания**		
7.1	Нормално функциониране	Проверява се поне веднъж всяко разрешено използване на всяка команда (напр. проверява се командата UPDATE BINARY с CLA = „00“, CLA = „0C“ и с различни параметри P1, P2 и Lc) Проверява се дали операциите действително са изпълнени в картата (напр.: чрез прочитане на файла, върху който е била изпълнена командата)	TCS_29 до TCS_139

№	Изпитване	Описание	Съответни изисквания
7.2	Съобщения за грешки	Изпробва се поне веднъж всяко съобщение за грешка (както е посочено в допълнение 2) за всяка команда. Изпробва се поне веднъж всяка типова (generic) грешка (с изключение на грешките за цялост „6400“, които се проверяват при сертифицирането за сигурност)	
7.3	Криптографска поредица (cypher suite) и стандартизирани домейн параметри		CSM_48, CSM_50
8	**Персонализиране**		
8.1	Визуално персонализиране	Приложение 1B, глава 4.1 „Видими данни“, 230) Лицевата страна трябва да съдържа: информация, специфична за издадената карта. Приложение 1B, глава 4.1 „Видими данни“, 231) Лицевата страна трябва да съдържа: дати с формат „дд/мм/гггг“ или „дд.мм.гггг“ (ден, месец, година). Приложение 1B, глава 4.1 „Видими данни“, 235) Тахографските карти трябва да имат следните елементи на защита на тялото на картата срещу подправяне и фалшифициране: — в зоната на снимката трябва да се припокриват фонът със защитни характеристики и снимката.	230, 231, 235

5. ИЗПИТВАНИЯ НА ВЪНШНОТО УСТРОЙСТВО ЗА GNSS

№	Изпитване	Описание	Съответни изисквания
1.	**Административен преглед**		
1.1	Документация	Коректност на документацията	
2.	**Визуално инспектиране на външното устройство за GNSS**		
2.1.	Съответствие с документацията		
2.2.	Идентификация/маркировки		224 до 226
2.3	Материали		219 до 223
3.	**Функционални изпитвания**		
3.1	Данни за идентифициране на датчика		98, 99
3.2	Свързване на модула за GNSS и бордовото устройство		123, 205

№	Изпитване	Описание	Съответни изисквания
3.3	Местоположение съгласно GNSS		36, 37
3.4	Интерфейс на бордовото устройство, когато приемникът за сигнали от GNSS е извън бордовото устройство		03
3.5	Криптографска поредица (cypher suite) и стандартизирани домейн параметри		CSM_48, CSM_50
4.	**Изпитания за въздействията на околната среда**		
4.1	Температура	Проверява се функционалността чрез следните изпитвания: Изпитване съгласно ISO 16750-4, глава 5.1.1.2: Изпитване за работа при ниска температура (72 часа при – 20 °C) Това изпитване е с позоваване на IEC 60068-2-1: Изпитване на въздействия на околната среда — Част 2-1: Изпитвания — Изпитване A: Студ Изпитване съгласно ISO 16750-4: Глава 5.1.2.2 Изпитване за работа при висока температура (72 часа при 70 °C) Това изпитване е с позоваване на IEC 60068-2-2: Основни процедури за изпитване на въздействия на околната среда; Част 2: Изпитвания; Изпитвания B: Суха топлина Изпитване съгласно ISO 16750-4: Глава 5.3.2: Бърза промяна на температурата при зададена продължителност на прехода (– 20 °C/70 °C, 20 цикъла, време на задържане при всяка от температурите 1 час) Възможно е да се проведат намален набор изпитвания (измежду посочените в раздел 3 на настоящата таблица) съответно при ниските температури, високите температури и температурните цикли	213
4.2	Влажност	Проверява се, че бордовото устройство може да понесе циклично изпитване на топлина във влажна среда съгласно IEC 60068-2-30, изпитване Db, със шест цикъла по 24 часа, като във всеки от тях температурата се изменя от + 25 °C до + 55 °C и относителната влажност е съответно 97 % при + 25 °C и 93 % при + 55 °C	214
4.3	Механични въздействия	1. Синусоидални вибрации. Проверява се, че бордовото устройство може да понесе синусоидни вибрации със следните характеристики: постоянно изместване, при честота между 5 и 11 Hz: максимум 10 mm постоянно ускорение, при честота между 11 и 300 Hz: 5 g Съответствието с това изискване с проверява чрез изпитване Fc по IEC 60068-2-6, с минимално времетраене на изпитването 3 × 12 часа (по 12 часа на координатна ос) Стандартът ISO 16750-3 не изисква да се провежда изпитване със синусоидални вибрации за устройства, намиращи се в отделна кабина на превозното средство (decoupled vehicle cab).	219

№	Изпитване	Описание	Съответни изисквания
		2. Случайни вибрации: Изпитване съгласно ISO 16750-3: Глава 4.1.2.8: Изпитване VIII: Търговски превозни средства (commercial vehicles) с отделна кабина Изпитване за случайни вибрации (Random vibration test), 10…2 000 Hz, вертикално средноквадратично отклонение 21,3 m/s^2, надлъжно средноквадратично отклонение 11,8 m/s^2, напречно средноквадратично отпклонение 13,1 m/s^2, 3 оси, по 32 часа за ос, включително температурен цикъл – 20…70 °C. Това изпитване е с позоваване на IEC 60068-2-64: Изпитване на въздействия на околната среда — Част 2-64: Изпитвания — Изпитване Fh: Вибрации, широколентови случайни, и указания 3. Удари: механичен удар с ускорение 3g, полусинусоидален, съгласно ISO 16750. Гореописаните изпитвания се извършват върху различни мостри на изпитваните съоръжения.	
4.4	Защита срещу вода и чужди тела	Изпитване съгласно ISO 20653: Пътни превозни средства. Степен на защита (IP код). Защита на електрическото оборудване срещу чужди обекти, вода и достъп (запазване на параметрите)	220, 221
4.5	Защита срещу пренапрежения	Проверява се, че бордовото устройство може да понесе захранващо напрежение както следва: при варианти за 24 V: 34 V при + 40 °C в продължение на 1 час при варианти за 12 V: 17 V при + 40 °C в продължение на 1 час (ISO 16750-2, глава 4.3)	216
4.6	Защита срещу обратна полярност	Проверява се, че бордовото устройство може да издържи на размяна на полюсите на своето електрическо захранване (ISO 16750-2, глава 4.7)	216
4.7	Защита срещу къси съединения	Проверява се, че входно/изходните сигнали са защитени срещу къси съединения към захранването и към масата (ISO 16750-2, глава 4.10)	216
5	**Изпитание за електромагнитна съвместимост (ЕМС)**		
5.1	Излъчени емисии и чувствителност към тях	Съответствие с Правило № 10 на ИКЕ на ООН	218

№	Изпитване	Описание	Съответни изисквания
5.2	Електростатичен разряд	Съответствие със стандарт ISO 10605:2008 + Техническа поправка: 2010 + AMD1:2014: +/– 4 kV за контактен разряд и +/– 8 kV за разряд през въздух	218
5.3	Чувствителност към преходни процеси по проводниците на захранването	При варианти за напрежение 24 V: съответствие със стандарт ISO 7637-2 + Правило № 10 на ИКЕ на ООН, Преработка 3: импулс 1a: Vs= – 450 V, Ri = 50 Ω импулс 2 a: Vs= + 37 V, Ri = 2 Ω импулс 2b: Vs= + 20 V, Ri = 0,05 Ω импулс 3 a: Vs= – 150 V, Ri = 50 Ω импулс 3b: Vs= + 150 V, Ri = 50 Ω импулс 4: Vs = – 16 V, Va = – 12 V, t6 = 100 ms импулс 5: Vs= + 120 V, Ri = 2,2 Ω, td = 250ms При варианти за напрежение 12 V: съответствие със стандарт ISO 7637-1 + Правило № 10 на ИКЕ на ООН, Преработка 3: импулс 1: Vs= – 75 V, Ri = 10 Ω импулс 2 a: Vs= + 37 V, Ri = 2 Ω импулс 2b: Vs= + 10 V, Ri = 0,05 Ω импулс 3 a: Vs= – 112 V, Ri = 50 Ω импулс 3b: Vs= + 75 V, Ri = 50 Ω импулс 4: Vs = – 6 V, Va = – 5 V, t6 = 100 ms импулс 5: Vs= + 65 V, Ri = 2,2 Ω, td = 250ms Импулс 5 се изпитва само за бордови устройства, предвидени за монтиране на превозни средства, които не разполагат с устройство за обща външна защита срещу повишено напрежение вследствие разкачане на акумулаторната батерия при зареждащ я алтернатор (protection against load dump) За примерни стойности на повишено напрежение вследствие разкачане на акумулаторната батерия при зареждащ я алтернатор, вижте стандарт ISO 16750-2, 4-то издание, глава 4.6.4.	218

6. ИЗПИТВАНИЯ НА УСТРОЙСТВОТО ЗА ВРЪЗКА ОТ РАЗСТОЯНИЕ

№	Изпитване	Описание	Съответни изисквания
1.	**Административен преглед**		
1.1	Документация	Коректност на документацията	
2.	**Визуално инспектиране**		
2.1.	Съответствие с документацията		
2.2.	Идентификация/маркировки		225, 226
2.3	Материали		219 до 223

№	Изпитване	Описание	Съответни изисквания
4.	**Изпитания за въздействията на околната среда**		
4.1	Температура	Проверява се функционалността чрез следните изпитвания: Изпитване съгласно ISO 16750-4, глава 5.1.1.2: Изпитване за работа при ниска температура (72 часа при – 20 °C) Това изпитване е с позоваване на IEC 60068-2-1: Изпитване на въздействия на околната среда — Част 2-1: Изпитвания — Изпитване A: Студ Изпитване съгласно ISO 16750-4: Глава 5.1.2.2: Изпитване за работа при висока температура (72 часа при 70 °C) Това изпитване е с позоваване на IEC 60068-2-2: Основни процедури за изпитване на въздействия на околната среда; Част 2: Изпитвания; Изпитвания B: Суха топлина Изпитване съгласно ISO 16750-4: Глава 5.3.2: Бърза промяна на температурата при зададена продължителност на прехода (– 20 °C/70 °C, 20 цикъла, време на задържане 1 час (?) при всяка от температурите) Възможно е да се проведат намален набор изпитвания (измежду посочените в раздел 3 на настоящата таблица) съответно при ниските температури, високите температури и температурните цикли	213
4.4	Защита срещу вода и чужди тела	Изпитване съгласно ISO 20653: Пътни превозни средства. Степен на защита (IP код). Защита на електрическото оборудване срещу чужди обекти, вода и достъп (целева стойност IP40)	220, 221
5	**Изпитание за електромагнитна съвместимост (EMC)**		
5.1	Излъчени емисии и чувствителност към тях	Съответствие с Правило № 10 на ИКЕ на ООН	218
5.2	Електростатичен разряд	Съответствие със стандарт ISO 10605:2008 + Техническа поправка:2010 + AMD1:2014: +/– 4 kV за контактен разряд и +/- 8 kV за разряд през въздух	218
5.3	Чувствителност към преходни процеси по проводниците на захранването	При варианти за напрежение 24 V: съответствие със стандарт ISO 7637-2 + Правило № 10 на ИКЕ на ООН, Преработка 3: импулс 1a: Vs = – 450 V, Ri=50 Ω импулс 2 a: Vs = + 37 V, Ri=2 Ω импулс 2b: Vs = + 20 V, Ri=0,05 Ω импулс 3 a: Vs = – 150 V, Ri=50 Ω импулс 3b: Vs = + 150 V, Ri=50 Ω импулс 4: Vs = – 16 V, Va = – 12 V, t6=100 ms импулс 5: Vs = + 120 V, Ri=2,2 Ω, td=250ms	218

№	Изпитване	Описание	Съответни изисквания
		При варианти за напрежение 12 V: съответствие със стандарт ISO 7637-1 + Правило № 10 на ИКЕ на ООН, Преработка 3: импулс 1: Vs = – 75 V, Ri=10 Ω импулс 2 a: Vs = + 37 V, Ri=2 Ω импулс 2b: Vs = + 10 V, Ri=0,05 Ω импулс 3 a: Vs = – 112 V, Ri=50 Ω импулс 3b: Vs = + 75 V, Ri=50 Ω импулс 4: Vs = – 6 V, Va = – 5 V, t6=100 ms импулс 5: Vs = + 65 V, Ri=2,2 Ω, td=250ms Импулс 5 се изпитва само за бордови устройства, предвидени за монтиране на превозни средства, които не разполагат с устройство за обща външна защита срещу повишено напрежение вследствие разкачане на акумулаторната батерия при зареждащ я алтернатор (protection against load dump) За примерни стойности на повишено напрежение вследствие разкачане на акумулаторната батерия при зареждащ я алтернатор, виж стандарт ISO 16750-2, 4-то издание, глава 4.6.4.	

7. ФУНКЦИОНАЛНИ ИЗПИТВАНИЯ ЗА РАЗПЕЧАТВАНЕ ВЪРХУ ХАРТИЕН НОСИТЕЛ

№	Изпитване	Описание	Съответни изисквания
1.	**Административен преглед**		
1.1	Документация	Коректност на документацията	
2	**Общи изпитвания**		
2.1	Брой знаци на ред	Визуално инспектиране на разпечатките.	172
2.2	Минимален размер на знаците	Визуално инспектиране на разпечатката и инспектиране на знаците.	173
2.3	Поддържани набори от символи	Печатащото устройство трябва да може да отпечатва символите, специфицирани в допълнение 1, глава 4, „Набори от символи“.	174
2.4	Дефиниране на разпечатките	Проверка на одобрението на типа на тахографа и визуално инспектиране на разпечатките	174
2.5	Четливост и идентифициране на разпечатките	Инспектиране на разпечатките Докладва се чрез доклади от изпитвания и протоколи от изпитвания от производителя. Всички хомологационни номера на тахографи, с които може да се използва съответната печатна хартия, са отбелязани върху хартията.	175, 177, 178
2.6	Добавяне на ръкописни бележки	Визуално инспектиране: Налично е поле за подпис на водача. Налични са полета за други ръкописни бележки.	180

№	Изпитване	Описание	Съответни изисквания
2.7	Допълнителни данни върху лицевата страна на хартията.	Върху лицевата и обратната страна на хартията могат да присъстват допълнителни данни и информация. Тези допълнителни данни и информация не трябва да пречат на четливостта на разпечатките. Визуално инспектиране.	177, 178
3	**Изпитвания за съхранение**		
3.1	Суха топлина	Предварителна подготовка: 16 часа при + 23°C ± 2°C/55 % ±3 % относителна влажност Среда за изпитването: 72 часа при +70 °C ± 2 °C; Възстановяване след изпитването: 16 часа при +23°C ± 2°C/55 % ±3 % относителна влажност	176, 178 IEC 60068-2-2-Bb
2.2	Топлина във влажна среда	Предварителна подготовка: 16 часа при +23°C ± 2°C/55 % ±3 % относителна влажност Среда за изпитването: 144 часа при + 55 °C ± 2°C/93 % ±3 % относителна влажност Възстановяване след изпитването: 16 часа при + 23°C ± 2° C/55 % ± 3 % относителна влажност	176, 178 IEC 60068-2-78-Cab
4	**Изпитвания на работна хартия**		
4.1	Устойчивост на влага на фона (хартията без отпечатване върху нея)	Предварителна подготовка: 16 часа при + 23°C ± 2°C/55 % ±3 % относителна влажност Среда за изпитването: 144 часа при +55 °C ± 2°C/93 % ±3 % относителна влажност Възстановяване: 16 часа при +23°C ± 2°C/55 % ±3 % относителна влажност	176, 178 IEC 60068-2-78-Cab
4.2	Пригодност за печатане	Предварителна подготовка: 24 часа при +40 °C ± 2°C/93 % ± 3 % относителна влажност Среда за изпитването: разпечатка, извършена при +23 ° C ± 2 °C Възстановяване: 16 часа при +23°C ± 2°C/55 % ±3 % относителна влажност	176, 178
4.3	Устойчивост на топлина	Предварителна подготовка: 16 часа при + 23°C ± 2°C/55 % ± 3 % относителна влажност Среда за изпитването: 2 часа при + 70 °C ± 2 °C; Възстановяване: 16 часа при +23°C ± 2°C/55 % ±3 % относителна влажност	176, 178 IEC 60068-2-2-Bb
4.4	Устойчивост на ниска температура	Предварителна подготовка: 16 часа при + 23°C ± 2°C/55 % ±3 % относителна влажност Среда за изпитването: 24 часа при – 20 °C ± 3 °C, сух студ Възстановяване: 16 часа при + 23°C ± 2°C/55 % ± 3 % относителна влажност	176, 178 ISO 60068-2-1-Ab

№	Изпитване	Описание	Съответни изисквания
4.5	Устойчивост на светлина	Предварителна подготовка: 16 часа при + 23°C ± 2°C/ 55 % ±3 % относителна влажност Среда за изпитването: 100 часа при осветеност 5 000 лукса и при + 23°C ± 2°C/55 % ±3 % относителна влажност Възстановяване: 16 часа при +23°C ± 2°C/55 % ±3 % относителна влажност	176, 178

Критерии за четливост за изпитванията 3.x и 4.x:

Четливостта на разпечатките е осигурена ако стойностите на оптичната плътност са в съответствие със следните гранични стойности:

Отпечатани знаци: минимум 1,0

Фон (хартия без отпечатване върху нея) максимум 0,2

Стойностите на оптичната плътност на съответните разпечатки трябва да се измерват в съответствие с DIN EN ISO 534.

Разпечатките не трябва да имат променени размери и трябва да остават ясно четливи.

8. ИЗПИТВАНИЯ ЗА ОПЕРАТИВНА СЪВМЕСТИМОСТ

№	Изпитване	Описание
9.1 Изпитвания за оперативна съвместимост между бордови устройства и тахографски карти		
1	Взаимно удостоверяване на автентичност	Проверява се дали взаимното удостоверяване на автентичност (authentication) между бордовото устройство и тахографската карта протича нормално
2	Изпитания за четене/записване	Върху бордовото устройство се изпълнява сценарий на типично действие. Сценарият трябва да е адаптиран към изпитвания тип карта и да включва записвания във възможно най-голям брой елементарни файлове (EF) в картата Чрез изтегляне на данните от бордовото устройство се проверява дали всички съответни записи са направени правилно. Чрез изтегляне на данните от картата се проверява дали всички съответни записи са направени правилно. Чрез дневни разпечатки се проверява дали всички съответни записи могат да бъдат прочетени правилно
9.2 Изпитвания за оперативна съвместимост между бордови устройства и датчици за движение		
1	Сдвояване	Проверява се дали сдвояването между бордовите устройства и датчиците за движение протича нормално
2	Изпитвания на действието	Върху датчика за движение се изпълнява сценарий на типично действие. Сценарият трябва да включва нормално действие и създаване на възможно най-много събития или неизправности. Чрез изтегляне на данните от бордовото устройство се проверява дали всички съответни записи са направени правилно. Чрез изтегляне на данните от картата се проверява дали всички съответни записи са направени правилно. Чрез дневна разпечатка се проверява дали всички съответни записи могат да бъдат прочетени правилно

№	Изпитване	Описание
9.3 Изпитвания за оперативна съвместимост между външни устройства за GNSS (в случаите, при които има такива устройства) и бордови устройства		
1	Взаимно удостоверяване на автентичност	Проверява се дали взаимното удостоверяване на автентичност (свързване) между външното устройство за GNSS и бордовото устройство протича нормално.
2	Изпитвания на действието	Върху външното устройство за GNSS се изпълнява сценарий на типично действие. Сценарият трябва да включва нормално действие и създаване на възможно най-много събития или неизправности. Чрез изтегляне на данните от бордовото устройство се проверява дали всички съответни записи са направени правилно. Чрез изтегляне на данните от картата се проверява дали всички съответни записи са направени правилно. Чрез дневна разпечатка се проверява дали всички съответни записи могат да бъдат прочетени правилно

Допълнение 10

ИЗИСКВАНИЯ ЗА СИГУРНОСТ

В настоящото допълнение са специфицирани изискванията за информационна сигурност по отношение на компонентите на интелигентните тахографски системи (тахографите от второ поколение).

SEC_001 Сертифициране за сигурност по Схемата за общите критерии се изисква за следните компоненти на интелигентната тахографска система:

— бордовото устройство,

— тахографската карта,

— датчика за движение,

— външното устройство за GNSS.

SEC_002 Минималните изисквания за информационна сигурност, на които трябва да отговаря всеки компонент, подлежащ на сертифициране за сигурност, се дефинират в защитен профил на компонента, в съответствие със Схемата за общите критерии.

SEC_003 За посочените по-долу четири защитни профила в съответствие с настоящото приложение Европейската комисия трябва да осигури те да бъдат спонсорирани, разработени, одобрени от държавните сертификационни органи по информационна сигурност, които са организирани в рамките на Съвместната интерпретационна работна група (Joint Interpretation Working Group — JIWG), която съдейства за взаимното признаване на сертификатите под егидата на Европейското споразумение за взаимно признаване на сертификатите за оценка на сигурността на информационните технологии (Agreement on Mutual Recognition of Information Technology Security Evaluation Certificates — SOGIS-MRA), както и регистрирани:

— Защитен профил за бордово устройство,

— Защитен профил за тахографска карта,

— Защитен профил за датчик за движение,

— Защитен профил за външно устройство за GNSS.

Защитният профил за бордово устройство трябва да се отнася за случаите, при които бордовият блок е проектиран да се използва със или без външно устройство за GNSS. В първия от тези два случая изискванията за сигурност за външното GNSS устройство се посочват в неговия защитен профил.

SEC_004 Производителите на компоненти трябва да уточняват и допълват съответния защитен профил, както е необходимо, без да изменят или изтриват съществуващи заплахи, цели, процедурни средства и спецификации за функции за обезпечаване на сигурност, така че да формулират цел за сигурност, спрямо която да кандидатстват за сертифициране за сигурност на съответния компонент.

SEC_005 По време на процеса на оценка трябва да бъде декларирано наличието на строго съответствие на такава специфична цел за сигурност със съответния защитен профил.

SEC_006 Нивото на сигурност на всеки защитен профил трябва да бъде EAL4, увеличено с компонентите за сигурност ATE_DPT.2 и AVA_VAN.5.

Допълнение 11

ОБЩИ МЕХАНИЗМИ ЗА СИГУРНОСТ

СЪДЪРЖАНИЕ

ПРЕАМБЮЛ

В настоящото допълнение са специфицирани механизмите за сигурност, които обезпечават:

— взаимно удостоверяване на автентичност между различни компоненти на тахографската система.

— поверителност, цялостност, автентичност и безотказно приемане на данните, предавани между различните компоненти на тахографската система или изтегляни от външни носители на информация.

Настоящото допълнение се състои от две части. В Част А са дефинирани механизмите за сигурност за тахографска система от първо поколение (цифров тахограф). В Част Б са дефинирани механизмите за сигурност за тахографска система от второ поколение (интелигентен тахограф).

Механизмите, специфицирани в Част А от настоящото допълнение, се прилагат ако поне един от компонентите на тахографската система, участващи в процес на взаимно удостоверяване на автентичност и/или прехвърляне на данни, е от първо поколение.

Механизмите, специфицирани в Част Б от настоящото допълнение, се прилагат ако и двата компонента на тахографската система, участващи в процес на взаимно удостоверяване на автентичност и/или прехвърляне на данни, са от второ поколение.

Допълнителна информация относно използването на компоненти от първо поколение в комбинация с компоненти от второ поколение е дадена в Допълнение 15.

ЧАСТ А

ТАХОГРАФСКА СИСТЕМА ОТ ПЪРВО ПОКОЛЕНИЕ

1. ВЪВЕДЕНИЕ

1.1. **Позовавания**

В настоящото допълнение са използвани позовавания на следните референтни документи:

SHA-1	National Institute of Standards and Technology (NIST). *FIPS Publication 180-1: Secure Hash Standard*. April 1995
PKCS1	RSA Laboratories. PKCS # 1: RSA Encryption Standard. Version 2.0. October 1998.
TDES	National Institute of Standards and Technology (NIST). *FIPS Publication 46-3*: *Data Encryption Standard*. Draft 1999.
TDES-OP	ANSI X9.52, Triple Data Encryption Algorithm Modes of Operation. 1998.
ISO/IEC 7816-4	Информационни технологии. Идентификационни карти. Карти с интегрална(и) схема(и) с контакти. Част 4: Вътрешно-отраслови команди за взаимен обмен. Първо издание: 1995 г. + Изменение 1: 1997 г..
ISO/IEC 7816-6	Информационни технологии. Идентификационни карти. Карти с интегрална(и) схема(и) с контакти. Част 6: Отраслови елементи от данни за взаимен обмен. Първо издание: 1996 г. + Поправка 1: 1998 г.
ISO/IEC 7816-8	Информационни технологии. Идентификационни карти. Карти с интегрална(и) схема(и) с контакти. Част 8: Отраслови команди за операции по сигурността. Първо издание:1999 г.
ISO/IEC 9796-2	Информационни технологии. Техники за сигурност. Схеми за електронен подпис, позволяващи възстановяване на съобщението. Част 2: Механизми, използващи хеш-функция. Първо издание: 1997 г.
ISO/IEC 9798-3	Информационни технологии. Техники за сигурност. Автентификация на обекта. Част 3: Механизми, използващи електронен подпис. Второ издание, 1998 г.
ISO 16844-3	Пътни превозни средства. Тахографски системи. Част 3: Интерфейс на датчика на движение.

1.2. **Означения и съкращения на термини**

В настоящото допълнение са използвани следните означения и съкращения на термини:

(K_a, K_b, K_c)	a key bundle for use by the Triple Data Encryption Algorithm (група от ключове, използвани в тройния алгоритъм за криптиране на данни),
CA	Certification Authority (удостоверяващ орган),
CAR	Certification Authority Reference (референтно означение на удостоверяващия орган),
CC	Cryptographic Checksum (криптографска контролна сума),
CG	Cryptogram (криптограма),
CH	Command Header (заглавна част на команда),
CHA	Certificate Holder Authorisation (оторизация на титуляря на сертификата),
CHR	Certificate Holder Reference (референтно означение на титуляря на сертификата).
D()	Decryption with DES (декриптиране с DES (Data Encryption Standard)),

DE	Data Element (елемент от данни),
DO	Data Object (обект от данни),
d	RSA private key, private exponent (частен ключ на RSA система, частен степенен показател),
e	RSA public key, public exponent (публичен ключ RSA система, публичен степенен показател),
E()	Encryption with DES (криптиране с DES),
EQT	Equipment (оборудване),
Hash()	Hash value, an output of *Hash* (хеш-стойност (стойност на сегментиране), изходен низ от хеширане),
Hash	*Hash* (хеш-функция),
KID	Key Identifier (идентификатор на ключ),
Km	TDES key. Master Key defined in ISO 16844-3 (ключ TDES, главен ключ, определен в стандарт ISO 16844 -3),
Km_{VU}	TDES key inserted in vehicle units (ключ TDES, въведен в бордови устройства),
Km_{WC}	TDES key inserted in workshop cards (ключ TDES, въведен в карти за монтаж и настройки),
m	message representative, an integer between 0 and *n*-1 (указател за представяне на съобщение, цяло число между 0 и n–1),
n	RSA keys, modulus (ключове RSA, модул (в модулно степенуване)),
PB	Padding Bytes (запълващи байтове),
PI	Padding Indicator byte (байт на индикатора за запълване (използван в криптограма за поверителни обекти от данни))
PV	Plain Value (открита стойност),
s	Signature representative, an integer between 0 and *n*-1 (указател за представяне на подпис, цяло число между 0 и n–1),
SSC	Send Sequence Counter (брояч на изпратени поредици),
SM	Secure Messaging (защитен обмен на съобщения),
TCBC	TDEA Cipher Block Chaining Mode of Operation (режим на работа чрез свързване на блокове от шифровани данни TDEA),
TDEA	Triple Data Encryption Algorithm (троен алгоритъм за криптиране на данни),
TLV	Tag Length Value (стойност на дължината на таг),
VU	Vehicle Unit (бордово устройство),
X.C	The certificate of user X issued by a certification authority (сертификатът на ползвателя X, издаден от сертифициращ орган),
X.CA	A certification authority of user X (сертифициращ орган на ползвателя X),
X.CA.PK $_{o}$ X.C	The operation of unwrapping a certificate to extract a public key. It is an infix operator, whose left operand is the public key of a certification authority, and whose right operand is the certificate issued by that certification authority. The outcome is the public key of the user X whose certificate is the right operand (Операция по разкриване съдържанието на сертификат с цел извличане на публичен ключ от него. Това е оператор, който е поставен между операнди, като операндът отляво е публичният ключ на даден сертифициращ орган, а операндът отдясно е сертификатът, издаден от този сертифициращ орган. Като резултат се получава публичният ключ на ползвателя X, чийто сертификат е операндът отдясно),
X.PK	RSA public key of a user X (публичен ключ RSA на ползвателя X),
X.PK[I]	RSA encipherment of some information I, using the public key of user X (криптиране RSA на някои информации I с помощта на публичния ключ на ползвателя X),
X.SK	RSA private key of a user X (частен ключ RSA на ползвателя X),
X.SK[I]	RSA encipherment of some information I, using the private key of user X (криптиране RSA на някои информации I с помощта на частния ключ на ползвателя X)
‘xx’	An Hexadecimal value (стойност в шестнадесетичната бройна система),
||	Concatenation operator (оператор за конкатенация).

2. КРИПТОГРАФСКИ СИСТЕМИ И АЛГОРИТМИ

2.1. **Криптографски системи**

CSM_001 Бордовите устройства и тахографските карти трябва да използват класическа криптографска система с публичен ключ RSA за предоставяне на следните механизми за сигурност:

— взаимно удостоверяване на автентичност между бордовите устройства и тахографските карти,

— маршрутизация на тройните ключове за сесия DES (Data Encryption Standard) между бордовите устройства и тахографските карти,

— електронен подпис за данните, изтегляни от бордовите устройства или от тахографските карти върху външни носители на информация.

CSM_002 Бордовите устройства и тахографските карти трябва да използват криптографска система с троен DES шифър със симетричен ключ за осигуряване на механизъм, който да гарантира целостта на данните при обмена на данни на ползвателя между бордовите устройства и тахографските карти, както и за осигуряване, в съответните случаи, на поверителност на обмена на данни между бордовите устройства и тахографските карти.

2.2. **Криптографски алгоритми**

2.2.1 *Алгоритъм RSA*

CSM_003 Алгоритъмът RSA се дефинира изцяло чрез следните отношения:

$$X.SK[m] = s = m^d \bmod n$$
$$X.PK[s] = m = s^e \bmod n$$

По-подробно писание на функцията RSA е дадено в референтния документ [PKCS1]. За целите на изчисленията за RSA, публичният степенен показател *e* представлява цяло число със стойност между 3 и n-1, отговарящо на условието gcd(e, lcm(p-1, q-1))=1.

2.2.2 *Алгоритъм за хеширане*

CSM_004 Механизмите за електронния подпис трябва да използват алгоритъма за хеширане SHA-1, така както е определен в референтния документ SHA-1.

2.2.3 *Алгоритъм за криптиране на данни*

CSM_005 Алгоритмите на база DES трябва да се използват при работен режим на свързване на блокове от шифровани данни.

3. КЛЮЧОВЕ И СЕРТИФИКАТИ

3.1. **Генериране и разпределение на ключове**

3.1.1 *Генериране и разпределение на ключове RSA*

CSM_006 Ключовете RSA се генерират на три йерархични функционални равнища:

— европейско равнище,

— равнище на държавата членка,

— равнище на вид оборудване.

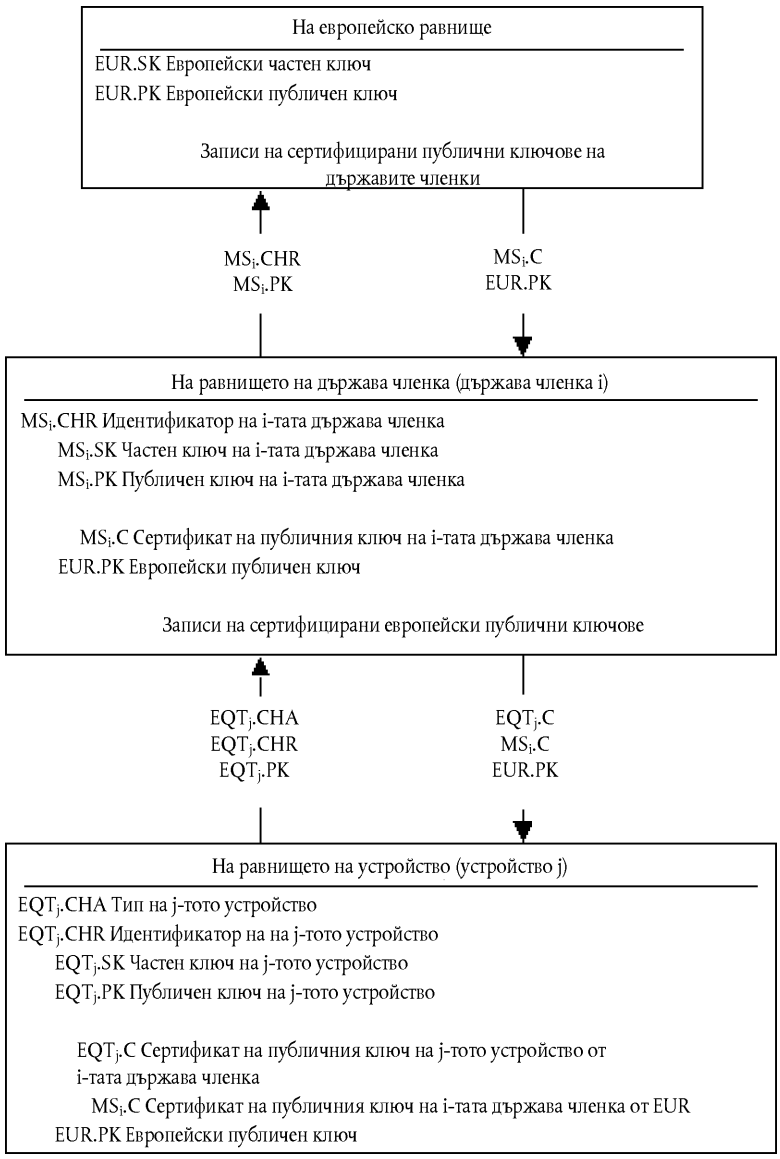
CSM_007 На европейското равнище се генерира само една двойка европейски ключове (EUR.SK и EUR.PK). Европейският частен ключ се използва за сертифицирането на публичните ключове на равнището на държавите членки. Трябва се съхраняват записи за всички сертифицирани ключове. Тези задачи се изпълняват от Европейски сертифициращ орган под контрола и отговорността на Европейската комисия.

CSM_008 На равнището на държава членка се генерира една двойка ключове за държавата членка (MS.SK и MS.PK). Публичните ключове на държавите членки трябва да бъдат сертифицирани от Европейския сертифициращ орган. Частният ключ на държавата членка се използва за сертифицирането на публичните ключове, които се въвеждат в оборудването (бордовото устройство или тахографската карта). Записите на всички сертифицирани публични ключове трябва да се съхраняват заедно с данните за идентифициране на оборудването, за което те са предназначени. Тези задачи се изпълняват от национален сертифициращ орган на държавата членка. Всяка държава членка има право да сменя периодично своята двойка ключове.

CSM_009 На равнището на оборудването се генерира и въвежда само една двойка ключове във всяко оборудване (EQT.SK и EQT.PK). Публичните ключове на оборудването трябва да бъдат сертифицирани от националния сертифициращ орган. Тези задачи могат да се изпълняват от производителите на оборудването, от изпълнителите на персонализацията на оборудването (equipment personalisers), или от органи на държавата членка. Тази двойка ключове се използва за операции във връзка с удостоверяването на автентичността, електронния подпис и криптирането.

CSM_010 Поверителността на частните ключове трябва да се запази при тяхното генериране, (евентуално) маршрутизиране и съхранение.

Движението на данните при този процес е обобщено на следната фигура:



3.1.2 *Ключове за контрол с RSA*

CSM_011 CSM_0113а целите на изпитванията на оборудване (включително изпитвания за оперативна съвместимост), Европейският сертифициращ орган генерира една различна европейска двойка контролни ключове и най-малко две двойки национални контролни ключове, чиито публични ключове се сертифицират с европейския частен контролен ключ. Производителите трябва да въвеждат в оборудването, което е в процес на сертифициране на типа, контролни ключове, сертифицирани чрез един от националните контролни ключове.

3.1.3 *Ключове за датчика за движение*

Поверителността на ключовете с троен DES шифър, описани по-долу, трябва да бъде запазена по подходящ начин при тяхното генериране, (евентуално) маршрутизиране и съхранение.

За да се даде възможност за поддържане на тахографски компоненти, отговарящи на стандарта ISO 16844, Европейският сертифициращ орган и националните сертифициращи органи на държавите членки трябва също да осигуряват следното:

CSM_036 Европейският сертифициращ орган генерира ключовете KmVU и KmWC, два независими и уникални ключа с троен DES шифър, както и Km по формулата: $Km = Km_{VU}$ XOR Km_{WC}. При поискване Европейският сертифициращ орган изпраща тези ключове, при спазване на подходящи защитни процедури, на сертифициращите органи на държавите членки.

CSM_037 Сертифициращите органи на държавите членки трябва:

— да използват ключа Km за криптиране на данните на датчици за движение, поискано от производителите на датчици за движение (данните за криптиране с ключа Km са определени в стандарт ISO 16844-3),

— да изпращат ключа Km_{VU} на производителите на бордови устройства, при спазване на подходящи защитни процедури, за да бъде този ключ въведен в бордови устройства,

— да осигуряват въвеждането на Km_{WC} във всички карти за монтаж и настройки (`SensorInstallationSecData` в елементарния файл `Sensor_Installation_Data`) по време на персонализацията на картата.

3.1.4 *Генериране и разпределение на сесийни T-DES ключове*

CSM_012 При процеса на взаимно удостоверяване на автентичността, бордовите устройства и тахографските карти трябва да генерират и обменят необходимите данни за изработването на общ сесиен T-DES ключ. Поверителността на този обмен на данни трябва да бъде защитена с механизъм за криптиране RSA.

CSM_013 При всички последващи криптографски операции този ключ трябва да се използва със защитен обмен на съобщения. Неговата валидност изтича в края на сесията (изваждане или инициализиране на картата) и/или след 240 употреби (една употреба на ключа = изпращане на команда към картата при защитен обмен на съобщения и съответният отговор).

3.2. **Ключове**

CSM_014 Ключовете RSA трябва да имат (независимо от равнището) следните дължини: модул *n* 1 024 бита, публичен степенен показател *e* максимум 64 бита, частен степенен показател *d* 1 024 бита.

CSM_015 Ключовете с троен DES шифър трябва да имат формата (K_a, K_b, K_a), където K_a и K_b са независими ключове с дължина 64 бита. Не се въвеждат никакви битове за откриване на грешка по четност.

3.3. **Сертификати**

CSM_016 Сертификатите с публични ключове RSA трябва да бъдат от типа „non self-descriptive“ („несамоописващи се“) и „card verifiable“(„проверими с карта“) (Справка: стандарт ISO/CEI 7816-8) ISO/IEC 7816-8

3.3.1 *Съдържание на сертификатите*

CSM_017 Сертификатите с публични ключове RSA трябва да съдържат посочените по-долу данни в следния ред:

Данни	Формат	Байтове	Забележки
CPI	INTEGER	1	Идентификатор на профила на сертификата (‘01’ за тази версия)
CAR	OCTET STRING	8	Референтно означение на сертифициращия орган
CHA	OCTET STRING	7	Оторизация на титуляря на сертификата
EOV	TimeReal	4	Изтичане на валидността на сертификата. Незадължително, може да се допълни с „FF“, ако не е използвано.
CHR	OCTET STRING	8	Референтно означение на титуляря на сертификата
n	OCTET STRING	128	Публичен ключ (модул)
e	OCTET STRING	8	Публичен ключ (публичен степенен показател)
		164	

Забележки:

1. „Идентификаторът на профила на сертификата“ (Certificate Profile Identifier — CPI) определя точната структура на даден сертификат за удостоверяване на автентичност. Той изпълнява функция на вътрешен идентификатор на оборудване в съответен списък на заглавни части (Headerlist), който описва конкатенацията на елементите от данни, съдържащи се в сертификата.

   Списъкът на заглавни части, свързан със съдържанието на този сертификат, има следния вид:

‘4D’	‘16’	‘5F 29’	‘01’	‘42’	‘08’	‘5F 4B’	‘07’	‘5F 24’	‘04’	‘5F 20’	‘08’	‘7F 49’	‘05’	‘81’	‘81 80’	‘82’	‘08’
Таг за разширен Headerlist	Дължина на Headerlist	Таг за идентификатор на профила на сертификата (CPI)	Дължина на CPI	Таг за CAR	Дължина на CAR	Таг за оторизация на титуляря на сертификата	Дължина на CHA	Таг за EOV	Дължина на EOV	Таг за CHR	Дължина на CHR	Таг за публичен ключ (конструиран)	Дължина на последващите обекти от данни	Таг на модула	Дължина на модула	Таг на публичния степенен показател	Дължина на публ. степенен показател

2. „Референтното означение на сертифициращия орган“ (CAR) е предназначено да идентифицира издалия сертификата орган по такъв начин, че елементът от данни да може да изпълнява едновременно функцията на идентификатор на органа за ключа, посочващ кой е сертифициращият орган, генерирал публичния ключ (за кодирането вж. по-долу „Идентификатор на ключ“).

3. „Оторизация на титуляря на сертификата“ (CHA) се издава за посочване на правата на титуляря на сертификата. Тя се състои от идентификатор на заявката за тахограф и от типа на оборудването, за което се отнася сертификатът (в зависимост от елемента от данни `EquipmentType`, за държава членка този идентификатор е ‘00’).

4. „Референтното означение на титуляря на сертификата“ (CHR) е предназначено да служи за уникално идентифициране на титуляря на сертификата по такъв начин, че елементът от данни да може да бъде използван в същото време и като идентификатор на предметен ключ, за означаване на публичния ключ на титуляря на сертификата.

5. Идентификаторите на ключове служат за уникално идентифициране на титуляря на сертификата или на сертифициращите органи. Те се кодират, както следва:

5.1. Оборудване (бордово устройство или карта):

Данни	Сериен номер на оборудването	Дата	Тип	Производител
Дължина	4 байта	2 байта	1 байт	1 байт
Стойност	Цяло число	Кодиране BCD мм гг	Специфични данни за производителя	Код на производителя

В случаите, при които става въпрос за бордово устройство, при исканията за сертификати е възможно производителят да знае или да не знае идентификационните данни на оборудването, в което ще бъдат въведени ключовете.

В първия случай производителят изпраща до сертифициращия орган в своята държава членка идентификационните данни на оборудването и публичния ключ. Сертификатът в такъв случай съдържа идентификационните данни на оборудването и производителят трябва да осигури въвеждането на ключовете и сертификата в съответното оборудване. Идентификаторът на ключа има указаната по-горе форма.

Във втория случай производителят трябва да идентифицира уникално всяко искане за сертификат и да изпрати до сертифициращия орган в своята държава членка тази идентификация и публичния ключ. В такъв случай сертификатът съдържа идентификацията на искането за сертификат. След инсталирането на ключ в оборудването производителят трябва да подаде до сертифициращия орган в своята държава членка обратна информация за определянето на ключ за оборудването (т.е. за идентификацията на искането за сертификат и за идентификацията на оборудването). Идентификаторът на ключа има указаната по-долу форма:

Данни	Сериен номер на искането за сертификат	Дата	Тип	Производител
Дължина	4 байта	2 байта	1 байт	1 байт
Стойност	Integer	Кодиране BCD мм гг	‘FF’	Код на производителя

5.2 Сертифициращ орган:

Данни	Идентификация на органа	Сериен номер на ключа	Допълнителна информация	Идентификатор
Дължина	4 байта	1 байт	2 байта	1 байт

Стойност	1 байт цифров код за националността 3 байта буквено-цифров код за националността	Integer	допълнително кодиране (специфично за сертифициращия орган) 'FF FF' ако не е използвано	'01'

Серийният номер на ключа се използва за разграничаване на различните ключове на дадена държава членка в случай, че ключът бъде променен.

6. Проверителите на сертификати трябва имплицитно да знаят, че сертифицираният публичен ключ е от тип RSA, който се използва за удостоверяване на автентичността, проверка и криптиране на електронен подпис при поверителни операции (сертификатът не съдържа никакъв идентификатор на обекта, който да го специфицира).

3.3.2 *Издадени сертификати*

CSM_018 Издаденият сертификат е електронен подпис с частично възстановяване на съдържанието на сертификата в съответствие със стандарт ISO/IEC 9796-2 (с изключение на неговото приложение A.4), допълнен с „Референтното означение на сертифициращия орган“ (Certification Authority Reference).

$$X.C = X.CA.SK['6A' \,||\, C_r \,||\, Hash(Cc) \,||\, 'BC'] \,||\, C_n \,||\, X.CAR$$

Със съдържание на сертификата = Cc = C_r || C_n

106 байта 58 байта

Забележки:

1. Дължината на този вид сертификат е 194 байта.

2. Референтното означение на сертифициращия орган (CAR), което е скрито от подписа, в същото време е прикрепено като допълнение към подписа, за да може публичният ключ на сертифициращия орган да бъде избран за извършване на проверката на сертификата.

3. Проверителят на сертификата трябва имплицитно да знае алгоритъма, използван от сертифициращия орган за подписване на сертификата.

4. Списъкът на заглавни части, свързан с този вид издаден сертификат, има следния вид:

'7F 21'	'09'	'5F 37'	'81 80'	'5F 38'	'3A'	'42'	'08'
Таг за проверим с карта сертификат (конструиран)	Дължина на последващите обекти от данни	Таг за подписа	Дължина на подписа	Таг за остатъка	Дължина на остатъка	Таг за CAR	Дължина на CAR

3.3.3 *Проверка и разкриване на съдържанието на сертификатите*

Проверката и разкриването на съдържанието на сертификатите се състои от проверка на подписа съгласно стандарт ISO/IEC 9796-2 и извличане на съдържанието на сертификата и на съдържащия се в сертификата публичен ключ: X.PK = X.CA.PKoX.C, както и от проверка на валидността на сертификата.

CSM_019 Това включва следните стъпки:

Проверка на подписа и извличане на съдържанието:

— От X.C, се извличат Sign., C_n' и CAR': X.C = Sign || C_n' || CAR'

128 байта 58 байта 8 байта

— От CAR' се избира публичният ключ на съответния сертифициращ орган (ако това не е било вече направено с други средства)

— Отваря се Sign с публичния ключ на сертифициращия орган: Sr'= X.CA.PK [Sign],

— проверява се дали Sr' започва с '6A' и завършва с 'BC'

— изчисляват се C_r' и H' както следва: Sr' = '6 A' || C_r' || H' || 'BC'

106 байта 20 байта

— Възстановява се съдържанието на сертификата C' = C_r' || C_n',

— проверява се *Hash*(C') = H'

Ако резултатите от проверките са положителни, сертификатът е истински и съдържанието му е C'.

Проверява се валидността. От C':

— проверява се датата на изтичане на валидността (ако има такава),

От C' се извлича и се запаметява публичният ключ, идентификаторът на ключа, оторизацията на титуляря на сертификата и датата на изтичане на валидността:

— X.PK = *n* || *e*

— X.KID = CHR,

— X.CHA = CHA,

— X.EOV = EOV

4. МЕХАНИЗЪМ ЗА ВЗАИМНО УДОСТОВЕРЯВАНЕ НА АВТЕНТИЧНОСТТА

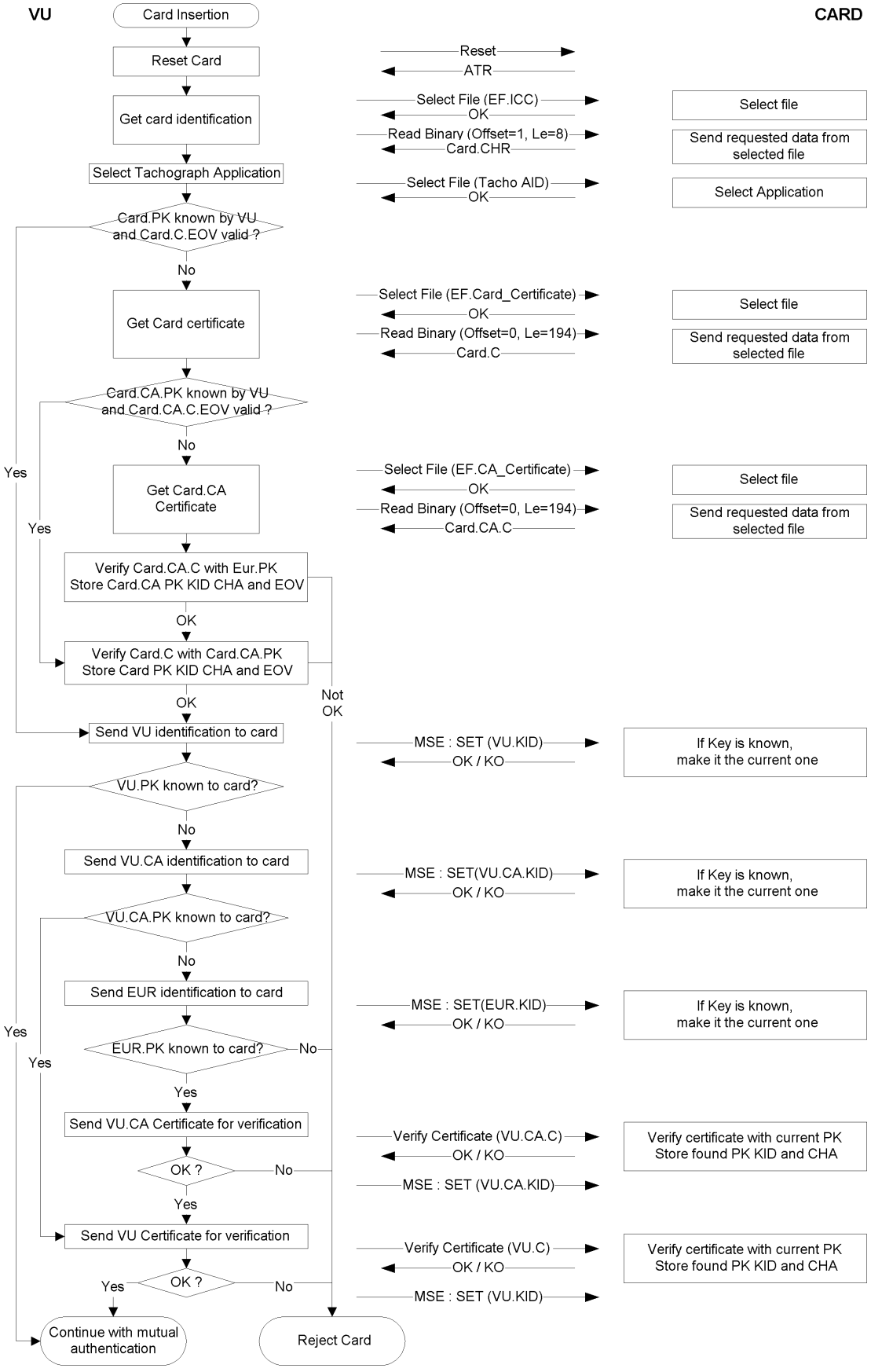
Взаимното удостоверяване на автентичността между картите и бордовите устройства се основава на следния принцип:

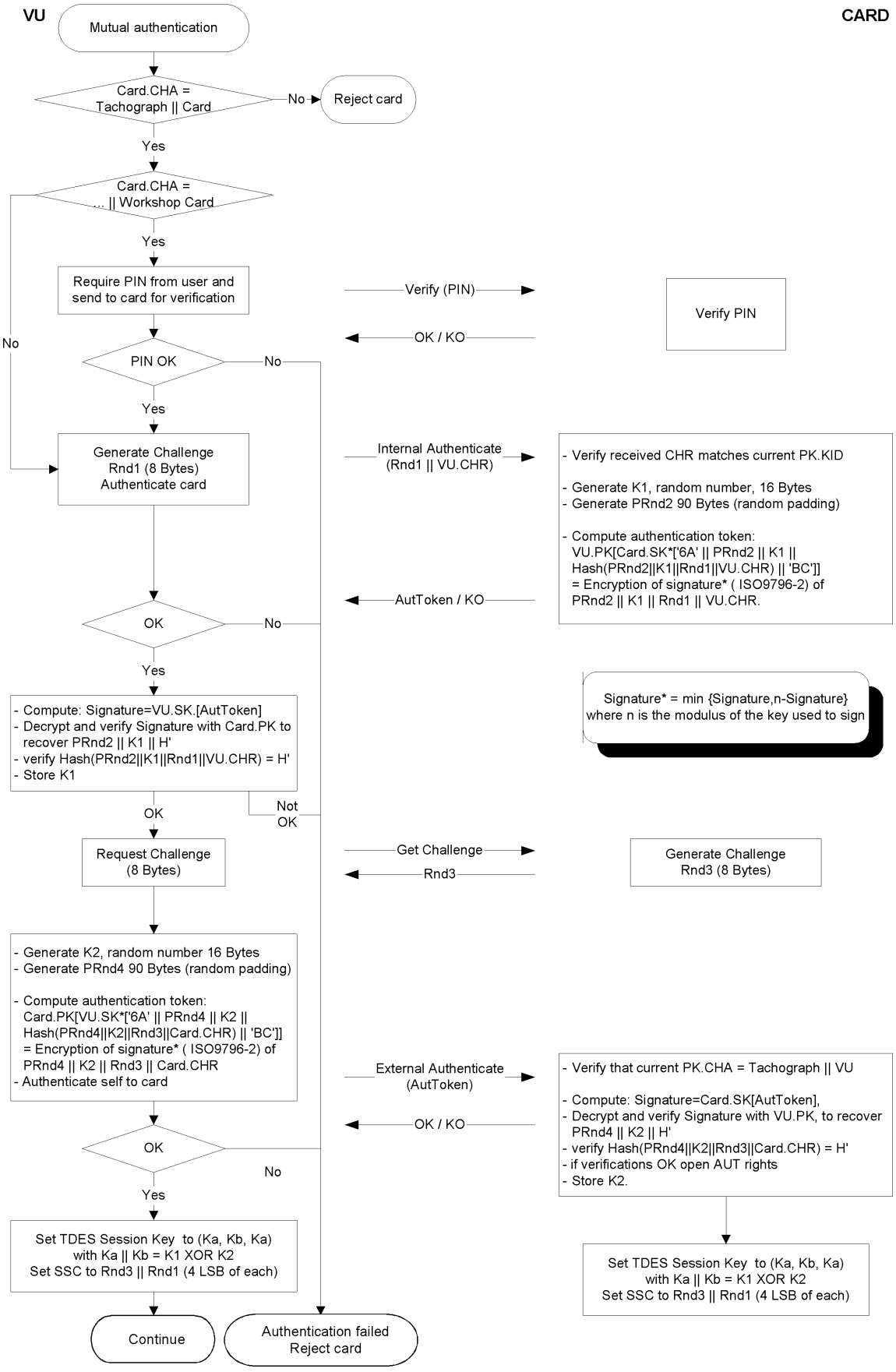
Всяка от страните трябва да демонстрира на другата, че притежава двойка валидни ключове, като публичният ключ, който е позволил тяхното сертифициране от национален сертифициращ орган, на свой ред е сертифициран от европейския сертифициращ орган.

Това демонстриране се състои в подписване с частния ключ на случайно число, изпратено от другата страна, която трябва да възстанови изпратеното случайно число при проверката на този подпис.

Механизмът се задейства от бордовото устройство при вкарване на карта в него. Той започва с размяна на сертификатите и разкриването на съдържанието на публичните ключове и завършва с определянето на ключ на сесията.

CSM_020 Използва се следният протокол (стрелките указват обменените команди и данни (вж. допълнение 2)):




VU
CARD
Mutual authentication
Card.CHA = Tachograph || Card
No
Reject card
Yes
Card.CHA = ... || Workshop Card
Yes
Require PIN from user and send to card for verification
Verify (PIN)
Verify PIN
OK / KO
No
PIN OK
No
Yes
Generate Challenge Rnd1 (8 Bytes) Authenticate card
Internal Authenticate (Rnd1 || VU.CHR)
- Verify received CHR matches current PK.KID
- Generate K1, random number, 16 Bytes
- Generate PRnd2 90 Bytes (random padding)
- Compute authentication token: VU.PK[Card.SK*['6A' || PRnd2 || K1 || Hash(PRnd2||K1||Rnd1||VU.CHR) || 'BC']] = Encryption of signature* (ISO9796-2) of PRnd2 || K1 || Rnd1 || VU.CHR.
AutToken / KO
OK
No
Yes
Signature* = min {Signature,n-Signature} where n is the modulus of the key used to sign
- Compute: Signature=VU.SK.[AutToken]
- Decrypt and verify Signature with Card.PK to recover PRnd2 || K1 || H'
- verify Hash(PRnd2||K1||Rnd1||VU.CHR) = H'
- Store K1
Not OK
OK
Request Challenge (8 Bytes)
Get Challenge
Rnd3
Generate Challenge Rnd3 (8 Bytes)
- Generate K2, random number 16 Bytes
- Generate PRnd4 90 Bytes (random padding)
- Compute authentication token: Card.PK[VU.SK*['6A' || PRnd4 || K2 || Hash(PRnd4||K2||Rnd3||Card.CHR) || 'BC']] = Encryption of signature* (ISO9796-2) of PRnd4 || K2 || Rnd3 || Card.CHR
- Authenticate self to card
External Authenticate (AutToken)
- Verify that current PK.CHA = Tachograph || VU
- Compute: Signature=Card.SK[AutToken],
- Decrypt and verify Signature with VU.PK, to recover PRnd4 || K2 || H'
- verify Hash(PRnd4||K2||Rnd3||Card.CHR) = H'
- if verifications OK open AUT rights
- Store K2.
OK / KO
OK
No
Yes
Set TDES Session Key to (Ka, Kb, Ka) with Ka || Kb = K1 XOR K2
Set SSC to Rnd3 || Rnd1 (4 LSB of each)
Set TDES Session Key to (Ka, Kb, Ka) with Ka || Kb = K1 XOR K2
Set SSC to Rnd3 || Rnd1 (4 LSB of each)
Continue
Authentication failed Reject card

5. МЕХАНИЗМИ ЗА ПОВЕРИТЕЛНОСТ, ЦЯЛОСТНОСТ И УДОСТОВЕРЯВАНЕ НА АВТЕНТИЧНОСТТА ПРИ ОБМЕН НА ДАННИ МЕЖДУ БОРДОВО УСТРОЙСТВО И КАРТА

5.1. **Защитен обмен на съобщения**

CSM_021 Цялостността при обмен на данни между бордово устройство и карти трябва да бъде опазвана чрез използване на защитен обмен на съобщения в съответствие с референтните документи [ISO/IEC 7816-4] и [ISO/IEC 7816-8].

CSM_022 Ако се налага защита на данните при тяхното прехвърляне, необходимо е към обектите от данни, изпращани в рамките на командата или отговора, да се добави обект от данни, представляващ криптографска контролна сума. Криптографската контролна сума се проверява от получателя на данните.

CSM_023 Криптографската контролна сума за данните, изпратени в рамките на дадена команда, трябва да включва заглавната част на командата, както и всички изпратени обекти от данни (=>CLA = '0C', и всички обекти от данни трябва да бъдат оградени с тагове, в които b1=1).

CSM_024 Ако отговорът не съдържа поле за данни, байтовете за състояние/информация в него трябва да бъдат защитени с криптографска контролна сума.

CSM_025 Криптографските контролни суми трябва да са с дължина 4 байта.

Така че при използване на защитен обмен на съобщения, командите и отговорите трябва да имат следната структура:

Използваните обекти от данни представляват частичен набор от обектите от данни за защитен обмен на съобщения, описани в ISO/IEC 7816-4:

Таг	Мнемоничен код	Значение
'81'	T_{PV}	Открита стойност (Plain Value), некодирана по BER-TVL (която трябва да бъде защитена с криптографска контролна сума)
'97'	$\mathbf{T_{LE}}$	Стойност на Le в незащитена от неоторизиран достъп команда (която трябва да бъде защитена с криптографска контролна сума)
'99'	T_{SW}	Информация за състоянието (която трябва да бъде защитена с криптографска контролна сума)
'8E'	T_{CC}	Криптографска контролна сума
'87'	$T_{PI\ CG}$	Байт на индикатора за запълването || Криптограма (открита стойност, некодирана в BER-TVL)

При дадена незащитена двойка от команда и отвор:

Заглавна част на командата				Тяло на командата		
CLA	INS	P1	P2	[L_c на поле]	[Поле за данни]	[L_e на поле]
четири байта				Байтове L, означени като B_1 до B_L		

Тяло на отговора	Завършваща част на отговора	
[Поле за данни]	SW1	SW2
Байтове данни L_r	Два байта	

Съответната защитена двойка от команда и отговор е:

Защитена от неоторизиран достъп команда:

Заглавна част на командата (CH)				Тяло на командата										
CLA	INS	P1	P2	[L_c на новото поле]	[Ново поле за данни]									[L_e на новото поле]
‘OC’				Дължина на новото поле за данни	T_{PV}	L_{PV}	PV	T_{LE}	L_{LE}	L_e	T_{CC}	L_{CC}	CC	‘00’
					‘81’	L_c	Поле за данни	‘97’	‘01’	L_e	‘8E’	‘04’	CC	

Данни, които се включват в контролната сума = CH || PB || T_{PV} || L_{PV} || PV || T_{LE} || L_{LE} || L_e || PB

PB = допълващи байтове (80 .. 00) съгласно ISO-IEC 7816-4 и ISO 9797, метод 2.

PV и LE на обекта от данни (DO) присъстват единствено ако незащитената команда съдържа съответстващи данни.

Защитен отговор:

1. Случай, когато полето за данни в отговора не е празно и не се нуждае от защита с цел поверителност:

Тяло на отговора						Завършваща част на отговора
[Ново поле за данни]						Нови SW1 SW2
T_{PV}	L_{PV}	PV	T_{CC}	L_{CC}	CC	
‘81’	L_r	Поле за данни	‘8E’	‘04’	CC	

Данни, които се включват в контролната сума = T_{PV} || L_{PV} || PV || PB

2. Случай, когато полето за данни на отговора не е празно и се нуждае от защита с цел поверителност:

Тяло на отговора						Завършваща част на отговора
[Ново поле за данни]						Нови SW1 SW2
$T_{PI\ CG}$	$L_{PI\ CG}$	PI CG	T_{CC}	L_{CC}	CC	
‘87’		PI || CG	‘8E’	‘04’	CC	

Данни, които се маршрутизират чрез CG: некодирани с BER-TLV данни и допълващи байтове.

Данни, които се включват в контролната сума = $T_{PI\ CG}$ || $L_{PI\ CG}$ || PI CG || PB

3. Случай, когато полето за данни на отговора е празно:

Тяло на отговора						Завършваща част на отговора
[Ново поле за данни]						Нови SW1 SW2
T_{SW}	L_{SW}	SW	T_{CC}	L_{CC}	CC	
‘99’	‘02’	Нови SW1 SW2	‘8E’	‘04’	CC	

Данни, които се включват в контролната сума = T_{SW} || L_{SW} || SW || PB

5.2. **Третиране на грешки при защитен обмен на съобщения**

CSM_026 Когато тахографската карта при интерпретирането на дадена команда разпознае грешка при защитен обмен на съобщения, необходимо е байтовете за състоянието да бъдат върнати без защитен обмен. В съответствие с ISO/IEC 7816-4, за посочване на грешки при защитен обмен на съобщения са определени следните байтове за състояние:

‘66 88’: Неуспешна проверка на криптографската контролна сума,

‘69 87’: Липса на очаквани обекти от данни за защитен обмен,

‘69 88’: Неверни обекти от данни за защитен обмен.

CSM_027 Когато тахографската карта върне байтове за състояние без посочени обекти от данни за защитен обмен (SM DOs) или с погрешен обект от данни за защитен обмен (SM DO), бордовото устройство трябва да прекрати сесията.

5.3. **Алгоритъм за изчисляване на криптографските контролни суми**

CSM_028 Криптографските контролни суми се съставят с използване на подробни кодове за автентификация на съобщенията (retail MACs), в съответствие със стандарт ANSI X9.19, с използване на DES:

— Начален стадий: Първоначалният контролен блок y0 е E(Ka, SSC).

— Последващ стадий: Контролните блокове y1, .., yn се изчисляват с използване на Ka.

— Краен стадий: Криптографската контролна сума се изчислява въз основа на последния контролен блок yn, както следва: E(Ka, D(Kb, yn)).

където съкращението E() означава криптиране с DES, а съкращението D() означава декриптиране с DES.

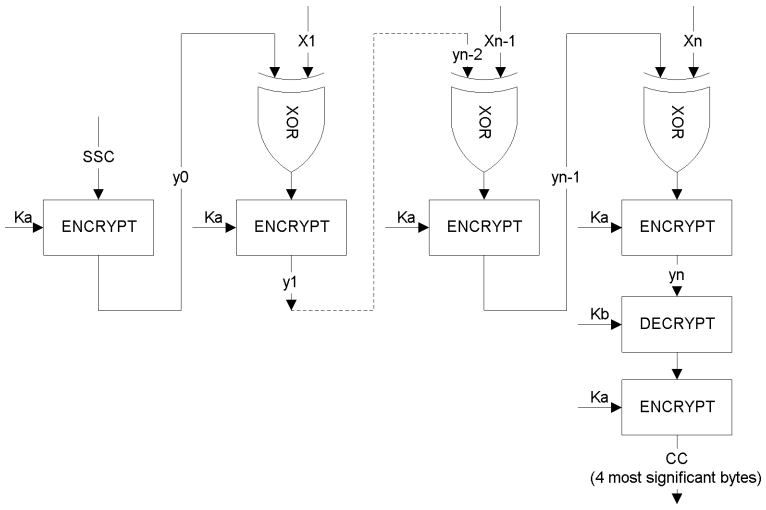
Прехвърлят се четирите най-старши байта от криптографската контролна сума.

CSM_029 При процедурата на договаряне на ключ се инициира броячът на изпратените поредици (SSC) по следния начин:

Начален SSC: Rnd3 (4-те най-младши байта) || Rnd1 (4-те най-младши байта).

CSM_030 Броячът на изпратените поредици се увеличава с 1 при всяко изчисляване на MAC (т.е. SSC за SSC след първата команда е началният SSC + 1 и SSC след първия отговор е SSC + 2).

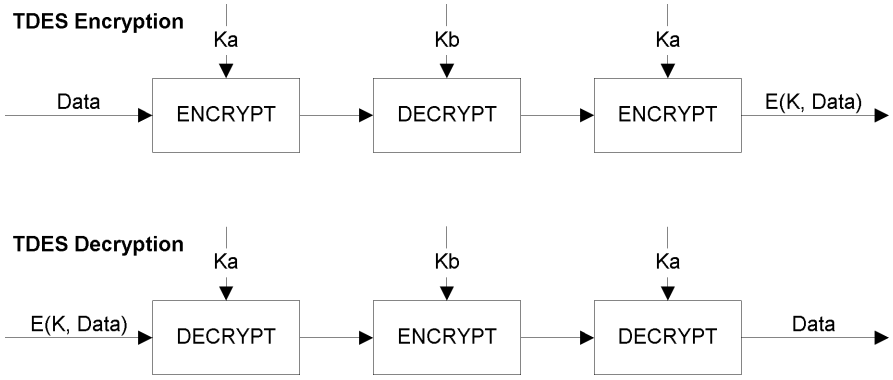
Процедурата по изчисляването на подробния MAC е показана на следната фигура:



5.4. Алгоритъм за изчисление на криптограмите за поверителни обекти от данни

CSM_031 Тези криптограми се изчисляват с използване на TDEA в работен режим TCBC, съгласно референтните документи [TDES] и [TDES-OP] и с нулев вектор като блок на началната стойност.

Прилагането на ключове в TDES е показано на следната фигура:



6. МЕХАНИЗМИ ЗА ИЗТЕГЛЯНЕ НА ДАННИ С ЕЛЕКТРОННИ ПОДПИСИ

CSM_032 Специализираното интелигентно устройство (IDE) записва във физически файл данните, прехвърлени от съответното оборудване (бордово устройство или карта) в рамките на една сесия на изтегляне на данни. Този файл трябва да съдържа сертификатите MS_i.C и EQT.C. Файлът съдържа електронни подписи на блоковете данни, както е специфицирано в допълнение 7 „Протоколи за изтегляне на данни“.

CSM_033 За електронните подписи на изтеглените данни трябва да се използва схема за електронни подписи с допълнение, така че при съответно желание изтеглените данни да могат да се четат без каквото и да е дешифриране.

6.1. Генериране на подписи

CSM_034 Генерирането от оборудването на електронни подписи на данните трябва да следва схемата за електронни подписи с допълнение, дефинирана в референтния документ [PKCS1] с хеш-функцията SHA-1:

Подпис = EQT.SK[‘00’ || ‘01’ || *PS* || ‘00’ || DER(SHA-1(Data))]

PS = Допълващ низ от октети със стойност ‘FF’, така че дължината да стане 128.

DER(SHA-1(M)) е кодирането на идентификатора на алгоритъма на хеш-функцията и хеш-стойността в стойност ASN.1 от типа DigestInfo (разграничени правила за кодиране):

‘30’||‘21’||‘30’||‘09’||‘06’||‘05’||‘2B’||‘0E’||‘03’||‘02’||‘1A’||‘05’||‘00’||‘04’||‘14’||Хеш-стойност.

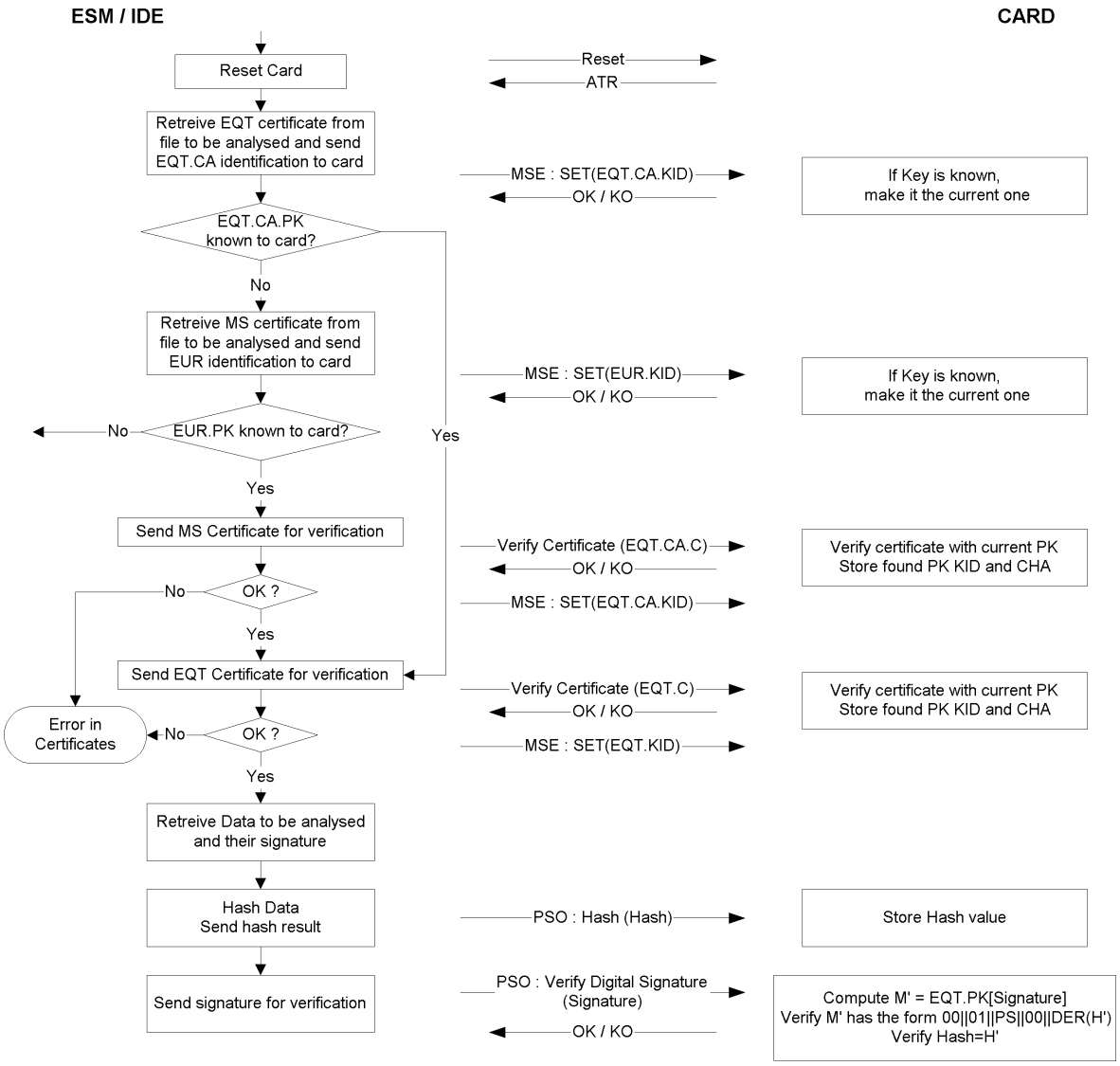
6.2. Проверка на подписите

CSM_035 При проверката на електронните подписи на изтеглените данни трябва да се следва схемата за електронни подписи с допълнение, дефинирана в референтния документ [PKCS1] с функцията за хеширане SHA-1.

Необходимо е европейският публичен ключ EUR.PK да бъде познат на проверителя по независим път и проверителят да има доверие в него.

В следната таблица е илюстриран протоколът, който може да бъде следван от специализирано интелигентно устройство (IDE) с вложена в него контролна карта за проверка на цялостността на данните, изтеглени и съхранени на външен носител на информация (ESM). Контролната карта се използва за дешифриране на електронните подписи. В такъв случай тази функция може да не е въведена в IDE.

Оборудването, което е изтеглило и подписало подлежащите на анализ данни, е означено със съкращението EQT.



ЧАСТ Б

ТАХОГРАФСКА СИСТЕМА ОТ ВТОРО ПОКОЛЕНИЕ

7. ВЪВЕДЕНИЕ

7.1. **Позовавания**

В настоящото допълнение се използват позовавания на следните референтни документи:

AES	National Institute of Standards and Technology (NIST), FIPS PUB 197: Advanced Encryption Standard (AES), November 26, 2001
DSS	National Institute of Standards and Technology (NIST), FIPS PUB 186-4: Digital Signature Standard (DSS), July 2013
ISO 7816-4	ISO/IEC 7816-4, Идентификационни карти. Карти с интегрална(и) схема(и). Част 4: Организация, сигурност и команди за обмен. Трето издание, 2013-04-15
ISO 7816-8	ISO/IEC 7816-8, Идентификационни карти. Карти с интегрална(и) схема(и). Част 8: Команди за операции по сигурността Второ издание 2004-06-01
ISO 8825-1	ISO/IEC 8825-1 Информационна технология. Правила за кодиране на ASN.1. Спецификация на основни (BER), канонични (CER) и разграничени (DER) правила за кодиране. Четвърто издание, 2008-12-15
ISO 9797-1	Информационни технологии. Техники за сигурност. Кодове за удостоверяване на автентичността на съобщението (MACs). Част 1: Механизми, използващи блоков шифър. Второ издание, 2011-03-01
ISO 10116	ISO/IEC 10116, Информационни технологии. Техники за сигурност. Режими ма работа, използващи *n*-битов блоков шифър. Трето издание, 2006-02-01
ISO 16844-3	ISO/IEC 16844-3, Пътни превозни средства. Тахографски системи. Част 3: Интерфейс на датчика на движение. Първо издание, 2004 г., включително Техническа поправка, 1.2006 г.
RFC 5480	Elliptic Curve Cryptography Subject Public Key Information, March 2009
RFC 5639	Elliptic Curve Cryptography (ECC) — Brainpool Standard Curves and Curve Generation, 2010
RFC 5869	HMAC-based Extract-and-Expand Key Derivation Function (HKDF), May 2010
SHS	National Institute of Standards and Technology (NIST), FIPS PUB 180-4: Secure Hash Standard, March 2012
SP 800-38B	National Institute of Standards and Technology (NIST), Special Publication 800-38B: Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, 2005
TR-03111	BSI Technical Guideline TR-03111, Elliptic Curve Cryptography, version 2.00, 2012-06-28

7.2. **Означения и съкращения**

В настоящото допълнение са използвани следните означения и съкращения на термини:

AES	Advanced Encryption Standard (усъвършенстван стандарт за криптиране)
CA	Certificate Authority (сертифициращ орган)
CAR	Certificate Authority Reference (референтно означение на сертифициращия орган)
CBC	Cipher Block Chaining (mode of operation) (свързване на блокове от шифровани данни (работен режим))

CH	Command Header (заглавна част на команда)
CHA	Certificate Holder Authorisation (оторизация на титуляря на сертификата)
CHR	Certificate Holder Reference (референтно означение на титуляря на сертификата)
CV	Constant Vector (константен вектор)
DER	Distinguished Encoding Rules (разграничени правила за кодиране)
DO	Data Object (обект от данни)
DSRC	Dedicated Short Range Communication (специализирана връзка (или съобщителна система) с малък обсег на действие)
ECC	Elliptic Curve Cryptography (криптография по елиптична крива)
ECDSA	Elliptic Curve Digital Signature Algorithm (алгоритъм за електронни подписи по елиптична крива)
ECDH	Elliptic Curve Diffie-Hellman (key agreement algorithm) (елиптична крива Diffie-Hellman — алгоритъм за договаряне на ключ)
EGF	External GNSS Facility (външно устройство за GNSS)
EQT	Equipment (оборудване)
IDE	Intelligent Dedicated Equipment (специализирано интелигентно устройство)
K_M	Motion Sensor Master Key, allowing the pairing of a Vehicle Unit to a Motion Sensor (главен ключ за датчика за движение, даващ възможност за сдвояване на бордовото устройство към датчика за движение)
$K_{M\text{-}VU}$	Key inserted in vehicle units, allowing a VU to derive the Motion Sensor Master Key if a workshop card is inserted into the VU (ключ, въвеждан в бордовите устройства, даващ възможност на съответното бордово устройство да изведе главния ключ (Master Key) на датчика за движение, ако в бордовото устройство бъде вкарана карта за монтаж и настройки)
$K_{M\text{-}WC}$	Key inserted in workshop cards, allowing a VU to derive the Motion Sensor Master Key if a workshop card is inserted into the VU (ключ, въвеждан в картите за монтаж и настройки, даващ възможност на съответното бордово устройство да изведе главния ключ на датчика за движение, ако в бордовото устройство бъде вкарана карта за монтаж и настройки)
MAC	Message Authentication Code (код за автентифициране на съобщение)
MoS	Motion Sensor (датчик за движение)
MSB	Most Significant Bit (най-старши бит)
PKI	Public Key Infrastructure (инфраструктура с публичен ключ)
RCF	Remote Communication Facility (устройство за връзка от разстояние)
SSC	Send Sequence Counter (брояч на изпратени поредици)
SM	Secure Messaging (защитен обмен на съобщения)
TDES	Triple Data Encryption Standard (троен DES — симетричен ключ, който изпълнява стандарта за криптиране на данни DES три пъти с различни ключове)
TLV	Tag Length Value (стойност на дължината на таг)
VU	Vehicle Unit (бордово устройство)
X.C	The public key certificate of user X (сертификатът на публичен ключ на ползвателя X)
X.CA	The certificate authority that issued the certificate of user X (сертифициращият орган, издал сертификата на ползвателя X)
X.CAR	The certificate authority reference mentioned in the certificate of user X (референтното означение на сертифициращия орган, посочено в сертификата на ползвателя X)
X.CHR	The certificate holder reference mentioned in the certificate of user X (референтното означение на титуляря на сертификата, посочено в сертификата на ползвателя X)
X.PK	Public key of user X (публичен ключ на ползвателя X)
X.SK	Private key of user X (частен ключ на ползвателя X)
$X.PK_{eph}$	Ephemeral public key of user X (краткотраен (ephemeral) публичен ключ на ползвателя X)
$X.SK_{eph}$	Ephemeral private key of user X (краткотраен (ephemeral) частен ключ на ползвателя X)
‘xx’	A hexadecimal value (шестнадесетична стойност)
||	Concatenation operator (оператор за конкатенация)

7.3. **Определения**

Определенията на използваните в настоящото допълнение термини са включени в раздел I от приложение 1B.

8. КРИПТОГРАФСКИ СИСТЕМИ И АЛГОРИТМИ

8.1. **Криптографски системи**

CSM_38 Бордовите устройства и тахографските карти трябва да използват класическа базираща се на елиптична крива криптографска система с публичен ключ за предоставяне на следните механизми за сигурност:

— взаимно удостоверяване на автентичност между бордово устройство и карта,

— договаряне на AES сесийни ключове между бордово устройство и карта,

— осигуряване на автентичност, цялостност и безотказно приемане на данните, изтегляни от бордовите устройства или от тахографските карти върху външни носители на информация.

CSM_39 Бордовите устройства и външните устройства за GNSS трябва да използват класическа базираща се на елиптична крива криптографска система с публичен ключ за предоставяне на следните механизми за сигурност:

— свързване на бордово устройство и външно GNSS устройство,

— взаимно удостоверяване на автентичност между бордово устройство и външно GNSS устройство,

— договаряне на AES сесийни ключове между бордово устройство и външно GNSS устройство.

CSM_40 Бордовите устройства и тахографските карти трябва да използват класическа базираща се на AES симетрична криптографска система за предоставяне на следните механизми за сигурност:

— осигуряване на автентичност и цялостност на данните, обменяни между бордово устройство и тахографска карта,

— в съответните случаи, осигуряване на поверителност на данните, обменяни между бордово устройство и тахографска карта.

CSM_41 Бордовите устройства и външните устройства за GNSS трябва да използват класическа базираща се на AES симетрична криптографска система за предоставяне на следните механизми за сигурност:

— осигуряване на автентичност и цялостност на данните, обменяни между бордово устройство и тахографска карта.

CSM_42 Бордовите устройства и датчиците за движение трябва да използват класическа базираща се на AES симетрична криптографска система за предоставяне на следните механизми за сигурност:

— сдвояване на бордово устройство и датчик за движение,

— взаимно удостоверяване на автентичност между бордово устройство и датчик за движение,

— осигуряване на поверителност на данните, обменяни между бордово устройство и датчик за движение.

CSM_43 Бордовите устройства и контролните карти трябва да използват класическа базираща се на AES симетрична криптографска система за предоставяне на следните механизми за сигурност:

— осигуряване на поверителност, автентичност и цялостност на данните, предавани между бордово устройство и контролна карта,

Забележки:

— По-точно казано, данните се предават от бордово устройство към дистанционно разпитващо устройство под контрола на инспектор, като се използва устройство за връзка от разстояние, което може да е вътрешно или външно за бордовото устройство, вж. допълнение 14. Дистанционното разпитващо устройство обаче изпраща получените данни на контролна карта за дешифриране и валидиране на автентичността. От гледна точка на сигурността, устройството за връзка от разстояние и дистанционното разпитващо устройство са изцяло прозрачни.

— Същите механизми за сигурност, които се изпълняват от контролната карта, се предоставят и от картата за монтаж и настройки по отношение на интерфейса за DSRC. Това дава възможност на съответния сервиз да валидира правилното функциониране на интерфейса за връзка от разстояние на дадено бордово устройство, включително и неговата сигурност. За повече информация вж. раздел 9.2.2.

8.2. **Криптографски алгоритми**

8.2.1 *Симетрични алгоритми*

CSM_44 Бордовите устройства, тахографските карти, датчиците за движение и външните устройства за GNSS трябва да поддържат алгоритъма AES, както е дефиниран в [AES], с дължина на ключовете 128, 192 и 256 бита.

8.2.2 *Асиметрични алгоритми и стандартизирани домейн параметри*

CSM_45 Бордовите устройства, тахографските карти и външните устройства за GNSS трябва да поддържат криптография по елиптична крива с размер на ключовете 256, 384 и 512/521 бита.

CSM_46 Бордовите устройства, тахографските карти и външните устройства за GNSS трябва да поддържат алгоритъма за подписи ECDSA, както е специфициран в [DSS].

CSM_47 Бордовите устройства, тахографските карти и външните устройства за GNSS трябва да поддържат алгоритъма за договаряне на ключ ECKA-EG, както е специфициран в [TR 03111].

CSM_48 Бордовите устройства, тахографските карти и външните устройства за GNSS трябва да поддържат всички стандартизирани домейн параметри, специфицирани по-долу в таблица 1 за криптография по елиптична крива.

Таблица 1

Стандартизирани домейн параметри

Наименование	Размер (битове)	Референтно означение	Идентификатор на обект (Object Identifier)
NIST P-256	256	[DSS], [RFC 5480]	`secp256r1`
BrainpoolP256r1	256	[RFC 5639]	`brainpoolP256r1`
NIST P-384	384	[DSS], [RFC 5480]	`secp384r1`
BrainpoolP384r1	384	[RFC 5639]	`brainpoolP384r1`
BrainpoolP512r1	512	[RFC 5639]	`brainpoolP512r1`
NIST P-521	521	[DSS], [RFC 5480]	`secp521r1`

Забележка: идентификаторите на обекти, споменати в последната колона на таблица 1, са специфицирани съответно в [RFC 5639] за кривите Brainpool и в [RFC 5480] за кривите NIST.

Пример 1: идентификаторът на обекти на кривата BrainpoolP256r1 е

```
{iso(1)
        identified-organization(3) teletrust(36) algorithm(3)
  signaturealgorithm(3) ecSign(2) ecStdCurvesAndGeneration (8)
                              ellipticCurve(1) versionOne(1) 7}.
```

Или ако се използва означаване с употреба на точки: `1.3.36.3.3.2.8.1.1.7.`

Пример 2: идентификаторът на обекти на кривата NIST P е

```
{iso(1) identified-organization(3) certicom(132) curve(0) 34}.
```

Или ако се използва означаване с употреба на точки: `1.3.132.0.34.`

8.2.3 *Алгоритми за хеширане*

CSM_49 Бордовите устройства и тахографските карти трябва да поддържат алгоритмите SHA-256, SHA-384 и SHA-512, специфицирани в [SHS].

8.2.4 *Криптографски поредици*

CSM_50 При симетричния алгоритъм се използват съвместно асиметричен алгоритъм и/или алгоритъм за хеширане, така че да формират протокол за сигурност, като съответните дължини на ключовете и хеш размери трябва да бъдат (приблизително) с еднаква сила (equal strength). Разрешените криптографски поредици са показани в таблица 2:

Таблица 2

Разрешени криптографски поредици

Идентификатор на криптографската поредица	Размер на ключа ECC (битове)	Размер на ключа AES (битове)	Алгоритъм за хеширане	Дължина на кода за автентифициране на съобщения (MAC, байтове)
CS#1	256	128	SHA-256	8
CS#2	384	192	SHA-384	12
CS#3	512/521	256	SHA-512	16

Забележка: Размерите на ECC ключове от 512 бита и 521 бита се считат за равни по сила за всички цели в рамките на настоящото допълнение.

9. КЛЮЧОВЕ И СЕРТИФИКАТИ

9.1. **Двойки от асиметрични ключове и сертификати на публични ключове**

9.1.1 *Общи положения*

Забележка: описаните в настоящия раздел ключове се използват за взаимно удостоверяване на автентичност и за защитен обмен на съобщения между бордови устройства и тахографски карти, както и между бордови устройства и външни устройства за GNSS. Тези процеси са описани подробно в глава 10 и глава 11 от настоящото допълнение.

CSM_51 В рамките на Европейската система за интелигентни тахографи, двойките ECC ключове и съответните сертификати се генерират и управляват на три функционални йерархични равнища:

— европейско равнище,

— равнище на държавата членка,

— равнище на вид оборудване.

CSM_52 В цялата Европейска система за интелигентни тахографи публичните и частните ключове и сертификати трябва да бъдат генерирани, управлявани и съобщавани по стандартизирани и сигурни методи.

9.1.2 *Европейско равнище*

CSM_53 На европейското равнище се генерира само една уникална двойка ECC ключове, с означение EUR. Тя се състои от частен ключ (EUR.SK) и публичен ключ (EUR.PK). Тази двойка ключове формира двойката основни ключове (root key pair) на цялата инфраструктура за публични ключове на Европейската система за интелигентни тахографи. Тази задача се изпълнява от Европейския орган за основни сертификати (European Root Certificate Authority — ERCA), който е под управлението и отговорността на Европейската комисия.

CSM_54 ERCA използва европейския частен ключ за подписване на (самоподписан) основен сертификат (root certificate) на европейския публичен ключ и да съобщава този европейски основен сертификат на всички държави членки.

CSM_55 При поискване ERCA използва европейския частен ключ за подписване на сертификатите на държавите членки. Задължение на ERCA е да съхранява архивни записи за всички подписани сертификати за публичен ключ на държави членки.

CSM_56 Както е показано на фигура 1 в раздел 9.1.7, на всеки 17 години ERCA трябва да генерира нова европейска двойка основни ключове. Когато ERCA генерира нова европейска двойка основни ключове, тя трябва да създаде нов самоподписан основен сертификат за новия европейски публичен ключ. Периодът на валидност на даден европейски основен сертификат е 34 години и 3 месеца.

Забележка: Въвеждането на нова двойка основни ключове означава също, че ERCA ще генерира нов главен ключ (master key) на датчика за движение и нов главен ключ за DSRC, вж. раздели 9.2.1.2 и 9.2.2.2.

CSM_57 Преди генерирането на нова европейска двойка основни ключове, ERCA трябва да направи анализ за необходимата криптографска сила на новата двойка ключове, като се има предвид че тя следва да запази своята сигурност в следващите 34 години. Ако това се окаже необходимо, ERCA трябва да премине към използване на по-силна криптографска поредица от използваната до този момент, както е специфицирано в CSM_50.

CSM_58 Когато генерира нова европейска двойка основни ключове, ERCA трябва да създаде свързващ сертификат за новия европейски публичен ключ и да го подпише с предходния европейски частен ключ. Периодът на валидност на свързващия сертификат е 17 години. Това е показано също на фигура 1 в раздел 9.1.7.

Забележка: Тъй като свързващият сертификат съдържа публичен ключ на ERCA от поколение *X* и е подписан с частен ключ на ERCA от поколение *X-1*, свързващият сертификат предоставя на оборудването с криптиране от поколение *X-1* метод, по който да се доверява на оборудване с криптиране от поколение *X*.

CSM_59 От момента когато стане валиден нов сертификат за основни ключове, ERCA трябва вече да не използва частния ключ от двойка основни ключове за каквото и да е предназначение.

CSM_60 Във всеки момент във времето ERCA трябва да разполага със следните криптографски ключове и сертификати:

— Текущата двойка ключове EUR и съответния сертификат

— Всички предходни сертификати EUR, използвани за проверка на сертификатите на сертифициращите органи на държавите членки (MSCA), които продължават да са валидни

— Свързващи сертификати за всички поколения EUR сертификати освен за първото

9.1.3 *Равнище на държава членка*

CSM_61 На равнището на държава членка, всички държави членки, от които се изисква да подписват сертификати за тахографски карти, трябва да генерират една или повече уникални двойки ключове ECC с обозначението MSCA_Card. Всички държави членки, от които се изисква да подписват сертификати за външни устройства за GNSS или за бордови устройства, трябва да генерират допълнително една или повече уникални двойки ключове ECC с обозначението MSCA_VU-EGF.

CSM_62 Задачата за генериране на двойки ключове на държава членка се изпълнява от сертифициращия орган на държавата членка (MSCA). Когато даден MSCA генерира двойка ключове на държава членка, той изпраща публичния ключ на Европейския орган за основни сертификати (ERCA), за да получи съответния подписан от ERCA сертификат на държава членка.

CSM_63 MSCA избира силата на двойка ключове на държава членка така, че тя да е равна на силата на европейската основна двойка ключове, използвана за подписване на съответния сертификат на държавата членка.

CSM_64 Когато съществува двойка ключове MSCA_VU-EGF, тя се състои от частен ключ MSCA_VU-EGF.SK и публичен ключ MSCA_VU-EGF.PK. MSCA трябва да използва частния ключ MSCA_VU-EGF.SK изключително само за подписване на сертификатите на публични ключове на външни устройства за GNSS и на бордови устройства.

CSM_65 Всяка двойка ключове MSCA_Card се състои от частен ключ MSCA_Card.SK и публичен ключ MSCA_Card.PK. MSCA използва частния ключ MSCA_Card.SK изключително само за подписване на сертификатите на публични ключове на тахографски карти.

CSM_66 MSCA трябва да съхранява архивни записи за всички подписани сертификати за бордови устройства, сертификати за външни GNSS устройства и сертификати за карти, заедно с идентификационните данни на оборудването, за което е предназначен всеки сертификат.

CSM_67 Периодът на валидност на сертификат MSCA_VU-EGF е 17 години и 3 месеца. Периодът на валидност на сертификат MSCA_Card е 7 години и 1 месеца.

CSM_68 Както е показано на фигура 1 в раздел 9.1.7, частният ключ от двойка ключове MSCA_VU-EGF и частният ключ от двойка ключове MSCA_Card са с период на използване две години.

CSM_69 След края на периода на използване съответният MSCA трябва вече да не използва за каквото и да е предназначение частния ключ от двойка ключове MSCA_VU-EGF. Също така, след края на периода на използване съответният MSCA трябва вече да не използва за каквото и да е предназначение частния ключ от двойка ключове MSCA_Card.

CSM_70 Във всеки момент във времето MSCA трябва да разполага със следните криптографски ключове и сертификати:

— Текущата двойка ключове MSCA_Card и съответния сертификат

— Всички предходни сертификати MSCA_Card, използвани за проверка на сертификатите на тахографски карти, които продължават да са валидни

— Текущият сертификат EUR, необходим за проверка на текущия сертификат на MSCA

— Всички предходни сертификати EUR, необходими за проверка на всички сертификати на MSCA, които продължават да са валидни

CSM_71 Ако от даден MSCA се изисква да подписва сертификати за външни устройства за GNSS или за бордови устройства, той трябва да разполага също и със следните ключове и сертификати:

— Текущата двойка ключове MSCA_VU-EGF и съответния сертификат

— Всички предходни публични ключове MSCA_VU-EGF, използвани за проверка на сертификатите на външни устройства за GNSS и на бордови устройства, които продължават да са валидни

9.1.4 *Равнище на съответното оборудване: бордови устройства*

CSM_72 За всяко бордово устройство трябва да бъдат генерирани две уникални двойки ключове ECC с обозначения съответно VU_MA и VU_Sign. Тази задача се изпълнява от производителите на бордови устройства. Когато бъде генерирана двойка ключове за бордово устройство, генерилата ключовете страна трябва да изпрати публичния ключ на MSCA в своята държава на пребиваване, за да получи съответен сертификат VU, подписан от MSCA. Частният ключ трябва да се използва само от бордовото устройство.

CSM_73 Сертификатите VU_MA и VU_Sign на дадено бордово устройство трябва да имат една и съща дата на влизане в сила.

CSM_74 Производителят на бордови устройства избира силата на двойка ключове на съответното бордово устройство така, че тя да е равна на силата на двойката ключове на MSCA, използвана за подписване на съответния сертификат на бордово устройство.

CSM_75 Всяко бордово устройство трябва да използва своята двойка ключове VU_MA, състояща се от частен ключ VU_MA.SK и публичен ключ VU_MA.PK изключително само за удостоверяване на автентичността на бордовото устройство по отношение на тахографските карти и външните устройства за GNSS, както е специфицирано в раздел 10.3 и раздел 11.4 от настоящото допълнение.

CSM_76 Всяко бордово устройство трябва да може да генерира двойки краткотрайни (ephemeral) ключове за ECC и трябва да използва дадена двойка краткотрайни (ephemeral) ключове изключително само за извършване на договаряне на сесиен ключ с тахографска карта или с външно устройство за GNSS, както е специфицирано в раздел 10.4 и раздел 11.4 от настоящото допълнение.

CSM_77 Всяко бордово устройство трябва да използва частния ключ VU_Sign.SK от своята двойка ключове VU_Sign изключително само за подписване на изтеглени файлове с данни, както е специфицирано в глава 14 от настоящото допълнение. Съответният публичен ключ VU_Sign.PK трябва да бъде използван изключително само за проверяване на подписите, създадени от бордовото устройство.

CSM_78 Както е показано на фигура 1 в раздел 9.1.7, периодът на валидност на сертификат VU_MA е 15 години и 3 месеца. Периодът на валидност на сертификат VU_Sign също е 15 години и 3 месеца.

Забележки:

— Удълженият период на валидност на сертификата VU_Sign дава възможност на бордовото устройство да създава валидни подписи върху изтеглени данни през първите три месеца след изтичането на сертификата, както се изисква съгласно Регламент (ЕС) № 581/2010.

— Удълженият период на валидност на сертификата VU_MA дава възможност на бордовото устройство да удостовери автентичността на контролна карта или на фирмена карта на превозвач през първите три месеца след изтичането на сертификата, така че да е възможно да се извърши изтегляне на данни.

CSM_79 След изтичането на съответния сертификат, бордовото устройство трябва да не използва за каквото и да е предназначение частния ключ от двойката ключове VU.

CSM_80 Двойките ключове VU (освен краткотрайните двойки ключове) и съответните сертификати на дадено бордово устройство не трябва да се заменят или обновяват в работна среда (in the field) след като бордовото устройство е пуснато в експлоатация.

Забележки:

— Това изискване не се отнася за двойките краткотрайни (ephemeral) ключове, тъй като нова двойка краткотрайни ключове се създава всеки път, когато се прави удостоверяване на автентичността на чип и се извършва договаряне на сесиен ключ, вж. раздел 10.4. Да се има предвид, че краткотрайните ключове нямат съответни сертификати.

— Настоящото изискване не ограничава възможността за замяна на двойки статични ключове VU при модернизация или поправка в сигурна среда, контролирана от производителя на бордовото устройство.

CSM_81 При пускането си в експлоатация бордовите устройства трябва да съдържат следните криптографски ключове и сертификати:

— Частния ключ VU_MA и съответния сертификат

— Частния ключ VU_Sign и съответния сертификат

— Сертификата MSCA_VU-EGF, съдържащ публичния ключ MSCA_VU-EGF.PK, който се използва за проверяване на сертификата VU_MA и на сертификата VU_Sign

— Сертификата EUR, съдържащ публичния ключ EUR.PK, който се използва за проверяване на сертификата MSCA_VU-EGF

— Ако съществува — сертификата EUR, чийто период на валидност непосредствено предшества този сертификат EUR, който се използва за проверяване на сертификата MSCA_VU-EGF

— Ако съществува — свързващия сертификат, който дава връзка между тези два сертификата EUR

CSM_82 В допълнение към криптографските ключове и сертификатите, посочени в CSM_81, бордовите устройства трябва да съдържат също ключовете и сертификатите, специфицирани в част A от настоящото допълнение, даващи възможност на бордовото устройство да взаимодейства с тахографски карти от първо поколение.

9.1.5 *Равнище на вид оборудване: Тахографски карти*

CSM_83 За всяка тахографска карта трябва да бъде генериран една уникална двойка ключове ECC, обозначена като Card_MA. Допълнително трябва да бъде генерирана втора уникална двойка ключове, обозначена като Card_Sign, за всяка карта на водач и всяка карта за монтаж и настройки. Тази задача може да бъде изпълнявана от производителите на карти или от персонализаторите на карти. Когато бъде генерирана двойка ключове за карта, генерираната ключовете страна трябва да изпрати публичния ключ на MSCA в своята държава на пребиваване, за да получи съответен картов сертификат, подписан от MSCA. Частният ключ трябва да се използва само от тахографската карта.

CSM_84 Сертификатите Card_MA и Card_Sign на дадена карта на водач или карта за монтаж и настройки трябва да имат една и съща дата на влизане в сила.

CSM_85 Производителят на картата или нейният персонализатор избира силата на двойка ключове на съответната карта така, че тя да е равна на силата на двойката ключове на MSCA, използвана за подписване на съответния картов сертификат.

CSM_86 Всяка тахографска карта трябва да използва своята двойка ключове Card_MA, състояща се от частен ключ Card_MA.SK и публичен ключ Card_MA.PK изключително само за извършване на взаимно удостоверяване на автентичността и договаряне на сесийни ключове с бордови устройства, както е специфицирано в раздел 10.3 и раздел 10.4 от настоящото допълнение.

CSM_87 Всяка карта на водач или карта за монтаж и настройки трябва да използва частния ключ Card_Sign. SK от своята двойка ключове Card_Sign изключително само за подписване на изтеглени файлове с данни, както е специфицирано в глава 14 от настоящото допълнение. Съответният публичен ключ Card_Sign.PK трябва да бъде използван изключително само за проверяване на подписите, създадени от картата.

CSM_88 Периодът на валидност на сертификат Card_MA е както следва:

— За карти на водач: 5 години

— За фирмени карти на превозвач: 2 години

— За контролни карти: 2 години

— За карти за монтаж и настройки: 1 година

CSM_89 Периодът на валидност на сертификат Card_Sign е както следва:

— За карти на водач: 5 години и 1 месец

— За карти за монтаж и настройки: 1 година и 1 месец

Забележка: удълженият период на валидност на сертификата Card_Sign дава възможност на карта на водач да създава валидни подписи върху изтеглени данни през първия месец след изтичането на сертификата. Това е необходимо във връзка с посоченото в Регламент (ЕС) № 581/2010, в който се изисква да има възможност за изтегляне на данни от карта на водач в период до 28 дни след записването на последните данни.

CSM_90 Веднъж след като дадена тахографска карта бъде издадена, не трябва да бъдат заменяни или подновявани двойките ключове и съответните сертификати в нея.

CSM_91 При издаването си тахографските карти трябва да съдържат следните криптографски ключове и сертификати:

— Частния ключ Card_MA и съответния сертификат

— Картите на водачи и картите за монтаж и настройки трябва да съдържат също и частния ключ Card_Sign и съответния сертификат

— Сертификата MSCA_Card, съдържащ публичния ключ MSCA_Card.PK, който се използва за проверяване на сертификата Card_MA и на сертификата Card_Sign

— Сертификата EUR, съдържащ публичния ключ EUR.PK, който се използва за проверяване на сертификата MSCA_Card

— Ако съществува — сертификата EUR, чийто период на валидност непосредствено предшества този сертификат EUR, който се използва за проверяване на сертификата MSCA_Card

— Ако съществува — свързващия сертификат, който дава връзка между тези два сертификата EUR

CSM_92 В допълнение към криптографските ключове и сертификатите, посочени в CSM_91, тахографските карти трябва да съдържат също ключовете и сертификатите, специфицирани в част А от настоящото допълнение, даващи възможност на тези карти да взаимодействат с бордови устройства от първо поколение.

9.1.6 *Равнище на вид оборудване: външни устройства за GNSS*

CSM_93 За всяко външно устройство за GNSS трябва да бъде генерирана една уникална двойка ключове, обозначена като EGF_MA. Тази задача се изпълнява от производителите на външни устройства за GNSS. Когато бъде генерирана двойка ключове EGF_MA, публичният ключ трябва да се изпрати на MSCA в държавата на пребиваване, за да се получи съответен сертификат EGF_MA, подписан от MSCA. Частният ключ трябва да се използва само от външното устройство за GNSS (EGF).

CSM_94 Производителят на EGF избира силата на двойка ключове EGF_MA така, че тя да е равна на силата на двойката ключове на MSCA, използвана за подписване на съответния сертификат EGF_MA.

CSM_95 Всяко външно устройство за GNSS трябва да използва своята двойка ключове EGF_MA, състояща се от частен ключ EGF_MA.SK и публичен ключ EGF_MA.PK изключително само за извършване на взаимно удостоверяване на автентичността и договаряне на сесийни ключове с бордови устройства, както е специфицирано в раздел 11.4 и раздел 11.4 от настоящото допълнение.

CSM_96 Периодът на валидност на даден сертификат EGF_MA е 15 години.

CSM_97 След изтичането на съответния сертификат, външното устройство за GNSS трябва да не използва частния ключ от своята двойка ключове EGF_MA за куплиране (coupling) към бордово устройство.

Забележка: както е изяснено в раздел 11.3.3, дадено външно устройство за GNSS може евентуално да използва своя частен ключ за взаимно удостоверяване на автентичност с бордово устройство, към което то е вече куплирано, дори и след изтичането на съответния сертификат.

CSM_98 Двойката ключове EGF_MA и съответния сертификат на дадено външно устройство за GNSS не трябва да се заменят или обновяват в работна среда (in the field) след като външното устройство за GNSS е пуснато в експлоатация.

Забележка: Настоящото изискване не ограничава възможността за замяна на двойки статични ключове EGF при модернизация или поправка в сигурна среда, контролирана от производителя на външното устройство за GNSS.

CSM_99 При пускането си в експлоатация външните устройства за GNSS трябва да съдържат следните криптографски ключове и сертификати:

— Частния ключ EGF_MA и съответния сертификат

— Сертификата MSCA_VU-EGF, съдържащ публичния ключ MSCA_VU-EGF.PK, който се използва за проверяване на сертификата EGF_MA

— Сертификата EUR, съдържащ публичния ключ EUR.PK, който се използва за проверяване на сертификата MSCA_VU-EGF

— Ако съществува — сертификата EUR, чийто период на валидност непосредствено предшества този сертификат EUR, който се използва за проверяване на сертификата MSCA_VU-EGF

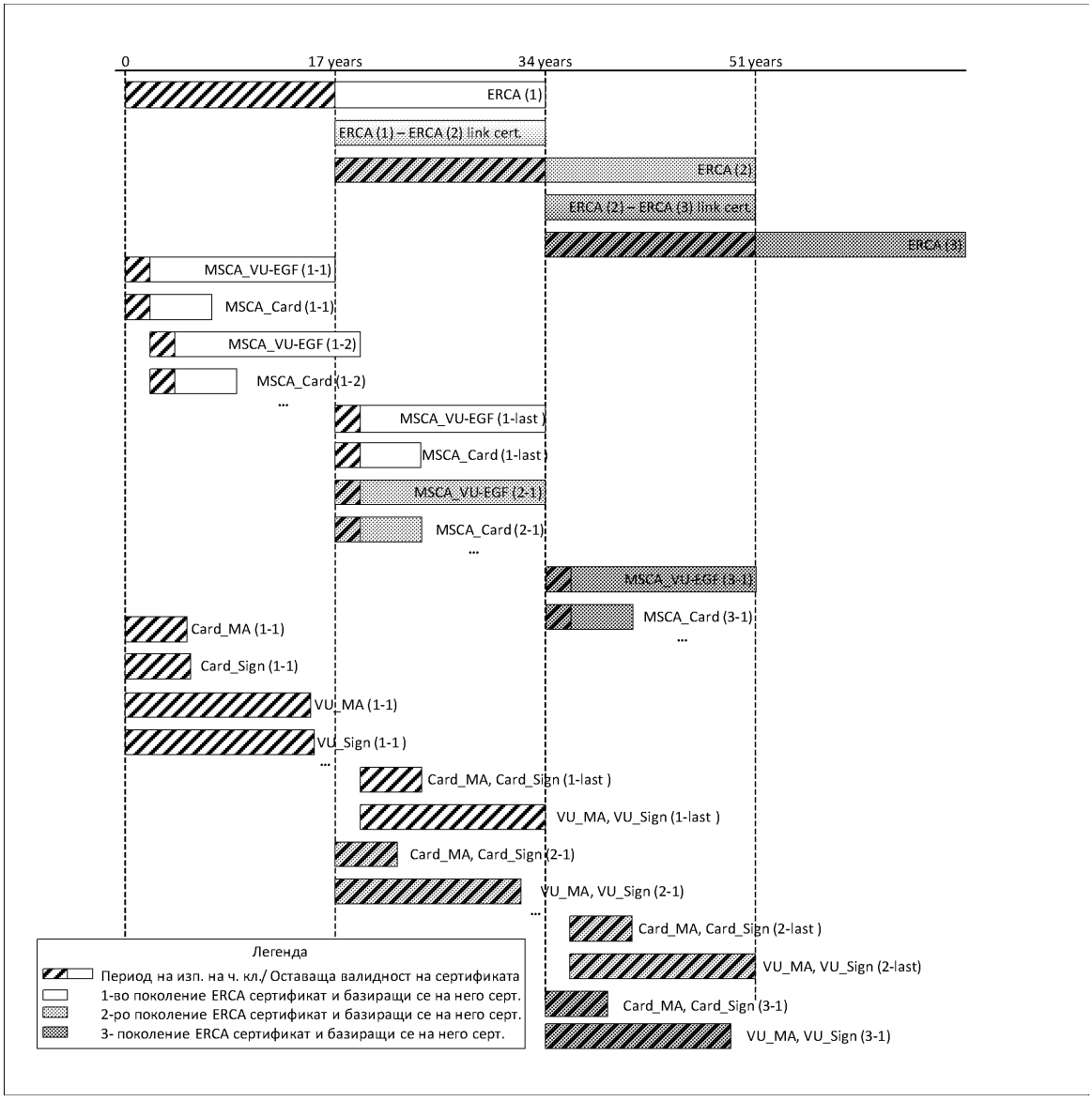
— Ако съществува — свързващия сертификат, който дава връзка между тези два сертификата EUR

9.1.7 *Обобщение: запяна на сертификати*

На фигура 1 по-долу е показано как се издават и използват във времето различните поколения основни сертификати на ERCA, свързващи сертификати на ERCA, сертификати на MSCA и сертификати на оборудване (на бордови устройства и карти):

Фигура 1

Издаване и използване на различни поколения основни сертификати на ERCA (ERCA root certificates), свързващи сертификати на ERCA (ERCA link certificates), сертификати на MSCA (MSCA certificates) и сертификати на оборудване (equipment certificates)



Забележки към фигура 1:

1. Различните поколения основни сертификати са означени с поставено в скоби число. Например ERCA (1) означава първо поколение на основен сертификат на ERCA. ERCA (2) е такъв сертификат от второ поколение и т.н.

2. Други сертификати са обозначени с по две числа в скоби, като първото от тях показва поколението на основния сертификат, въз основа на който са издадени, а второто показва поколението на самия сертификат. Например MSCA_Card (1-1) е първият сертификат MSCA_Card, издаден въз основа на ERCA (1); MSCA_Card (2-1) е първият сертификат MSCA_Card, издаден въз основа на ERCA (2); MSCA_Card (2-last) е последният сертификат MSCA_Card, издаден въз основа на ERCA (2); Card_MA(2-1) е първият картов сертификат за взаимно удостоверяване на автентичността, издаден въз основа на ERCA (2), и т.н.

3. Сертификатите MSCA_Card (2-1) и MSCA_Card (1-last) се издават почти (но не точно) на една и съща дата. Сертификатът MSCA_Card (2-1) е първият сертификат MSCA_Card, който ще бъде издаден въз основа на ERCA (2), и неговото издаване е малко по-късно от това на MSCA_Card (1-last) — последният сертификат въз основа на ERCA (1).

4. Както е показано на фигурата, първите сертификати VU и Card, издадени въз основа на ERCA (2), ще се появят почти две години преди да се появят последните сертификати, издадени въз основа на ERCA (1). Това е така поради факта, че сертификатите VU и Card се издават въз основа на сертификат MSCA, а не пряко въз основа на сертификат ERCA. Сертификатът MSCA (2-1) ще бъде издаден веднага след като ERCA (2) стане валиден, но сертификатът MSCA (1-last) ще бъде издаден малко преди това, докато сертификатът ERCA (1) е все още валиден. По такъв начин двата сертификата MSCA ще имат почти един и същ период на валидност, въпреки факта, че са от различни поколения.

5. Показаният период на валидност за картите е същият като този за картите на водачи (5 години).

6. За спестяване на място, разликата между периодите на валидност на сертификатите Card_MA и Card_Sign, както и между сертификатите VU_MA и VU_Sign, е показана само за първото поколение.

9.2. **Симетрични ключове**

9.2.1 *Ключове за обезпечаване на сигурността на връзката бордово устройство — датчик за движение*

9.2.1.1 *Общи положения*

Забележка: предполага се, че читателите на настоящия раздел са запознати със съдържанието на [ISO 16844-3], описващ интерфейса между бордово устройство и датчик за движение. Процесът на сдвояване между бордово устройство и датчик за движение е описан подробно в глава 12 от настоящото допълнение.

CSM_100 За сдвояване на бордовите устройства и датчиците за движение е необходим известен брой симетрични ключове, които служат за взаимно удостоверяване на автентичността между бордовите устройства и датчиците за движение, а също и за криптиране на връзката между бордовите устройства и датчиците за движение, както е показано в таблица 3. Всички тези ключове трябва да са от типа AES, с дължина равна на дължината на главния ключ на датчика за движение, която трябва да е във връзка с дължината на (предвижданата) европейска двойка основни ключове, описана в CSM_50.

Таблица 3

Ключове за обезпечаване на сигурността на връзката бордово устройство — датчик за движение

Ключ	Символ	Генериран от	Метод за генериране	Съхранява се от
Главен ключ на датчика за движение — част VU	$K_{M\text{-}VU}$	ERCA	Случаен	ERCA, съответните MSCA, участващи в издаването на сертификати за бордови устройства, производителите на бордови устройства, бордовите устройства

Ключ	Символ	Генериран от	Метод за генериране	Съхранява се от
Главен ключ на датчика за движение — сервизна част	K_{M-WC}	ERCA	Случаен	ERCA, MSCA, производителите на карти, картите за монтаж и настройка
Главен ключ за датчика за движение	K_M	Не се генерира независимо	Изчислява се по формулата: $K_M = K_{M-VU}$ XOR K_{M-WC}	ERCA, съответните MSCA, участващи в издаването на ключове за датчици за движение (като опция) (*)
Идентификационен ключ	K_{ID}	Не се генерира независимо	Изчислява се по формулата: $K_{ID} = K_M$ XOR CV, където CV е специфицирано в CSM_106	ERCA, съответните MSCA, участващи в издаването на ключове за датчици за движение (като опция) (*)
Ключ за сдвояване	K_P	Производителя на датчика за движение	Случаен	Един датчик за движение
Сесиен ключ	K_S	Бордовото устройство (при сдвояване на бордово устройство и датчик за движение	Случаен	Едно бордово устройство и един датчик за движение

(*) Съхраняването на K_M и K_{ID} не е задължително, тъй като тези ключове могат да бъдат изведени от $K_{M–VU}$, $K_{M–WC}$ и CV.

CSM_101 Европейският орган за основни сертификати (ERCA) генерира K_{M-VU} and K_{M-WC}, два случайни и уникални ключа AES, от които може да бъде изчислен главният ключ (master key) на датчика за движение K_M като K_{M-VU} XOR K_{M-WC}. При поискване ERCA съобщава K_M, K_{M-VU} и K_{M-WC} на сертифициращите органи на държавите членки.

CSM_102 Към всеки главен ключ K_M на датчик за движение ERCA прикрепя уникален номер на версия, който е валиден също за конституиращите ключове K_{M-VU} и K_{M-WC} и за съответния идентификационен ключ K_{ID}. ERCA информира за номера на версията сертифициращите органи на държавите членки (MSCAs), когато им изпраща K_{M-VU} и K_{M-WC}.

Забележка: Номерът на версията се използва за разграничаване на различните поколения на тези ключове, както е обяснено подробно в раздел 9.2.1.2.

CSM_103 При поискване сертифициращият орган на съответната държава членка препраща K_{M-VU} заедно с номера на неговата версия на производителите на бордови устройства. Производителите на бордови устройства трябва да влагат във всички произведени бордови устройства K_{M-VU} и номера на неговата версия.

CSM_104 Сертифициращият орган на държавата членка трябва да гарантира, че във всяка карта за монтаж и настройки, издадена в рамките на неговата отговорност, е вложен K_{M-WC}, заедно с номера на неговата версия.

Забележки:

— Вж. описанието на типа данни `SensorInstallationSecData` в Допълнение 2.

— Както е изяснено в раздел 9.2.1.2, фактически е възможно в една карта за монтаж и настройки да е необходимо да бъдат вложени няколко поколения K_{M-WC}.

CSM_105 В допълнение към ключа AES, специфициран в CSM_104, всеки сертифициращ орган на държава членка (MSCA) трябва да гарантира, че TDES ключът Km_{WC}, специфициран в изискване CSM_037 в част А от настоящото допълнение, е вложен във всяка карта за монтаж и настройки, издадена в рамките на отговорността на този сертифициращ орган.

Забележки:

— Това дава възможност да се използва карта за монтаж и настройки от второ поколение за куплиране с бордово устройство от първо поколение.

— Картата за монтаж и настройки от второ поколение ще съдържа две различни приложения — едно в съответствие с част Б от настоящото приложение и едно в съответствие с част А. Последното ще съдържа TDES ключа Km_{WC}.

CSM_106 Сертифициращият орган на държава членка (MSCA), участващ в издаването на ключове за датчици за движение, трябва да изведе идентификационния ключ от главния ключ на датчика за движение чрез прилагане на операцията XOR върху него с константен вектор (CV). Стойността на CV трябва да бъде както следва:

— За 128-битови главни ключове на датчици за движение: CV = 'B6 44 2C 45 0E F8 D3 62 0B 7A 8A 97 91 E4 5E 83'

— За 192-битови главни ключове на датчици за движение: CV = '72 AD EA FA 00 BB F4 EE F4 99 15 70 5B 7E EE BB 1C 54 ED 46 8B 0E F8 25'

— За 256-битови главни ключове на датчици за движение: CV = '1D 74 DB F0 34 C7 37 2F 65 55 DE D5 DC D1 9A C3 23 D6 A6 25 64 CD BE 2D 42 0D 85 D2 32 63 AD 60'

Забележка: Константните вектори са генерирани както следва:

Pi_10 = първите десет байта от десетичната част на математическата константа π = '24 3F 6A 88 85 A3 08 D3 13 19'

CV_128-bits = първите 16 байта от SHA-256(Pi_10)

CV_128-bits = първите 24 байта от SHA-384(Pi_10)

CV_128-bits = първите 32 байта от SHA-512(Pi_10)

CSM_107 Производителите на датчици за движение трябва да генерират за всеки датчик за движение случаен и уникален ключ за сдвояване K_P, и трябва да изпращат всеки ключ за сдвояване до сертифициращия орган на държавата членка (MSCA). MSCA трябва да криптира всеки ключ за сдвояване поотделно с главния ключ K_M и трябва да върне криптирания ключ на производителя на датчика за движение. По отношение на всеки криптиран ключ MSCA трябва да уведоми производителя на датчика за движение за номера на версията на съответния K_M.

Забележка: Както е изяснено в раздел 9.2.1.2, фактически е възможно за един датчик за движение да е необходимо производителят да генерира няколко уникални ключа за сдвояване.

CSM_108 Производителите на датчици за движение трябва да генерират уникален сериен номер за всеки датчик за движение и трябва да изпращат всички серийни номера до сертифициращия орган на държавата членка (MSCA). MSCA трябва да криптира всеки сериен номер поотделно с идентификационния ключ K_{ID} и трябва да върне криптирания сериен номер производителя на датчика за движение. По отношение на всеки криптиран сериен номер MSCA трябва да уведоми производителя на датчика за движение за номера на версията на съответния K_{ID}.

CSM_109 Във връзка с изискванията CSM_107 и CSM_108 MSCA трябва да използва алгоритъма AES в работния режим на свързване на блокове от шифровани данни, дефиниран в [ISO 10116], с параметър на редуване (interleave parameter) m = 1 и инициализиращ вектор SV = '00' {16}, т.е. шестнадесет байта с двоична стойност 0. В случаите, при които е необходимо, MSCA трябва да използва метода на запълване 2 (padding method 2), дефиниран в [ISO 9797-1].

CSM_110 Производителят на датчика за движение трябва да запише в бъдещия датчик за движение криптирания ключ за сдвояване и криптирания сериен номер, а също съответните стойности „в открит текст" (plain text values) и съответния номер на версията на K_M и на K_{ID},използвани за криптирането.

Забележка: Както е изяснено в раздел 9.2.1.2, фактически е възможно в един датчик за движение да е необходимо производителят да вложи няколко криптирани ключа за сдвояване и няколко криптирани серийни номера.

CSM_111 Освен посочения в CSM_110 криптографски материал на базата на AES, производителят на датчика за движение може също да запише във всеки датчик за движение и криптографски материал на базата на TDES, специфициран в изискване CSM_037 в част А от настоящото допълнение.

Забележка: Това би дало възможност за куплиране на датчик за движение от второ поколение с бордово устройство от първо поколение.

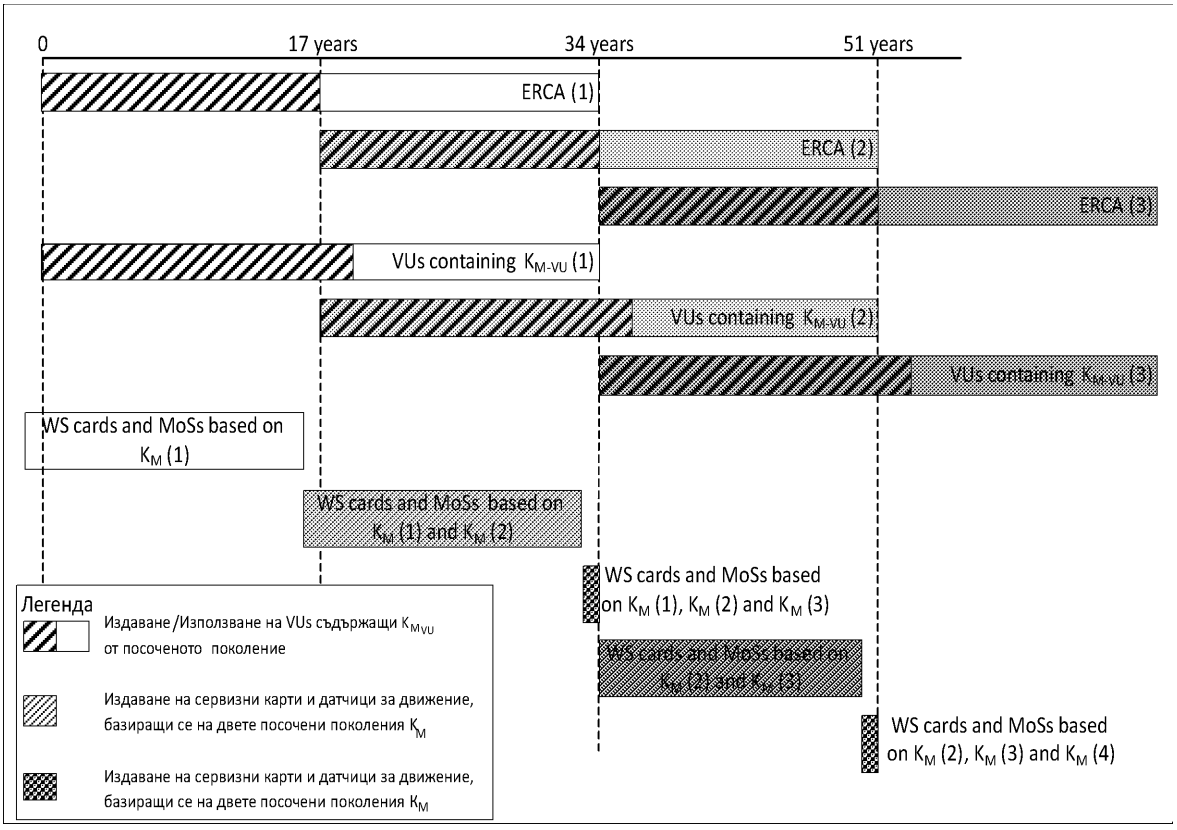
CSM_112 Дължината на сесийния ключ $K_{S,}$ генериран от бордово устройство при сдвояване с датчик за движение, трябва да е свързана с дължината на неговия ключ $K_{M\text{-}VU,}$ както е описана в CSM_50.

9.2.1.2 *Замяна на главния ключ на датчик за движение в оборудване от второ поколение*

CSM_113 Всеки главен ключ на датчик за движение (и всички съответни ключове — вж. таблица 3) е свързан с конкретно поколение на двойката основни ключове на ERCA. Следователно тези ключове трябва да бъдат заменяни на всеки 17 години. Периодът на валидност на всяко поколение главен ключ за датчик за движение започва една година преди началото на валидността на свързаната с него двойка основни ключове на ERCA и завършва с изтичането на валидността на свързаната с него двойка основни ключове на ERCA. Това е описано във фигура 2.

Фигура 2

Издаване и използване на различни поколения на главния ключ за датчик за движение в бордови устройства, датчици за движение и карти за монтаж и настройки (сервизни карти)



CSM_114 Поне една година преди генерирането на нова европейска двойка основни ключове, както е описано в CSM_56, ERCA генерира нов главен ключ за датчика за движение K_M, като генерира нови $K_{M\text{-}VU}$ и $K_{M\text{-}WC}$. Дължината на главния ключ за датчика за движение трябва да е свързана с предвижданата сила на новата европейска двойка основни ключове, в съответствие с CSM_50. При поискване ERCA съобщава новите K_M, $K_{M\text{-}VU}$ и $K_{M\text{-}WC}$ на сертифициращите органи на държавите членки (MSCAs), заедно с техния номер на версия.

CSM_115 MSCA трябва да гарантира, че всички валидни поколения $K_{M\text{-}WC}$ са записани във всяка карта за монтаж и настройки, издадена в рамките на неговото управление, заедно с техните номера на версии, както е показано във фигура 2.

Забележка: Това означава, че в последната година на валидност на даден сертификат на ERCA съответните карти за монтаж и настройки ще се издават с три различни поколения K_{M-WC}, както е показано във фигура 2.

CSM_116 Във връзка с процеса, описан по-горе в CSM_107 и CSM_108: съответният MSCA трябва да криптира всеки ключ за сдвояване K_P, получен от производител на датчик за движение, поотделно с всяко валидно поколение главен ключ за датчик за движение K_M. Също така, MSCA трябва да криптира всеки сериен номер, получен от производител на датчик за движение, поотделно с всяко валидно поколение идентификационен ключ K_{ID}. Производителят на датчика за движение трябва да запише в изработвания датчик за движение криптирания ключ за сдвояване и криптирания сериен номер, а също съответните стойности „в открит текст“ (plain text values) и номера(та) на версията (ите) на K_M и на K_{ID},използвани за криптирането.

Забележка: Това означава, че в последната година на валидност на даден сертификат на ERCA датчиците за движение ще излизат с криптирани данни на базата на три различни поколения K_M, както е показано във фигура 2.

CSM_117 Във връзка с процеса, описан по-горе в CSM_107: тъй като дължината на ключа за сдвояване K_P трябва да бъде свързана с дължината на K_M (вж. CSM_100), възможно е производителят на датчика за движение да е необходимо да генерира за един датчик за движение три различни ключове за сдвояване (с три различни дължини), в случай че последващите поколения K_M са с различна дължина. В такъв случай производителят трябва да изпрати на MSCA всеки един от ключовете за сдвояване. Съответният MSCA трябва да гарантира, че всеки ключ за сдвояване е криптиран с правилното поколение главен ключ за датчика за движение, т.е. с поколението, имащо същата дължина.

Забележка: в случай, че производителят на датчика за движение избере да генерира базиращ се на TDES ключ за сдвояване на датчик за движение от второ поколение (вж. CSM_111), производителят трябва да посочи на MSCA, че за криптирането на този ключ за сдвояване трябва да се използва базиращият се на TDES главен ключ на датчика за движение. Това е необходимо защото дължината на ключ TDES може да е същата като дължината на ключ AES, така че MSCA не може да направи преценка само въз основа на дължината на ключа.

CSM_118 Производителите на бордови устройства трябва да влагат във всяко бордово устройство само едно поколение K_{M-VU}, заедно с неговия номер на версия. Поколението на този K_{M-VU} трябва да бъде свързано със сертификата на ERCA, на който се базират сертификатите на бордовото устройство.

Забележки:

— Бордово устройство, което се базира на сертификат на ERCA от поколение *X*, трябва да съдържа само K_{M-VU} от поколение *X*, дори ако издаването на бордовото устройство е след началото на периода на валидност на сертификат на ERCA от поколение *X+1*. Това е показано на фигура 2.

— Бордово устройство от поколение *X* не може да се сдвоява с датчик за движение от поколение *X-1*.

— Тъй като картите за монтаж и настройки имат период на валидност една година, в резултат от изискванията CSM_113 — CSM_118 всички карти за монтаж и настройки ще съдържат новия K_{M-WC} в момента на издаване на първото бордово устройство, съдържащо новия K_{M-VU}. Следователно такова бордово устройство винаги ще може винаги да изчислява новия K_M. Също така, по това време и повечето нови датчици за движение ще съдържат криптирани данни, базиращи се на новия K_M.

9.2.2 *Ключове за обезпечаване на сигурността на специализирана връзка с малък обсег на действие (DSRC Communication)*

9.2.2.1 *Общи положения*

CSM_119 Автентичността и поверителността на данните, съобщавани от бордово устройство на контролен орган посредством канал за дистанционна връзка DSRC трябва да бъдат обезпечени посредством набор от специфични за бордовото устройство AES ключове, получени от един главен ключ за DSRC, KM_{DSRC}.

CSM_120 Главният ключ за DSRC KM_{DSRC} трябва да е AES ключ, който да бъде генериран, съхраняван и предоставян от ERCA по сигурен начин. Дължината на ключа може да е 128, 192 или 256 бита и трябва да е свързана с дължината на европейската основна двойка ключове, както е описано в CSM_50.

CSM_121 ERCA трябва при поискване да съобщава главния ключ за DSRC на сертифициращите органи на държавите членки по сигурен начин, така че да им даде възможност да изчисляват специфичните за бордовите устройства ключове за DSRC и да гарантират влагане на главния ключ за DSRC във всички контролни карти и карти за монтаж и настройки, издавани в рамките на тяхната отговорност.

CSM_122 Към всеки главен ключ за DSRC ERCA прикрепя уникален номер на версия. ERCA информира за номера на версията сертифициращите органи на държавите членки (MSCAs), когато им изпраща главния ключ за DSRC.

Забележка: Номерът на версията се използва за разграничаване на различните поколения на главния ключ за DSRC, както е обяснено подробно в раздел 9.2.2.2.

CSM_123 За всяко бордово устройство производителят на бордови устройства трябва да създаде уникален сериен номер VU и трябва да изпрати този номер на своя сертифициращ орган на държавата членка, с искане да получи набор от два специфични за бордово устройство ключа за DSRC. Серийният номер VU трябва да съдържа данни от типа `VuSerialNumber` и за кодирането трябва да се използват Разграничените правила за кодиране (DER) съгласно [ISO 8825-1].

CSM_124 При получаването на искане за специфични за бордово устройство ключове DSRC, съответният MSCA трябва да изчисли два AES ключа за бордовото устройство, наричани K_VU_{DSRC}_ENC и K_VU_{DSRC}_MAC. Тези специфични за бордово устройство ключове трябва да са със същата дължина като главния ключ за DSRC. Съответният MSCA трябва да използва функцията за извеждане на ключа, дефинирана в [RFC 5869]. Хеш функцията, която е необходима за приписване на значение на кода HMAC-Hash трябва да е свързана с дължината на главния ключ за DSRC, както е описано в CSM_50. Функцията за извеждане на ключа съгласно [RFC 5869] трябва да се използва както следва:

Стъпка 1 (Извличане):

— *PRK* = HMAC-Hash (*salt, IKM*) където *salt* е празен низ ‘ ’ и *IKM* е KM_{DSRC}.

Стъпка 2 (Разширение):

— *OKM* = *T(1)*, където

T(1) = HMAC-Hash (*PRK, T(0)* || *info* || ‘01’) с

— *T(0)* = празен низ (‘ ’)

— *info* = сериен номер на VU, както е специфициран в CSM_123

— K_VU_{DSRC}_ENC = първите *L* октета от *OKM* и

K_VU_{DSRC}_MAC = последните *L* октета от *OKM*

където *L* е изискваната дължина на K_VU_{DSRC}_ENC и K_VU_{DSRC}_MAC в октети.

CSM_125 Съответният MSCA трябва по сигурен начин да предостави K_VU_{DSRC}_ENC и K_VU_{DSRC}_MAC на производителя на бордови устройства, за влагане в бъдещото бордово устройство.

CSM_126 Когато бъде издадено, бордовото устройство трябва да има записани K_VU_{DSRC}_ENC и K_VU_{DSRC}_MAC в неговата защитена памет, за да може да осигурява цялостността, автентичността и поверителността на данните, изпращани по канала за дистанционна връзка. В бордовото устройство трябва да е записан също и номерът на версията на главния ключ за DSRC, използван за извеждане на специфичните за бордовото устройство ключове.

CSM_127 При издаването на контролните карти и картите за монтаж и настройки в тяхната защитена памет трябва да е записан KM_{DSRC}, за да могат да проверяват цялостността и автентичността на данните, изпратени от VU по канал за дистанционна връзка, както и да могат да декриптират тези данни. Също така, в контролните карти и картите за монтаж и настройка трябва да е записан номерът на версията на главния ключ за DSRC.

Забележка: Както е изяснено в раздел 9.2.2.2, фактически е възможно в една карта за монтаж и настройки или контролна карта да е необходимо да бъдат вложени няколко поколения KM_{DSRC}.

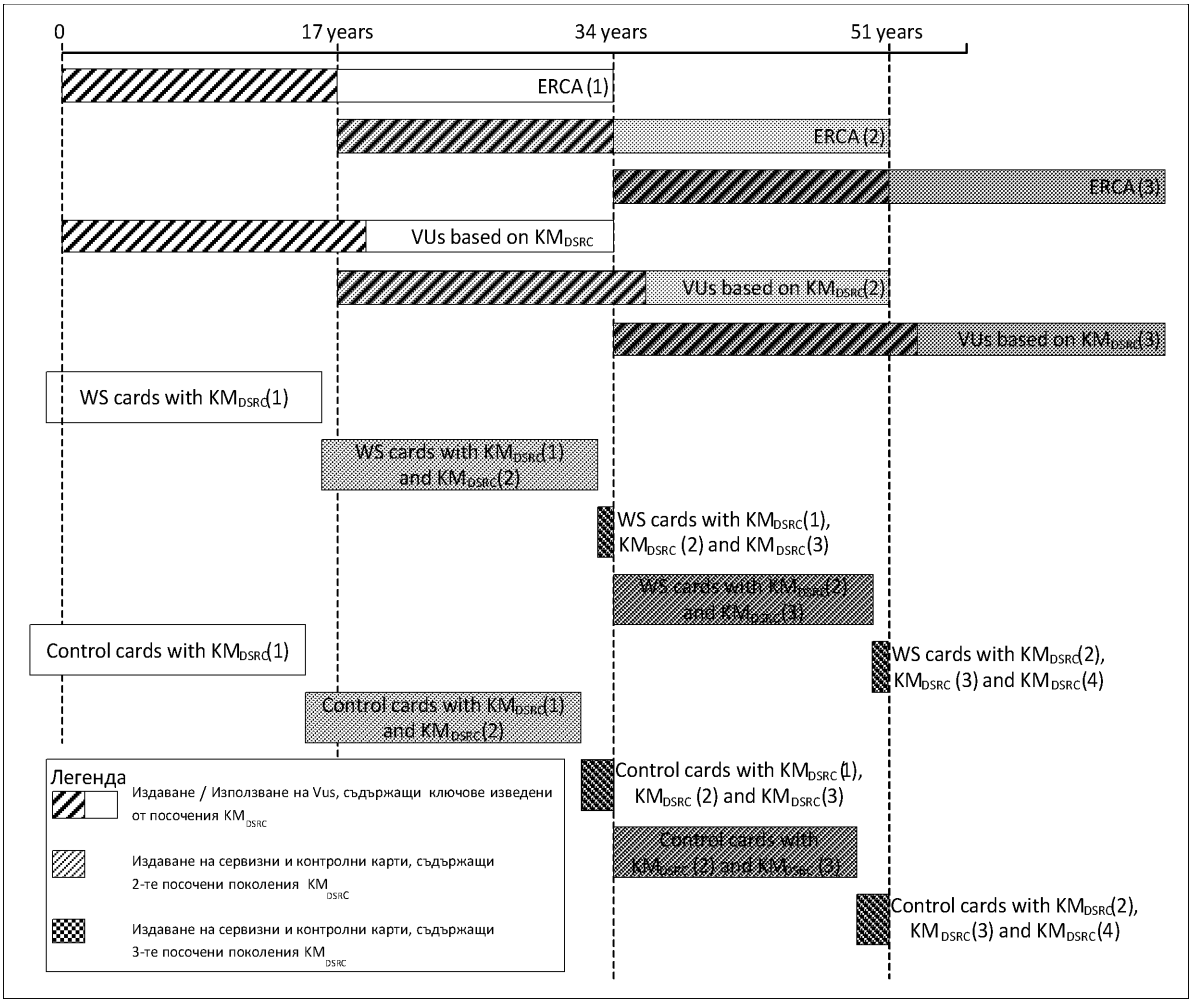
CSM_128 Съответният MSCA трябва да съхранява архивни записи за всички специфични за бордово устройство ключове за DSRC, които е генерирал, техния номер на версия и идентификацията на бордовото устройство, за което е предназначен всеки набор от ключове.

9.2.2.2 *Замяна на главен ключ за DSRC*

CSM_129 Всеки главен ключ за DSRC е свързан с конкретно поколение на двойката основни ключове на ERCA. Следователно ERCA трябва да заменя главния ключ за DSRC на всеки 17 години. Периодът на валидност на всяко поколение главен ключ за DSRC започва две години преди началото на валидността на свързаната с него двойка основни ключове на ERCA и завършва с изтичането на валидността на свързаната с него двойка основни ключове на ERCA. Това е описано във фигура 3.

Фигура 3

Издаване и използване на различни поколения на главния ключ за DSRC в бордови устройства, карти за монтаж и настройки (сервизни карти) и контролни карти



CSM_130 Поне две години преди генерирането на нова европейска двойка основни ключове, както е описано в CSM_56, ERCA генерира нов главен ключ за датчика за DSRC. Дължината на главния ключ за DSRC трябва да е свързана с предвижданата сила на новата европейска двойка основни ключове, в съответствие с CSM_50. При поискване ERCA съобщава новия главен ключ за DSRC на сертифициращите органи на държавите членки (MSCAs), заедно с неговия номер на версия.

CSM_131 Всеки MSCA трябва да гарантира, че всички валидни поколения на KM_{DSRC} са записани във всяка контролна карта, издадена в рамките на неговото управление, заедно с техните номера на версии, както е показано във фигура 3.

Забележка: Това означава, че в последните две години на валидност на даден сертификат на ERCA съответните контролни карти ще се издават с три различни поколения KM_{DSRC}, както е показано във фигура 3.

CSM_132 MSCA трябва да гарантира, че всички валидни поколения на KM_{DSRC}, които са били валидни в продължение на поне една година и продължават да са валидни, са записани във всяка карта за монтаж и настройки, издадена в рамките на неговото управление, заедно с техните номера на версии, както е показано във фигура 3.

Забележка: Това означава, че в последната година на валидност на даден сертификат на ERCA съответните карти за монтаж и настройки ще се издават с три различни поколения KM_{DSRC}, както е показано във фигура 3.

CSM_133 Производителите на бордови устройства трябва да влагат във всяко бордово устройство само един набор от специфични за бордовото устройство ключове DSRC, заедно с неговия номер на версия. Този набор от ключове се получава от KM_{DSRC} от поколението, свързано със сертификата на ERCA, на който се базират сертификатите на бордовото устройство.

Забележки:

— Това означава, че бордово устройство, което се базира на сертификат на ERCA от поколение *X*, трябва да съдържа K_VU_{DSRC}_ENC и K_VU_{DSRC}_MAC от поколение *X*, дори ако издаването на бордовото устройство е след началото на периода на валидност на сертификат на ERCA от поколение *X+1*. Това е показано на фигура 3.

— Тъй като периодът на валидност на картите за монтаж и настройка е една година, а за контролните карти този период е две години, в резултат от изискванията CSM_131 — CSM_133 всички карти за монтаж и настройки и всички контролни карти ще съдържат новия главен ключ DSRC в момента на издаване на първото бордово устройство, съдържащо специфичните за бордово устройство ключове, базиращи се на този главен ключ.

9.3. **Сертификати**

9.3.1 *Общи положения*

CSM_134 Всички сертификати в Европейската система за интелигентни тахографи трябва да бъдат самоописващи се и проверими с карта (CV) сертификати в съответствие с [ISO 7816-4] и [ISO 7816-8].

CSM_135 Разграничените правила за кодиране (DER) съгласно [ISO 8825-1] трябва да бъдат използвани за кодиране както на структурите от данни ASN.1, така също и на (специфични за отделни приложения) обекти от данни в сертификатите.

Забележка: Това кодиране води до следната структура Таг-Дължина-Стойност (TLV):

Таг: Тагът се кодира в един или два октета и показва съдържанието.

Дължина: Дължината се кодира като беззнаково цяло число в един, два или три октета, като в резултат максималната дължина е 65 535 октета. Използва се минималният брой октети.

Стойност: Стойността се кодира в нула или повече октети.

9.3.2 *Съдържание на сертификатите*

CSM_136 Всички сертификати трябва да са със структурата, показана в профила на сертификатите във таблица 4.

Таблица 4.

Профил на сертификат, версия 1

Поле	ID на полето	Таг	Дължи-на (бай-това)	ASN.1 тип на данните (вж. допълнение 1)
ECC сертификат	C	‘7F 21’	променлива	
Тяло на ECC сертификат	B	‘7F 4E’	променлива	

Поле	ID на полето	Таг	Дължи-на (бай-това)	ASN.1 тип на данните (вж. допълнение 1)
Идентификатор на профила на сертифи-ката	CPI	‘5F 29’	‘01’	INTEGER(0..255)
Референтно означение на сертифициращия орган	CAR	‘42’	‘08’	KeyIdentifier
Оторизация на титуляря на сертификата	CHA	‘5F 4C’	‘07’	CertificateHolder Authorisation
Публичен ключ	PK	‘7F 49’	променлива	
Домейн параметри	DP	‘06’	променлива	OBJECT IDENTIFIER
Публична точка	PP	‘86’	променлива	OCTET STRING
Референтно означение на титуляря на сер-тификата	CHR	‘5F 20’	‘08’	KeyIdentifier
Дата на влизане в сила на сертификата	CEfD	‘5F 25’	‘04’	TimeReal
Дата на изтичане на сертификата	CExD	‘5F 24’	‘04’	TimeReal
Подпис на ECC сертификат	S	‘5F 37’	променлива	OCTET STRING

Забележка: идентификаторите на полета се използват в следващи раздели на настоящото приложение за означаване на отделните полета в даден сертификат, например X.CAR е референтно означение на сертифициращия орган, посочен в сертификата на ползвател X.

9.3.2.1 Идентификатор на профила на сертификата

CSM_137 Сертификатите трябва да имат идентификатор на профила на сертификата, показващ какъв е използваният профил на сертификат. Версия 1, посочена във таблица 4, се идентифицира със стойността ‘00’.

9.3.2.2 Референтно означение на сертифициращия орган

CSM_138 Референтното означение на сертифициращия орган се използва за идентифициране на публичния ключ, който служи за проверяване на подписа на сертификата. Следователно референтното означение на сертифициращия орган трябва да е еднакво с референтното означение на титуляря на сертификата на съответния сертифициращ орган.

CSM_139 Всеки основен сертификат на ERCA трябва да е самоподписан, т.е. референтното означение на сертифициращия орган и референтното означение на титуляря на сертификата в този сертификат трябва да са еднакви.

CSM_140 При свързващ сертификат на ERCA референтното означение на титуляря на сертификата (CHR) трябва да е еднакво с CHR на новия основен сертификат на ERCA. При свързващ сертификат CHR трябва да е еднакво с CHR на предходния основен сертификат на ERCA.

9.3.2.3 Оторизация на титуляря на сертификата

CSM_141 Оторизацията на титуляря на сертификата се използва за идентифициране на типа на сертификата. Тя се състои от шестте най-старши байта от идентификатора на заявката за тахограф, с конкатенация за типа оборудване, за което е предназначен сертификатът.

9.3.2.4 Публичен ключ

В публичния ключ са поместени два елемента от данни: стандартизираните домейн параметри, използвани с публичния ключ в сертификата и стойността на публичната точка.

CSM_142 Елементът от данни „домейн параметри“ трябва да съдържа един от идентификаторите на обекти, специфицирани в таблица 1 за означаване на набор от стандартизирани домейн параметри.

CSM_143 Елементът от данни „публична точка“ трябва да съдържа публичната точка. Публичните точки от елиптичната крива трябва да се преобразуват в октетни низове както е специфицирано в [TR-03111]. Трябва да се използва некомпресираният формат за кодиране. При възстановяването на точка от елиптичната крива от нейния кодиран формат винаги трябва да се извършват валидиранията, описани в [TR-03111].

9.3.2.5 Референтно означение на титуляря на сертификата

CSM_144 Референтното означение на титуляря на сертификата е идентификатор за публичния ключ, даден в сертификата. То трябва да се използва за означаване на този публичен ключ в други сертификати.

CSM_145 В картовите сертификати и сертификатите за външни GNSS устройства, референтното означение на титуляря на сертификата трябва да е с тип на данните `ExtendedSerialNumber`, специфициран в допълнение 1.

CSM_146 При бордовите устройства, когато производителят отправя искане за сертификат е възможно той да знае или да не знае специфичния сериен номер на бордовото устройство, за което е предназначен този сертификат и свързания с него частен ключ. В първия случай референтното означение на титуляря на сертификата трябва да е с тип на данните `ExtendedSerialNumber`, специфициран в допълнение 1. Във втория случай референтното означение на титуляря на сертификата трябва да е с тип на данните `CertificateRequestID`, специфициран в допълнение 1.

CSM_147 При сертификатите на ERCA и MSCA референтното означение на титуляря на сертификата трябва да е с тип на данните `CertificationAuthorityKID`, специфициран в допълнение 1.

9.3.2.6 Дата на влизане в сила на сертификат

CSM_148 Датата на влизане в сила на сертификата показва началната дата и час на периода на валидност на сертификата. Датата на влизане в сила на сертификата трябва да е датата на неговото генериране.

9.3.2.7 Дата на изтичане на сертификата

CSM_149 Датата на изтичане на сертификата показва крайната дата и час на периода на валидност на сертификата.

9.3.2.8 Подпис върху сертификат

CSM_150 Подписът върху сертификата се създава върху кодираното тяло на сертификата, включително с тага и дължината на тялото на сертификата. Алгоритъмът за подписа трябва да бъде ECDSA, както е специфициран в [DSS], с използване на алгоритъма за хеширане, свързан с размера на ключа на подписващия орган, както е специфицирано в CSM_50. Форматът на подписа трябва да бъде открит (plain), както е специфицирано в [TR-03111].

9.3.3 *Поискване на сертификати*

CSM_151 При поискване на сертификат заявителят трябва да изпрати на сертифициращия орган следните данни:

— Идентификатора на профила на искания сертификат

— Референтното означение на сертифициращия орган, за което се очаква да бъде използвано за подписване на сертификата.

— Публичния ключ, който да бъде подписан

CSM_152 В допълнение към данните в CSM_151, когато заявителят е MSCA, той трябва да изпрати следните данни в искане за сертификат до ERCA, които да дадат възможност на ERCA да създаде референтното означение на титуляря на сертификата на новия сертификат на MSCA:

— Цифровия национален код на сертифициращия орган (тип на данните `NationNumeric`, дефиниран в допълнение 1)

— Буквено-цифровия национален код на сертифициращия орган (тип на данните `NationAlpha`, дефиниран в допълнение 1)

— 1-байтовия сериен номер за разграничаване на различните ключове на сертифициращия орган, в случай че ключовете са сменени

— Двубайтовото поле, съдържащо специфична допълнителна информация на сертифициращия орган

CSM_153 В допълнение към данните в CSM_151, когато заявителят е производител на оборудване, той трябва да изпрати следните данни в искане за сертификат до MSCA, които да дадат възможност на MSCA да създаде референтното означение на титуляря на сертификата на новия сертификат на производителя на оборудване:

— Специфичен за производителя идентификатор на типа оборудване

— Сериен номер на оборудването, ако е известен (вж. CSM_154), който да е уникален за производителя, типа на оборудването и месеца на производство. В противен случай, уникален идентификатор на искането за сертификат.

— Месеца и годината на производство на оборудването или на искането за сертификат.

Производителят трябва да осигури тези данни да са правилни, както и да осигури влагането в оборудването на получения от MSCA сертификат.

CSM_154 В случай на бордово устройство, когато производителят отправя искане за сертификат, е възможно той да знае или да не знае специфичния сериен номер на бордовото устройство, за което е предназначен този сертификат и свързания с него частен ключ. Ако серийният номер е известен, производителят на бордовото устройство трябва да го изпрати на MSCA. Ако този номер не е известен, производителят трябва уникално да идентифицира всяко искане за сертификат и да изпрати на MSCA серийния номер на съответното искане за сертификат. В такъв случай полученият в резултат сертификат ще съдържа серийния номер на искането за сертификат. След влагането на сертификата в конкретното бордово устройство, производителят трябва да съобщи на MSCA връзката между серийния номер на искането за сертификат и идентификацията на бордовото устройство.

10. ВЗАИМНО УДОСТОВЕРЯВАНЕ НА АВТЕНТИЧНОСТТА И ЗАЩИТЕН ОБМЕН НА СЪОБЩЕНИЯ БОРДОВО УСТРОЙСТВО — КАРТА

10.1. **Общи положения**

CSM_155 При високо равнище на сигурност, защитената връзка между бордово устройство и тахографска карта трябва да се базира на следните стъпки:

— Първо, всяка страна трябва да демонстрира на другата, че притежава валиден сертификат за публичен ключ, подписан от сертифициращ орган на държава членка (MSCA). На свой ред, сертификатът за публичен ключ на MSCA трябва да е подписан от европейския орган за основни сертификати (ERCA). Тази стъпка се нарича проверка на веригата на сертифициране и е подробно специфицирана в раздел 10.2.

— Второ, бордовото устройство трябва да демонстрира на картата, че притежава частния ключ, съответстващ на публичния ключ в представения сертификат. То прави това чрез подписване на случайно число, изпратено на картата. Картата проверява подписа върху случайното число. Ако тази проверка е успешна, бордовото устройство е автентифицирано. Тази стъпка се нарича удостоверяване на автентичността на бордовото устройство и е подробно специфицирана в раздел 10.3.

— Трето, и двете страни независимо изчисляват два AES сесийни ключа, като използват асиметричен алгоритъм за договаряне на ключове. Като използва един от тези сесийни ключове, картата създава код за автентифициране на съобщение (MAC) върху данни, изпратени от бордовото устройство. Бордовото устройство проверява този MAC. Ако проверката е успешна, картата е автентифицирана. Тази стъпка се нарича удостоверяване на автентичността на карта и е подробно специфицирана в раздел 10.4.

— Четвърто, бордовото устройство и картата трябва да използват договорените сесийни ключове за осигуряване на поверителността, цялостността и автентичността на всички обменени съобщения. Това се нарича защитен обмен на съобщения и е подробно специфицирано в раздел 10.5.

CSM_156 Описаният в CSM_155 механизъм трябва да бъде задействан от бордовото устройство винаги когато бъде вкарана карта в едно от неговите четящи устройства.

10.2. **Взаимна проверка на веригата на сертифициране**

10.2.1 *Проверка от бордовото устройство на веригата на сертифициране на картата*

CSM_157 За проверяване на веригата на сертифициране на тахографска карта, бордовите устройства трябва да използват протокола, описан във фигура 4.

Забележки към фигура 4:

— Посочените във фигурата сертификати и публични ключове Card са тези, които се използват за взаимно удостоверяване на автентичността. В раздел 9.1.5 те са означени като Card_MA.

— Упоменатите във фигурата сертификати и публични ключове Card.CA са тези, които се използват за подписване на картови сертификати и се посочват в референтното означение на сертифициращия орган (CAR) на сертификатите Card. В раздел 9.1.3 те са означени като MSCA_Card.

— Упоменатият във фигурата сертификат Card.CA.EUR е европейският основен сертификат, който е посочен в референтното означение на сертифициращия орган (CAR) на сертификата Card.CA.

— Упоменатият във фигурата сертификат Card.Link е свързващият сертификат на картата, ако има такъв. Както е посочено в раздел 9.1.2, това е свързващ сертификат за нова европейска двойка основни ключове, създадена от ERCA и подписана с предходния европейски частен ключ.

— Сертификатът Card.Link.EUR е европейският основен сертификат, който е посочен в референтното означение на сертифициращия орган (CAR) на сертификата Card.Link.

CSM_158 Както е описано във фигура 4, проверката на веригата на сертифициране на картата започва с вкарването на картата. Бордовото устройство трябва да прочете референтното означение на титуляря на картата (`cardExtendedSerialNumber`) от EF ICC. Бордовото устройство трябва да провери дали познава картата, т.е. дали в миналото успешно е проверявало веригата на сертифициране на картата и я е записало за бъдещи справки. Ако това е така и ако сертификатът на картата продължава да е валиден, процесът продължава с проверка на веригата на сертифициране на бордовото устройство. В противен случай бордовото устройство трябва последователно да прочете от картата сертификата MSCA_Card, който да се използва за проверка на картовия сертификат, Card.CA.EUR, който да се използва за проверка на сертификата MSCA_Card и евентуално свързващия сертификат, докато намери сертификат, който познава или може да провери. Ако такъв сертификат бъде намерен, бордовото устройство трябва да го използва за да провери съответните картови сертификати, които то е прочело от картата. Ако проверката на картата е успешна, процесът продължава с проверяване на веригата на сертифициране на бордовото устройство. Ако проверката на картата не е успешна, бордовото устройство трябва да я игнорира.

Забележка: Има три начина, по които бордовото устройство може да познава сертификата Card.CA.EUR:

— сертификатът Card.CA.EUR е същият като собствения сертификат EUR на бордовото устройство;

— сертификатът Card.CA.EUR предхожда собствения сертификат EUR на бордовото устройство и бордовото устройство вече е имало този сертификат при своето издаване (вж. CSM_81);

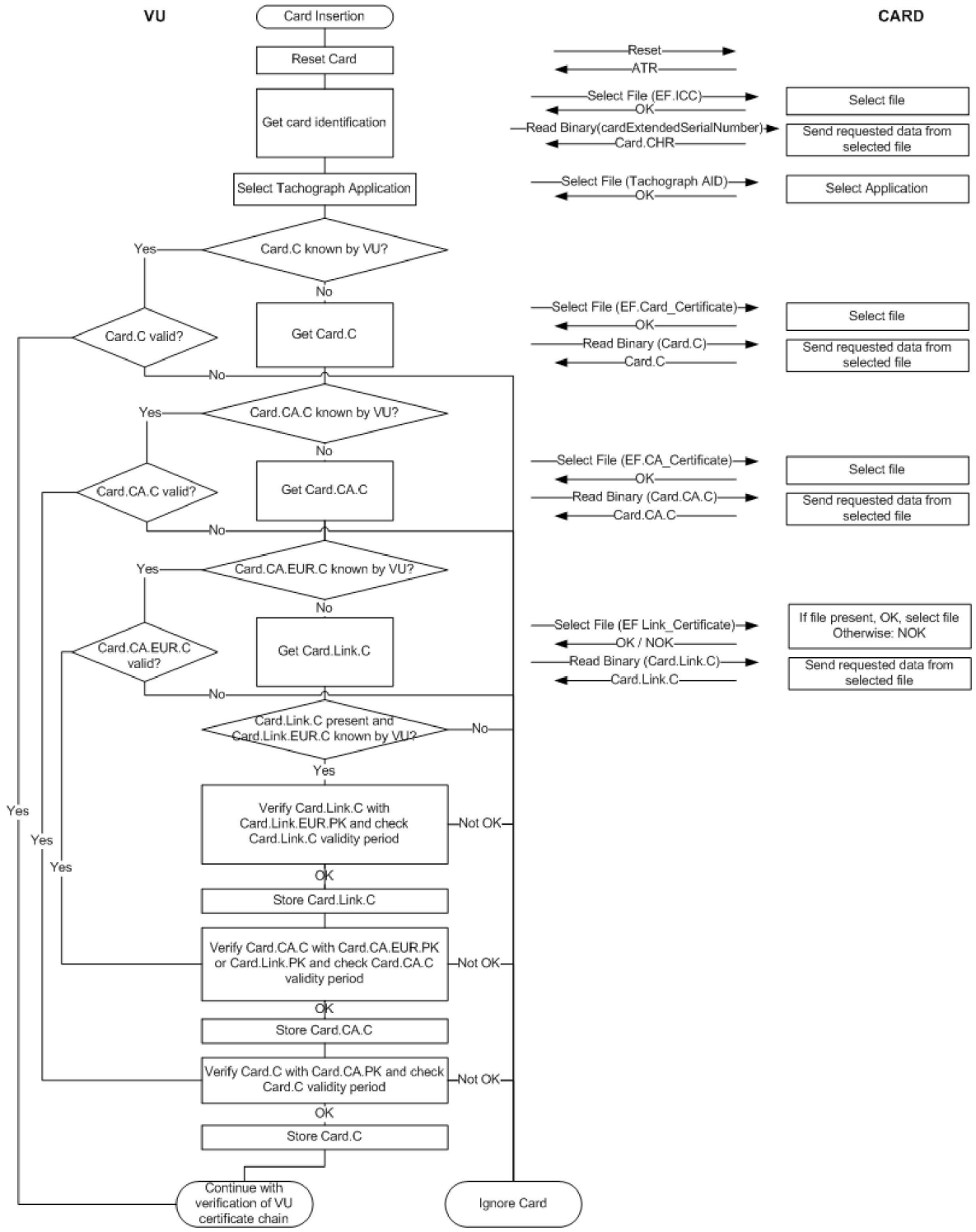
— сертификатът Card.CA.EUR е следващ сертификат след собствения сертификат EUR на бордовото устройство и в миналото бордовото устройство е получило свързващ сертификат от друга тахографска карта, проверило го е и го е съхранило за бъдещи справки.

CSM_159 Както е посочено във фигура 4, след като веднъж бордовото устройство удостовери автентичността и валидността на непознат по-рано сертификат, то може да съхрани този сертификат за бъдещи справки, така че да не е необходимо пак да проверява автентичността му ако този сертификат му бъде представен отново. Вместо да съхранява целия сертификат, бордовото устройство може да избере да съхранява само тялото на сертификата, както е специфицирано в 9.3.2.

CSM_160 Бордовото устройство трябва да проверява валидността във времето на всеки прочетен в карта или съхранен в паметта му сертификат и трябва да отхвърля изтеклите сертификати. За проверяването на валидността във времето на представен от карта сертификат бордовото устройство трябва да използва своя вътрешен часовник.

Фигура 4

Протокол за проверка от бордово устройство на веригата на сертифициране на карта

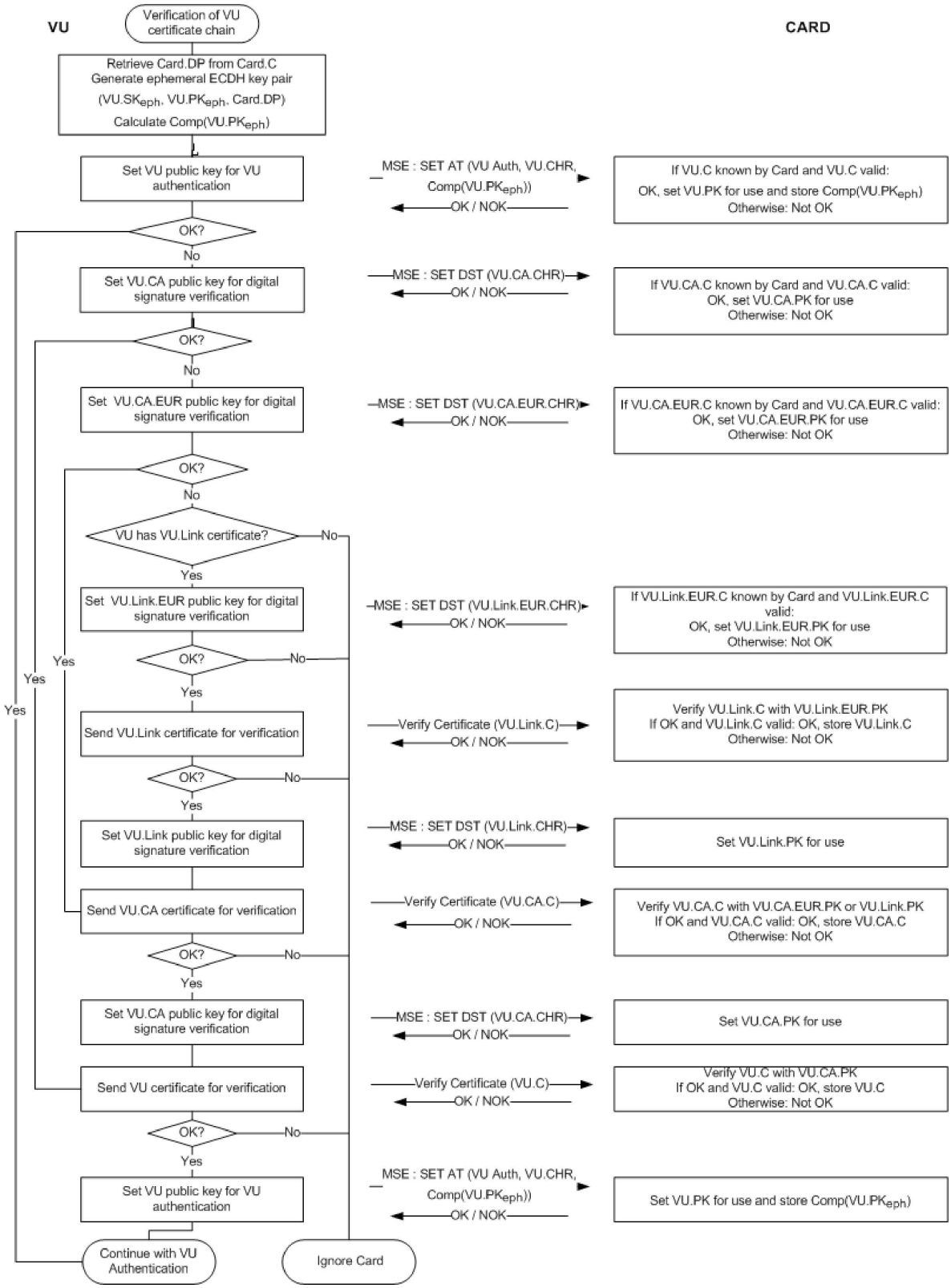


10.2.2 *Проверка от карта на веригата на сертифициране на бордово устройство*

CSM_161 За проверяване на веригата на сертифициране на бордово устройство, тахографските карти трябва да използват протокола, описан във фигура 5.

Фигура 5

Протокол за проверка от карта на веригата на сертифициране на бордово устройство



Забележки към фигура 5:

— Посочените във фигурата сертификати и публични ключове VU са тези, които се използват за взаимно удостоверяване на автентичността. В раздел 9.1.4 те са означени като VU_MA.

— Посочените във фигурата сертификати и публични ключове VU.CA са тези, които се използват за подписване на сертификати на бордови устройства и на външни устройства за GNSS. В раздел 9.1.3 те са означени като MSCA_VU-EGF.

— Упоменатият във фигурата сертификат VU.CA.EUR е европейският основен сертификат, който е посочен в референтното означение на сертифициращия орган (CAR) на сертификата VU.CA.

— Посоченият във фигурата сертификат VU.Link е свързващият сертификат на бордовото устройство, ако има такъв. Както е посочено в 9.1.2, това е свързващ сертификат за нова европейска двойка основни ключове, създадена от ERCA и подписана с предходния европейски частен ключ.

— Сертификатът VU.Link.EUR е европейският основен сертификат, който е посочен в референтното означение на сертифициращия орган (CAR) на сертификата VU.Link.

CSM_162 Както е описано във фигура 5, проверката на веригата на сертифициране на бордовото устройство започва с опит на бордовото устройство да зададе своя собствен публичен ключ за използване в тахографската карта. Ако този опит е успешен, това означава че в миналото тахографската карта успешно е проверила веригата на сертифициране на бордовото устройство и е съхранила сертификата на бордовото устройство за бъдещи справки. В такъв случай сертификатът на бордовото устройство е зададен за употреба и процесът продължава с удостоверяване на автентичността на бордовото устройство. Ако картата не разпознава сертификата на бордовото устройство, за да се стигне до познат или проверим от картата сертификат, то трябва да представи последователно сертификата VU.CA за проверка на неговия сертификат, сертификата VU.CA.EUR за проверка на сертификата VU.CA и евентуално и свързващия сертификат, за да намери картата познат или проверим от нея сертификат. Ако такъв сертификат бъде намерен, картата трябва да го използва за да провери съответните сертификати на VU, които са ѝ представени. Ако проверката е успешна, бордовото устройство накрая задава своя публичен ключ за употреба в тахографската карта. Ако проверката не е успешна, бордовото устройство трябва да игнорира картата.

Забележка: Има три начина, по които картата може да познава сертификата VU.CA.EUR:

— сертификатът VU.CA.EUR е същият като собствения сертификат EUR на картата;

— Сертификатът VU.CA.EUR предхожда собствения сертификат EUR на картата и картата вече е имала този сертификат при своето издаване (вж. CSM_91);

— Сертификатът VU.CA.EUR е следващ сертификат след собствения сертификат EUR на картата и в миналото картата е получила свързващ сертификат от друго бордово устройство, проверила го е и го е съхранила за бъдещи справки.

CSM_163 Бордовото устройство трябва да използва командата MSE: SET AT за да зададе своя публичен ключ за употреба в тахографската карта. Както е специфицирано в допълнение 2, тази команда съдържа индикация за криптографския механизъм, който ще бъде използван със задавания ключ. Този механизъм трябва да бъде „Автентифициране на бордово устройство с използване на алгоритъма ECDSA, в комбинация с алгоритъма за хеширане, съответстващ на размера на ключовете в двойката ключове VU_MA на бордовото устройство, както е специфицирано в CSM_50“.

CSM_164 Командата MSE: Set AT съдържа също индикация за двойката краткотрайни ключове (ephemeral key pair), която бордовото устройство ще използва при договарянето на сесиен ключ (вж. раздел 10.4). Следователно, преди да изпрати командата MSE: Set AT, бордовото устройство трябва да генерира двойка краткотрайни ключове за ECC. За генерирането на двойката краткотрайни ключове бордовото устройство трябва да използва стандартизираните домейн параметри, посочени в сертификата на картата. Двойката краткотрайни ключове се означава по следния начин: ($VU.SK_{eph}$, $VU.PK_{eph}$, Card.DP). Като идентификация на ключа бордовото устройство взема координатата x на кратковременната публична точка в ECDH; това се нарича компресирано представяне на публичния ключ и се означава като $Comp(VU.PK_{eph})$.

CSM_165 Ако командата MSE: Set AT е успешна, картата трябва да зададе посочения VU.PK за последваща употреба при автентифициране на бордовото устройство и временно да съхрани $Comp(VU.PK_{eph})$. В случай, че са изпратени две или повече успешни команди MSE: Set AT преди да е направено договаряне на сесиен ключ, картата трябва да съхрани само последния получен $Comp(VU.PK_{eph})$.

CSM_166 Картата трябва да проверява валидността във времето на всеки представен от бордовото устройство сертификат или посочен от бордовото устройство съхраняван в паметта на картата сертификат, и трябва да отхвърля изтеклите сертификати.

CSM_167 За целите на проверяването на валидността във времето на представен от бордовото устройство сертификат, всяка тахографска карта трябва вътрешно да съхранява данни, изразяващи текущото време. Тези данни трябва да не могат да бъдат директно актуализирани от бордово устройство. При нейното издаване текущото време на дадена карта трябва да бъде зададено да съвпада с датата на влизане в сила на сертификата Card_MA на картата. Ако датата на влизане в сила на представен от дадено бордово устройство автентичен сертификат, представляващ „валиден източник на данни за времето“, е по-скорошна в сравнение с текущото време на картата, тя трябва да актуализира своето текущо време. В такъв случай картата трябва да настрои своето текущо време да съвпада с датата на влизане в сила на този сертификат. Като валиден източник на данни за времето картата трябва да възприема само следните сертификати:

— Свързващи сертификати на ERCA от второ поколение

— Сертификати на MSCA от второ поколение

— Сертификати на бордово устройство от второ поколение, издадени от същата държава като собствения сертификат (собствените сертификати) на картата.

Забележка: Последното изискване означава, че картата трябва да може да разпознае референтното означение на сертифициращия орган (CAR) на сертификата на бордовото устройство, т.е. на сертификата MSCA_VU-EGF. То няма да е същото като CAR на нейния собствен сертификат, който е сертификат MSCA_Card.

CSM_168 Както е посочено във фигура 5, след като веднъж картата удостовери автентичността и валидността на непознат по-рано сертификат, тя може да съхрани този сертификат за бъдещи справки, така че да не е необходимо пак да проверява автентичността му ако този сертификат ѝ бъде представен отново. Вместо да съхранява целия сертификат, картата може да избере да съхранява само тялото на сертификата, както е специфицирано в 9.3.2.

10.3. **Удостоверяване на автентичността на бордово устройство**

CSM_169 За удостоверяване на автентичността на бордово устройство по отношение на карта, бордовите устройства и картите трябва да използват протокола VU Authentication, описан във фигура 6. Протоколът VU Authentication дава възможност на тахографската карта експлицитно да провери, че бордовото устройство е автентично. За целта бордовото устройство трябва да използва своя частен ключ за да подпише генерирано от картата случайно число (challenge).

CSM_170 Бордовото устройство трябва да включи в подписа, непосредствено след изпратеното от картата случайно число, референтното означение на титуляря на картата, взето от сертификата на картата.

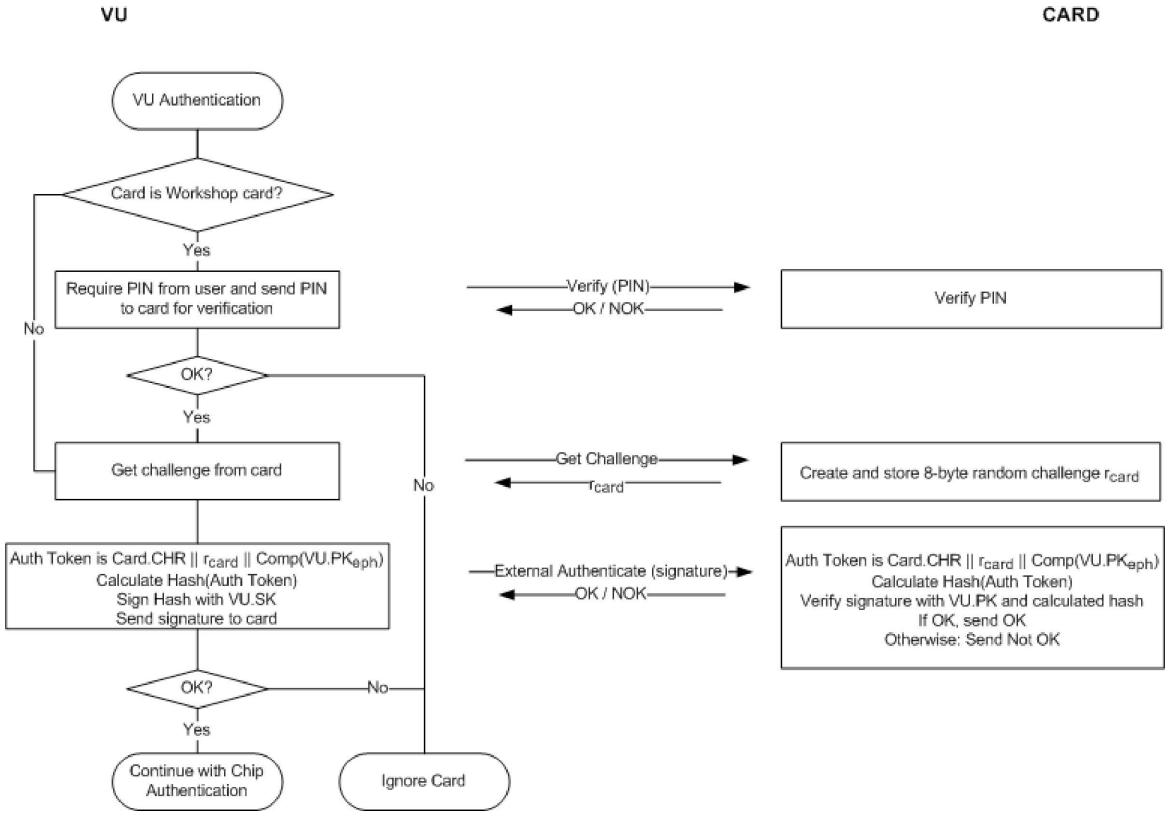
Забележка: Така се гарантира, че картата спрямо която се автентифицира бордовото устройство, е същата карта, чиято верига на сертифициране то е проверило преди това.

CSM_171 Бордовото устройство трябва да включи също в подписа идентификатора на краткотрайния (ephemeral) публичен ключ Comp(VU.PK_{eph}), който бордовото устройство ще използва за защитен обмен на съобщения по време на процеса на удостоверяване на автентичността на чипа, специфициран в раздел 10.4.

Забележка: Това гарантира, че бордовото устройство, с което комуникира дадена карта по време на сесия на защитен обмен на съобщения, е същото бордово устройство, което е било автентифицирано от картата.

Фигура 6

Протокол за удостоверяване на автентичността на бордово устройство



CSM_172 Ако по време на процеса на автентифициране на бордовото устройство то изпрати няколко команди GET CHALLENGE, картата трябва всеки път да връща ново 8-байтово случайно число, но трябва да съхранява само последното случайно число.

CSM_173 Използваният от бордовото устройство алгоритъм за подписване при автентифицирането на бордовото устройство трябва да бъде ECDSA, както е специфициран в [DSS], с използване на алгоритъма за хеширане, свързан с размера на двойката ключове на бордовото устройство VU_MA, както е специфицирано в CSM_50. Форматът на подписа трябва да бъде открит (plain), както е специфицирано в [TR-03111]. Бордовото устройство трябва да изпрати така получения подпис на картата.

CSM_174 При получаване на подписа на бордовото устройство в команда EXTERNAL AUTHENTICATE, картата трябва да изпълни следните операции:

— Да изчисли автентификационния маркер (authentication token) чрез конкатенация на Card.CHR, случайното число от картата r_{card} и идентификатора на краткотрайния (ephemeral) публичен ключ Comp($VU.PK_{eph}$),

— Да изчисли хеша върху автентификационния маркер като използва алгоритъма за хеширане, съответстващ на размера на ключовете в двойката ключове VU_MA на бордовото устройство, както е специфицирано в CSM_50,

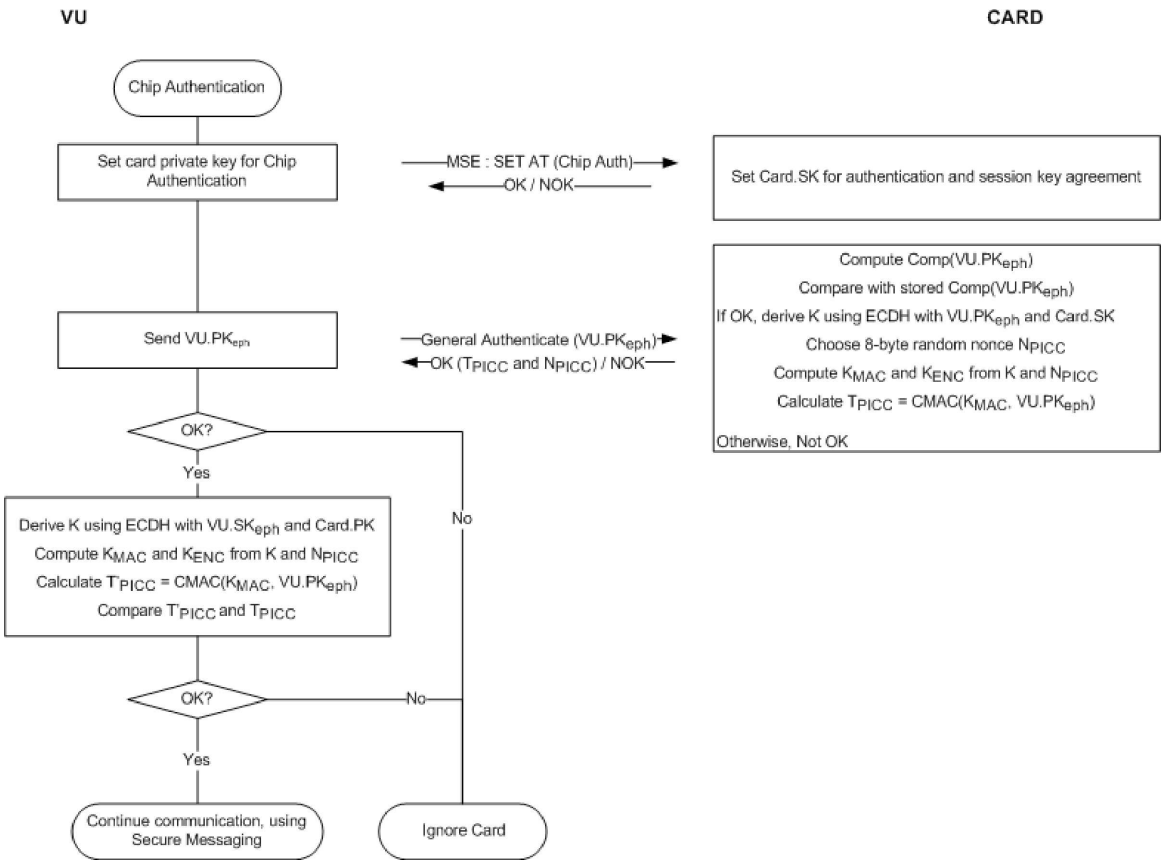
— Да провери подписа на бордовото устройство като използва алгоритъма ECDSA, в комбинация с VU.PK и изчисления хеш.

10.4. **Удостоверяване на автентичността на чипа и договаряне на ключ за сесията**

CSM_175 За удостоверяване на автентичността на картата по отношение на бордовото устройство, бордовите устройства и картите трябва да използват протокола Chip Authentication, описан във **фигура 7**. Протоколът Chip Authentication дава възможност на бордовото устройство експлицитно да провери, че картата е автентична.

Фигура 7

Удостоверяване на автентичността на чипа и договаряне на ключ за сесията



CSM_176 Бордовото устройство и картата трябва да изпълнят следните стъпки:

1. Бордовото устройство инициира процеса на удостоверяване на автентичността на чипа като изпраща командата MSE: Set AT с индикация „Удостоверяване на автентичността на чип с използване на алгоритъм ECDH, водещ до дължина на сесийния ключ AES, която е свързана с размера на ключовете в двойката ключове на картата Card_MA, както е специфицирано в CSM_50“. Бордовото устройство трябва да определи размера на ключовете в двойката ключове на картата от картовия сертификат.

2. Бордовото устройство изпраща на картата публичната точка $VU.PK_{eph}$ от своята двойка краткотрайни (ephemeral) ключове. Както е изяснено в CSM_164, бордовото устройство е генерирало тази двойка краткотрайни ключове преди проверката на неговата верига на сертифициране. Бордовото устройство е изпратило до картата краткотрайния публичен ключ $Comp(VU.PK_{eph})$ и картата го е съхранила.

3. Картата изчислява $Comp(VU.PK_{eph})$ от $VU.PK_{eph}$ и сравнява така получената стойност със съхранената стойност на $Comp(VU.PK_{eph})$.

4. Като използва алгоритъма ECDH в комбинация със своя статичен частен ключ и с краткотрайния публичен ключ на бордовото устройство, картата изчислява секретна стойност K.

5. После картата избира случаен 8-байтов еднократен код (nonce) N и го използва за да получи от K два сесийни ключа AES — K_{MAC} и K_{ENC}. Вж. CSM_179.

6. Използвайки K_{MAC}, картата изчислява автентификационен маркер (authentication token) върху идентификатора на кратковременния публичен ключ на бордовото устройство: T_{PICC} = CMAC (K_{MAC}, $VU.PK_{eph}$). Картата изпраща на бордовото устройство N_{PICC} и T_{PICC}.

7. Като използва алгоритъма ECDH в комбинация със статичния публичен ключ на картата и със своя краткотраен частен ключ, бордовото устройство изчислява същата секретна стойност K, която е изчислена от картата в стъпка 4.

8. Въз основа на K и N_{PICC} бордовото устройство извежда сесийните ключове K_{MAC} и K_{ENC}; вж. CSM_179.

9. Бордовото устройство проверява автентификационния маркер T_{PICC}.

CSM_177 В по-горната стъпка 3 картата трябва да изчисли Comp(VU.PKeph) като стойност на координатата x на публичната точка във VU.PKeph.

CSM_178 В по-горните стъпки 4 и 7 картата и бордовото устройство трябва да използват алгоритъма ECKA-EG, както е дефиниран в [TR-03111].

CSM_179 В по-горните стъпки 5 и 8 картата и бордовото устройство трябва да използват за определяне на сесийните ключове AES функцията за извеждане на ключове, дефинирана в [TR-03111], със следните уточнения и промени:

— Стойността на брояча трябва да бъде '00 00 00 01' за K_{ENC} и '00 00 00 02' за $K_{MAC.}$

— Трябва да се използва опционният еднократен код *r*, чиято стойност трябва да е равна на $N_{PICC.}$

— За извеждането на 128-битови ключове AES използваният алгоритъм за хеширане трябва да е SHA-256.

— За извеждането на 192-битови ключове AES използваният алгоритъм за хеширане трябва да е SHA-384.

— За извеждането на 256-битови ключове AES използваният алгоритъм за хеширане трябва да е SHA-512.

Дължината на сесийните ключове (т.е. дължината, при която се отрязва хеша) трябва да е свързана с размера на двойката ключове Card_MA, както е специфициран в CSM_50.

CSM_180 В по-горните стъпки 6 и 9 картата и бордовото устройство трябва да използват алгоритъма AES в режим CMAC, както е специфицирано в [SP 800-38B]. Дължината на T_{PICC} трябва да е свързана с дължината на сесийните ключове AES, както е специфицирано в CSM_50.

10.5. **Защитен обмен на съобщения**

10.5.1 *Общи положения*

CSM_181 Всички команди и отговори, които се разменят между бордово устройство и тахографска карта след успешно проведено удостоверяване на автентичността на чипа до края на сесията трябва да бъдат защитени чрез защитен обмен на съобщения.

CSM_182 Освен в случай на четене на файл с условие за достъп SM-R-ENC-MAC-G2 (вж. допълнение 2, раздел 4), защитеният обмен на съобщения трябва да се използва в режим „само с удостоверяване“. В този режим към всички команди и отговори се добавя криптографска контролна сума (наричана също MAC) за осигуряване на автентичността и цялостността на съобщенията.

CSM_183 При четенето на данни от файл с условие за достъп SM-R-ENC-MAC-G2, защитеният обмен на съобщения трябва да се използва в режим „криптиране с последващо автентифициране“, т.е. данните в отговорите първо се криптират за осигуряване на поверителност на съобщението и после върху форматираните криптирани данни се изчислява MAC за осигуряване на автентичност и цялостност.

CSM_184 За защитеният обмен на съобщения трябва да се използва AES, както е дефиниран в [AES], със сесийните ключове K_{MAC} и K_{ENC}, които са договорени при удостоверяването на автентичността на чипа.

CSM_185 С цел предотвратяване на атаки с повторно възпроизвеждане (replay attacks) трябва да се използва беззнаково цяло число в качеството на брояч на изпратените поредици (SSC). Размерът на SSC трябва да бъде равен на размера на AES блок, т.е. 128 бита. Форматът на SSC трябва да е с най-старшия бит на първо място (MSB-first format). При стартирането на защитения обмен на съобщения броячът на изпратените поредици трябва да бъде инициализиран с нулева стойност (т.е. '00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00'). Стойността на SSC трябва да нараства всеки път преди генерирането на командна или ответна APDU, т.е. след като началната стойност на SSC при сесия на защитен обмен на съобщения е 0, при първата команда стойността на SSC ще е 1. След това при първия отговор стойността на SSC ще е 2.

CSM_186 За криптиране на съобщенията трябва да се използва K_{ENC} с AES в работен режим на свързване на блокове от шифровани данни (CBC), както е дефиниран в [ISO 10116], с параметър на редуване (interleave parameter) m = 1 и инициализиращ вектор SV = E(K_{ENC}, SSC), т.е. текущата стойност на брояча на изпратените поредици, криптирана с K_{ENC}.

CSM_187 За автентифициране на съобщенията трябва да се използва K_{MAC} с AES в работен режим CMAC, както е специфициран в [SP 800-38B]. Дължината на MAC трябва да е свързана с дължината на сесийните ключове AES, както е специфицирано в CSM_50. Броячът на изпратените поредици трябва да бъде включен в MAC чрез добавянето му пред датаграмата, която ще се автентифицира.

10.5.2 *Структура на защитено съобщение*

CSM_188 При защитения обмен на съобщения трябва да се използват само обекти от данни за защитен обмен на съобщения (вж. [ISO 7816-4]), които са посочени в таблица 5. Тези обекти от данни трябва във всяко съобщение да се използват в реда, специфициран в следната таблица.

Таблица 5

Обекти от данни за защитен обмен на съобщения

Наименование на обекта от данни	Таг	Присъствие: Задължително(M), Условно(C) или Забранено (F) в	
		Команди	Отговори
Открита (plain) стойност, некодирана по BER-TLV	‘81’	C	C
Открита стойност, кодирана по BER-TLV, но невключваща обекти от данни за защитен обмен (SM DOs)	‘B3’	C	C
Индикатор за запълващото съдържание (padding-content indicator), открита (plain) стойност, некодирана по BER-TLV	‘87’	C	C
Защитена Le	‘97’	C	F
Състояние на обработка	‘99’	F	M
Криптографска контролна сума	‘8E’	M	M

Забележка: Както е с специфицирано в допълнение 2, възможно е тахографските карти да поддържат командите READ BINARY и UPDATE BINARY с нечетен INS байт (‘B1’, респективно ‘D7’). Тези варианти на командите са необходими за четене и актуализация на файлове с големина над 32 768 или повече байта. В случай че се използва такъв вариант, трябва да се използва обект от данни с таг ‘B3’ вместо обект от данни с таг ‘81’. За допълнителна информация вж. допълнение 2.

CSM_189 Всички обекти от данни при защитен обмен на съобщения трябва да бъдат кодирани в DER TLV, както е специфицирано в [ISO 8825-1]. Това кодиране води до следната структура Таг-Дължина-Стойност (TLV):

Таг: Тагът се кодира в един или два октета и показва съдържанието.

Дължина: Дължината се кодира като беззнаково цяло число в един, два или три октета, като в резултат максималната дължина е 65 535 октета. Използва се минималният брой октети.

Стойност: Стойността се кодира в нула или повече октети.

CSM_190 Единиците данни APDUs, защитени чрез защитен обмен на съобщения, трябва да бъдат създавани както следва:

— Заглавната част на командата (command header) трябва да бъде включена в изчислението на MAC, поради което трябва да бъде използвана стойността ‘0C’ за байта CLA за определяне на класа.

— Както е специфицирано в допълнение 2, всички INS байтове трябва да са четни, с възможно изключение за нечетни INS байтове за командите READ BINARY и UPDATE BINARY.

— След прилагането на защитен обмен на съобщения действителната стойност на Lc ще се измени на Lc’.

— Полето от данни ще се състои от обекти от данни за защитен обмен на съобщения (SM).

— В защитената командна APDU за байта за новата Le се задава ‘00’. Ако е необходимо, в полето за данни се включва обект от данни ‘97’ за представяне на първоначалната стойност на Le.

CSM_191 Всеки обект от данни, който ще се криптира, трябва да бъде запълнен в съответствие с [ISO 7816-4], като се използва индикатор за запълващо съдържание ‘01’. При изчисляването на MAC, всеки обект от данни в APDU трябва също да бъде запълнен поотделно, в съответствие с [ISO 7816-4].

Забележка: Запълването при защитен обмен на съобщения винаги се прави чрез слоя за защитен обмен на съобщения, а не чрез алгоритмите CMAC или CBC.

Обобщение и примери

Командната APDU с приложен защитен обмен на съобщения има следната структура, в зависимост от случая за съответната незащитена команда (DO означава обект от данни)

Случай 1:	CLA INS P1 P2 || Lc’ || DO ‘8E’ || Le
Случай 2:	CLA INS P1 P2 || Lc’ || DO ‘97’ || DO‘8E’ || Le
Случай 3 (четен INS байт):	CLA INS P1 P2 || Lc’ || DO ‘81’ || DO‘8E’ || Le
Случай 3 (нечетен INS байт):	CLA INS P1 P2 || Lc’ || DO ‘B3’ || DO‘8E’ || Le
Случай 4 (четен INS байт):	CLA INS P1 P2 || Lc’ || DO ‘81’ || DO‘97’ || DO‘8E’ || Le
Случай 4 (нечетен INS байт):	CLA INS P1 P2 || Lc’ || DO ‘B3’ || DO‘97’ || DO‘8E’ || Le

където Le = ‘00’ или ‘00 00’ в зависимост от това дали се използват полета с малка дължина или с увеличена дължина; вж. [ISO 7816-4].

Ответната APDU при защитен обмен на съобщения има следната структура, в зависимост от случая за съответния незащитен отговор:

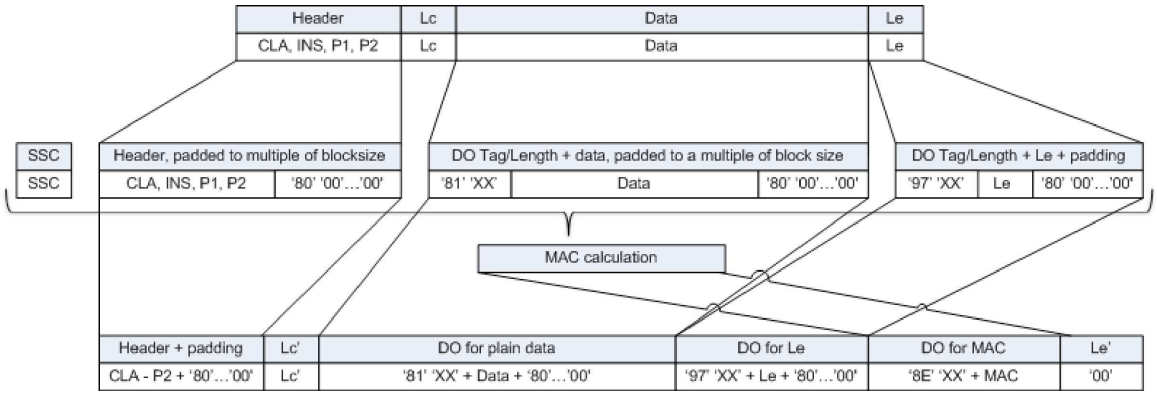
Случай 1 или 3:	DO ‘99’ || DO ‘8E’ || SW1SW2
Случай 2 или 4 (четен INS байт) с криптиране:	DO ‘81’ || DO ‘99’ || DO ‘8E’ || SW1SW2
Случай 2 или 4 (четен INS байт) без криптиране:	DO ‘87’ || DO ‘99’ || DO ‘8E’ || SW1SW2
Случай 2 или 4 (нечетен INS байт) без криптиране:	DO ‘B3’ || DO ‘99’ || DO ‘8E’ || SW1SW2

Забележка: случай 2 или 4 (нечетен INS байт) с криптиране никога не се използва при комуникацията между бордово устройство и карта.

По-долу са дадени три примера за преобразуване на командни APDU с четен INS код. На фигура 8 е показана автентифицирана командна APDU, случай 4, на фигура 9 е показана автентифицирана ответна APDU, случай 2/случай 4 и на фигура 10 е показана криптирана и автентифицирана ответна APDU, случай 2/случай 4.

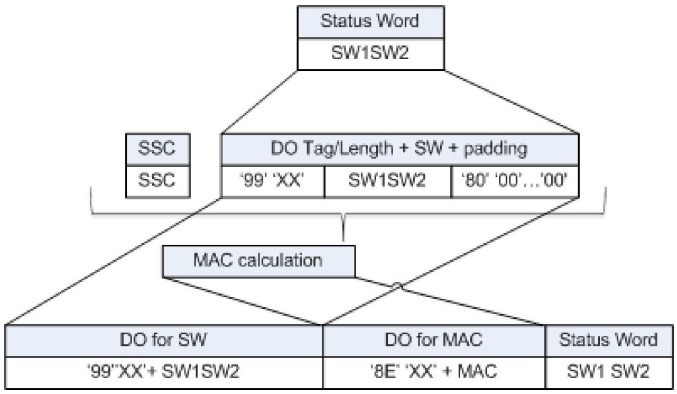
Фигура 8

Преобразуване на автентифицирана командна APDU, случай 4



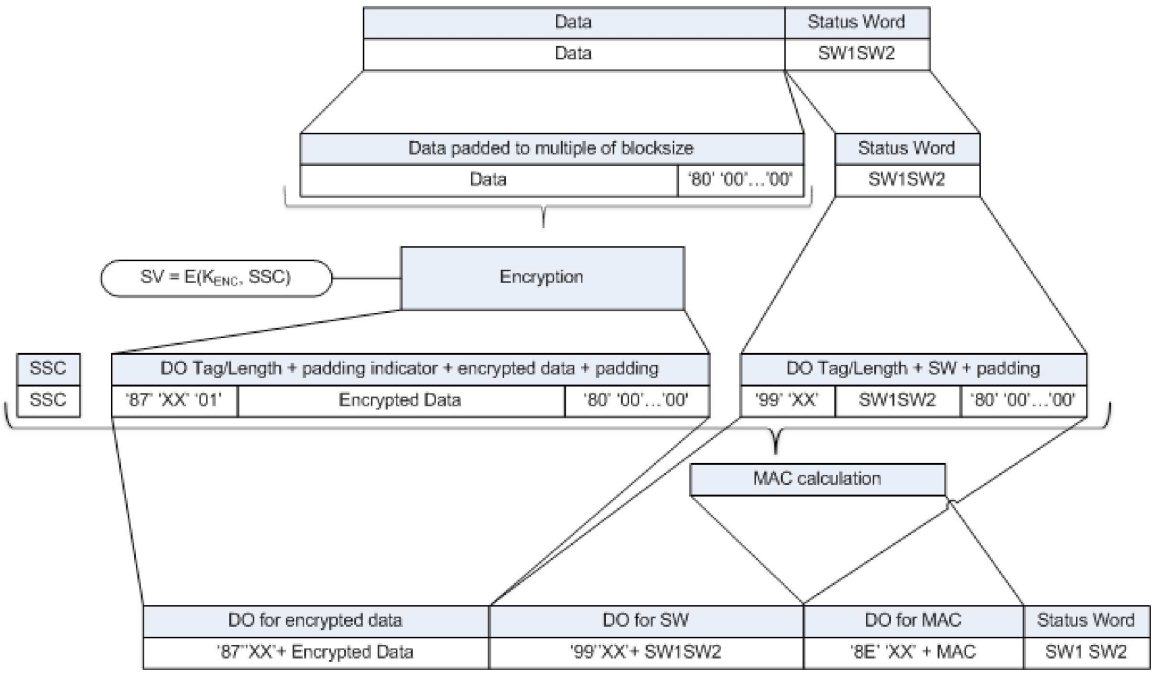
Фигура 9

Преобразуване на автентифицирана ответна APDU, случай 1/случай 3



Фигура 10

Преобразуване на криптирана и автентифицирана ответна APDU, случай 2/случай 4



10.5.3 *Прекратяване на сесия на защитен обмен на съобщения*

CSM_192 Бордовото устройство трябва да прекрати текуща сесия на защитен обмен на съобщения ако и само ако е изпълнено едно от следните условия:

— бордовото устройство получи ответна APDU в открит текст,

— бордовото устройство открие в ответна APDU грешка по отношение на защитения обмен на съобщения, както следва:

— Липсва очакван обект от данни за защитен обмен на съобщения, подреждането на обектите от данни е неправилно или е включен непознат обект от данни.

— Даден обект от данни за защитен обмен на съобщения е неправилен, например стойността на MAC е невярна, структурата на TLV е неправилна или индикаторът за запълване в таг ‘87’ не е равен на ‘01’.

— картата изпраща байт за състояние, показващ че тя е открила грешка в защитения обмен на съобщения (вж. CSM_194),

— достигнат е лимитът за броя на командите и съответните отговори в рамките на текущата сесия. Този лимит за дадено бордово устройство трябва да е определен от неговия производител, като се имат предвид изискванията за сигурност във връзка с използвания хардуер, с максимална стойност 240 команди и съответни отговори на сесия за защитен обмен на съобщения.

CSM_193 Тахографската карта трябва да прекрати текуща сесия на защитен обмен на съобщения ако и само ако е изпълнено едно от следните условия:

— тахографската карта получи ответна APDU в открит текст,

— тахографската карта открие в ответна APDU грешка по отношение на защитения обмен на съобщения, както следва:

— Липсва очакван обект от данни за защитен обмен на съобщения, подреждането на обектите от данни е неправилно или е включен непознат обект от данни.

— Даден обект от данни за защитен обмен на съобщения е неправилен, например стойността на MAC е невярна или структурата на TLV е неправилна.

— тахографската карта е без захранване (depowered) или е инициализирана (reset),

— бордовото устройство избере приложение в картата,

— бордовото устройство започне процес на удостоверяване на автентичността на бордово устройство

— достигнат е лимитът за броя на командите и съответните отговори в рамките на текущата сесия. Този лимит за дадена карта трябва да е определен от нейния производител, като се имат предвид изискванията за сигурност във връзка с използвания хардуер, с максимална стойност 240 команди и съответни отговори на сесия за защитен обмен на съобщения.

CSM_194 Относно реагирането на тахографска карта при грешка в защитения обмен на съобщения.

— Ако в дадена командна APDU липсват някои очаквани обекти от данни за защитен обмен на съобщения, подреждането на обектите от данни е неправилно или са включени непознати обекти от данни, тахографската карта трябва да отговори с байтове за състояние ‘69 87’.

— Ако обект от данни за защитен обмен на съобщения в командна APDU е неправилен, тахографската карта трябва да отговори с байтове за състояние ‘69 88’.

В такъв случай байтовете за състояние се изпращат обратно без използване на защитен обмен на съобщения.

CSM_195 Ако бъде прекратена сесия на защитен обмен на съобщения между бордово устройство и тахографска карта, бордовото устройство и тахографската карта трябва:

— да унищожат по сигурен начин съхранените сесионни ключове

— веднага да създадат нова сесия за защитен обмен на съобщения, както е описано в раздели 10.2 — 10.5.

CSM_196 Ако по някаква причина бордовото устройство реши да рестартира взаимното удостоверяване на автентичност с вкарана карта, процесът трябва да рестартира с проверка на веригата на сертифициране на картата, както е описано в раздел 10.2, и да продължи както е описано в раздели 10.2 — 10.5.

11. КУПЛИРАНЕ БОРДОВО УСТРОЙСТВО — ВЪНШНО УСТРОЙСТВО ЗА GNSS, ВЗАИМНО УДОСТОВЕРЯВАНЕ НА АВТЕНТИЧНОСТТА И ЗАЩИТЕН ОБМЕН НА СЪОБЩЕНИЯ

11.1. **Общи положения**

CSM_197 Устройството за GNSS, използвано от бордово устройство за определяне на местоположението му, може да бъде вътрешно (т.е. вградено в корпуса на бордовото устройство и неотделящо се) или да представлява външен модул. В първия случай не е необходимо да се стандартизира вътрешната комуникация между устройството за GNSS и бордовото устройство и изискванията в настоящата глава не се отнасят за него. Във втория случай комуникацията между бордовото устройство и външното устройство за GNSS трябва да бъде стандартизирана и защитена, както е описано в настоящата глава.

CSM_198 Защитената комуникация между бордово устройство и външно устройство за GNSS трябва да се извършва по същия начин както защитената комуникация между бордово устройство и тахографска карта, като външното устройство за GNSS (EGF) е в ролята на картата. EGF трябва да изпълнява всички изисквания, посочени в глава 10 за тахографските карти, като се имат предвид посочените в настоящата глава отклонения, изяснения и допълнения. По-специално, взаимната проверка на веригата на сертифициране, удостоверяването на автентичността на бордовото устройство и на чипа трябва да бъдат извършвани както е описано в раздели 11.3 и 11.4.

CSM_199 Комуникацията между бордово устройство и EGF се различава от комуникацията между бордово устройство и карта поради факта, че дадено бордово устройство и EGF трябва да бъдат вече куплирани веднъж в завод/сервиз, преди те да могат да обменят базиращи се на GNSS данни при нормална работа. Процесът на куплирането е описан в раздел 11.2.

CSM_200 При комуникацията между бордово устройство и EGF трябва да се използват командните и ответните APDU, базиращи се на [ISO 7816-4] и [ISO 7816-8]. Точната структура на тези APDU е дефинирана в допълнение 2 към настоящото приложение.

11.2. **Куплиране на бордово устройство с външно устройство за GNSS**

CSM_201 Бордовото устройство и EGF в дадено превозно средство трябва да бъдат куплирани от завод/сервиз (by a workshop). При нормална работа могат да комуникират само куплирани бордово устройство и EGF.

CSM_202 Куплирането на бордово устройство и EGF трябва да е възможно само ако бордовото устройство е в режим на калибриране. Куплирането трябва да се инициира от бордовото устройство.

CSM_203 В завод/сервиз (workshop) може по всяко време да се рекуплира дадено бордово устройство с друго или със същото EGF. При рекуплирането бордовото устройство трябва в сигурен режим да унищожи съществуващия сертификат EGF_MA в своята памет и да съхрани сертификата EGF_MA на съответното EGF, с което се куплира.

CSM_204 В завод/сервиз (workshop) може по всяко време да се рекуплира дадено устройство за GNSS с друго или със същото бордово устройство. При рекуплирането EGF трябва в сигурен режим да унищожи съществуващия сертификат VU_MA в своята памет и да съхрани сертификата VU_MA на съответното бордово устройство, с което се куплира.

11.3. **Взаимна проверка на веригата на сертифициране**

11.3.1 *Общи положения*

CSM_205 Взаимната проверка на веригата на сертифициране между бордово устройство и EGF трябва да се провежда само по време на куплирането на бордовото устройство и EGF от завод/сервиз (workshop). При нормална работа на куплирани бордово устройство и EGF не се прави проверка на сертификати. Вместо това бордовото устройство и EGF трябва да се доверяват на сертификатите, които са съхранили по време на куплирането, след като проверят валидността във времето на тези сертификати. Бордовото устройство и EGF не се доверяват на никакви други сертификати за защита на комуникацията бордово устройство — EGF при нормална работа.

11.3.2 *По време на куплирането бордово устройство — EGF*

CSM_206 При куплирането си към EGF бордовото устройство трябва да използва протокола, описан във фигура 4 (раздел 10.2.1), за проверка на веригата на сертифициране на външното устройство за GNSS.

Забележки в този контекст към фигура 4:

— Управлението на комуникацията е извън обхвата на настоящото допълнение. Но все пак EGF не е карта с чип и поради това бордовото устройство вероятно няма да изпраща команда Reset за иницииране на комуникация и няма да получава ATR.

— Посочените във фигурата картови сертификати и публични ключове трябва да се интерпретират като сертификати и публични ключове на EGF за взаимно удостоверяване на автентичността. В раздел 9.1.6 те са означени като EGF_MA.

— Посочените във фигурата Card.CA сертификати и публични ключове трябва да се интерпретират като сертификати и публични ключове на MSCA за подписване на сертификатите на EGF. В раздел 9.1.3 те са означени като MSCA_VU-EGF.

— Упоменатият във фигурата сертификат Card.CA.EUR трябва да се интерпретира като европейския основен сертификат, който е посочен в референтното означение на сертифициращия орган (CAR) на сертификата MSCA_VU-EGF.

— Упоменатият във фигурата сертификат Card.Link трябва да се интерпретира като свързващия сертификат на EGF, ако има такъв. Както е посочено в 9.1.2, това е свързващ сертификат за нова европейска двойка основни ключове, създадена от ERCA и подписана с предходния европейски частен ключ.

— Сертификатът Card.Link.EUR е европейският основен сертификат, който е посочен в референтното означение на сертифициращия орган (CAR) на сертификата Card.Link.

— Вместо `cardExtendedSerialNumber`, бордовото устройство трябва да прочете `sensorGNSSserialNumber` от EF ICC.

— Вместо да избере Tachograph AID, бордовото устройство трябва да избере EGF AID.

— 'Ignore Card' трябва да се интерпретира като 'Ignore EGF'.

CSM_207 След като веднъж е проверило сертификата EGF_MA, бордовото устройство трябва да съхрани този сертификат за използване при нормална работа; вж. раздел 11.3.3.

CSM_208 При куплирането си към бордово устройство, външното устройство за GNSS трябва да използва протокола, описан във фигура 5 (раздел 10.2.2), за проверка на веригата на сертифициране на бордовото устройство.

Забележки в този контекст към фигура 5:

— Бордовото устройство трябва да генерира свежа (fresh) двойка краткотрайни ключове, използвайки домейн параметрите в сертификата на EGF.

— Упоменатите във фигурата сертификати и публични ключове VU са тези, които се използват за взаимно удостоверяване на автентичността. В раздел 9.1.4 те са означени като VU_MA.

— Упоменатите във фигурата сертификати и публични ключове VU.CA са тези, които се използват за подписване на сертификати на бордови устройства и на външни устройства за GNSS. В раздел 9.1.3 те са означени като MSCA_VU-EGF.

— Упоменатият във фигурата сертификат VU.CA.EUR е европейският основен сертификат, който е посочен в референтното означение на сертифициращия орган (CAR) на сертификата VU.CA.

— Упоменатият във фигурата сертификат VU.Link е свързващият сертификат на бордовото устройство, ако има такъв. Както е посочено в 9.1.2, това е свързващ сертификат за нова европейска двойка основни ключове, създадена от ERCA и подписана с предходния европейски частен ключ.

— Сертификатът VU.Link.EUR е европейският основен сертификат, който е посочен в референтното означение на сертифициращия орган (CAR) на сертификата VU.Link.

CSM_209 В отклонение от изискването CSM_167, EGF трябва да използва отчитаното от GNSS време за проверка на валидността във времето на всеки представен сертификат.

CSM_210 След като веднъж е проверило сертификата VU_MA, външното устройство за GNSS трябва да съхрани този сертификат за използване при нормална работа; вж. раздел 11.3.3.

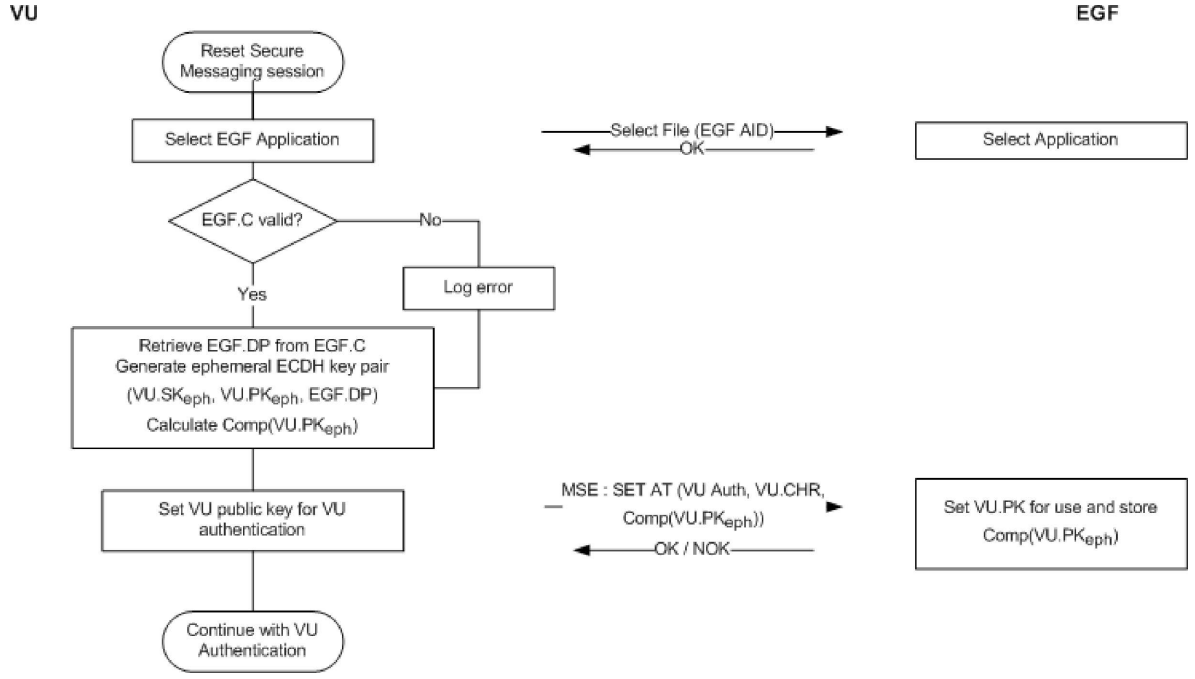
11.3.3 *При нормална работа*

CSM_211 При нормална работа дадено бордово устройство и EGF трябва да използват протокола, описан във фигура 11, за проверка на валидността във времето на съхранените сертификати EGF_MA и VU_MA и за задаване на публичния ключ VU_MA за последващо автентифициране на бордовото устройство. При нормална работа не трябва да се прави по-нататъшна взаимна проверка на веригите за сертифициране.

Забележете, че по същество фигура 11 се състои от първите стъпки, посочени в фигура 4 и фигура 5. И още веднъж, имайте предвид че тъй като EGF не е карта с чип, бордовото устройство вероятно няма да изпраща команда Reset за иницииране на комуникация и няма да получава ATR. При всички случаи това е извън обхвата на настоящото допълнение.

Фигура 11

Взаимна проверка на валидността във времето на сертификатите при нормална работа VU — EGF



CSM_212 Както е показано във фигура 11, в случай че сертификатът EGF_MA вече не е валиден, бордовото устройство трябва да регистрира грешка. Въпреки това, взаимното удостоверяване на автентичността, договарянето на ключовете и последващата комуникация посредством защитен обмен на съобщения трябва да продължат нормално.

11.4. Автентифициране на бордовото устройство, автентифициране на чипа и договаряне на сесийни ключове

CSM_213 Автентифицирането на бордовото устройство, автентифицирането на чипа и договарянето на сесийни ключове между бордово устройство и EGF трябва да се прави по време на куплирането и по време на последващо влизане в сесия за защитен обмен на информация при нормална работа. Бордовото устройство и EGF трябва да изпълняват процесите, описани в раздели 10.3 и 10.4. Валидни са всички изисквания, описани в тези раздели.

11.5. Защитен обмен на съобщения

CSM_214 Всички команди и отговори, които се разменят между бордово устройство и външното устройство за GNSS след успешно проведено удостоверяване на автентичността на чипа до края на сесията трябва да бъдат защитени чрез защитен обмен на съобщения. Валидни са всички изисквания, описани в раздел 10.5.

CSM_215 Ако дадена сесия за защитен обмен на съобщения между бордово устройство и EGF бъде прекратена, бордовото устройство трябва веднага да създаде нова сесия за защитен обмен на съобщения, както е описано в раздели 11.3.3 и 11.4.

12. СДВОЯВАНЕ И КОМУНИКАЦИЯ БОРДОВО УСТРОЙСТВО — ДАТЧИК ЗА ДВИЖЕНИЕ

12.1. **Общи положения**

CSM_216 Бордовото устройство и датчикът за движение трябва да комуникират при сдвояване и нормална работа като използват интерфейсния протокол, специфициран в [ISO 16844-3], в съответствие с измененията, описани в настоящата глава и в раздел 9.2.1.

Забележка: читателите на настоящата глава следва да са запознати със съдържанието на [ISO 16844-3].

12.2. **Сдвояване бордово устройство — датчик за движение с използване на различни поколения ключове**

Както е изяснено в раздел 9.2.1, главният ключ на датчика за движение и всички свързани с него ключове редовно се заменят. Това води до наличието в картите за монтаж и настройка на до три свързани с датчика на движение AES ключа K_{M-WC} (от последователни поколения ключове). Подобно на това, в датчиците за движение могат да присъстват до три различни базиращи се на AES криптирания на данни (на базата на последователни поколения на главния ключ на датчика за движение K_M). Бордовото устройство съдържа само един свързан с датчика за движение ключ $K_{M-VU.}$

CSM_217 Бордово устройство от второ поколение и датчик за движение от второ поколение трябва да бъдат сдвоявани както следва (сравнете с посоченото в таблица 6 от [ISO 16844-3]):

1. В бордовото устройство се вкарва карта за монтаж и настройки от второ поколение и бордовото устройство се свързва с датчика за движение.

2. Бордовото устройство прочита всички налични ключове K_{M-WC} от картата за монтаж и настройки, инспектира техните номера на версии и избира един от тях, който съответства на номера на версията на ключа K_{M-VU} в бордовото устройство. Ако в картата за монтаж и настройки липсва съответстващ ключ K_{M-WC}, бордовото устройство прекратява процеса на сдвояване и показва на титуляря на картата за монтаж и настройки подходящо съобщение за грешка.

3. Въз основа на K_{M-VU} и K_{M-WC} бордовото устройство изчислява главния ключ на датчика за движение K_M и съответно от K_M изчислява K_{ID}, както е специфицирано в раздел 9.2.1.

4. Бордовото устройство изпраща на датчика за движение инструкцията за иницииране на процес на сдвояване, както е описано в [ISO 16844-3], и криптира получения от датчика за движение сериен номер с идентификационния ключ $K_{ID.}$ След това бордовото устройство изпраща криптирания сериен номер обратно на датчика за движение.

5. Датчикът за движение сравнява криптирания сериен номер последователно с всеки от криптираните серийни номера, които той съдържа вътре в себе си. Ако се установи съответствие, бордовото устройство е автентифицирано. Датчикът за движение отбелязва генерирането на K_{ID}, използван от бордовото устройство, и връща съответстващата криптирана версия на своя ключ за сдвояване; т.е. криптирането, създадено с използване на същото поколение K_M.

6. Бордовото устройство декриптира ключа за сдвояване като използва K_M, създава сесиен ключ $K_{S,}$ криптира го с ключа за сдвояване и изпраща така получения резултат на датчика за движение. Датчикът за движение декриптира K_S.

7. Бордовото устройство информацията за сдвояване, както е дефинирана в [ISO 16844-3], криптира информацията с ключа за сдвояване и изпраща резултата на датчика за движение. Датчикът за движение декриптира информацията за сдвояване.

8. След това датчикът за движение криптира получената информация за сдвояване с получения ключ K_S и я връща на бордовото устройство. Бордовото устройство проверява дали информацията за сдвояване е същата като тази, която то е изпратило на датчика за движение при предишната стъпка. Ако е така, това доказва че датчикът за движение е използвал същия ключ K_S като бордовото устройство и следователно в стъпка 5 е изпратило своя ключ за сдвояване, криптиран с правилното поколение K_M. По този начин датчикът за движение е автентифициран.

Забележете, че стъпки 2 и 5 са различни от стандартния процес в [ISO 16844-3]; останалите стъпки са същите като в стандарта.

Пример: Да предположим, че сдвояването се провежда в първата година на валидност на сертификата ERCA (3); вж. фигура 2 в раздел 9.2.1.2. Освен това,

— Да предположим, че датчикът за движение е издаден в последната година на валидност на сертификата ERCA (1). Следователно той ще съдържа следните ключове и данни:

  — $N_s[1]$: неговият сериен номер, криптиран с K_{ID} от поколение 1,

  — $N_s[2]$: неговият сериен номер, криптиран с K_{ID} от поколение 2,

  — $N_s[3]$: неговият сериен номер, криптиран с K_{ID} от поколение 3,

  — $K_P[1]$: неговият ключ за сдвояване от поколение 1 ([1]), криптиран с K_M от поколение 1,

  — $K_P[2]$: неговият ключ за сдвояване от поколение 2, криптиран с K_M от поколение 2,

  — $K_P[3]$: неговият ключ за сдвояване от поколение 3, криптиран с K_M от поколение 2,

— Да предположим, че картата за монтаж и настройки е издадена в първата година на валидност на сертификата ERCA (3). В такъв случай тя ще съдържа поколение 2 и поколение 3 на ключа $K_{M\text{-}WC}$.

— Да предположим, че бордовото устройство е от поколение 2 и съдържа поколение 2 на ключа $K_{M\text{-}VU}$.

В такъв случай при стъпки 2 — 5 ще се случи следното:

— Стъпка 2: Бордовото устройство прочита от картата за монтаж и настройки поколение 2 и поколение 3 на ключа $K_{M\text{-}WC}$ и инспектира техните номера на версии.

— Стъпка 3: Бордовото устройство комбинира ключа $K_{M\text{-}WC}$ от поколение 2 със своя ключ $K_{M\text{-}VU}$ за да изчисли K_M и K_{ID}.

— Стъпка 4: Бордовото устройство криптира с K_{ID} серийния номер, получен от датчика за движение.

— Стъпка 5: Датчикът за движение сравнява получените данни с $N_s[1]$ и не намира съответствие. След това той сравнява данните с $N_s[2]$ и установява съответствие. Прави заключението, че бордовото устройство е от поколение 2 и поради това изпраща обратно $K_P[2]$.

12.3. **Сдвояване и връзка бордово устройство — датчик за движение с използване на AES**

CSM_218 Както е специфицирано в таблица 3 в раздел 9.2.1, всички ключове, участващи в сдвояване на бордово устройство (от второ поколение) и датчик за движение, както и в последващата комуникация, трябва по-скоро да са AES ключове, а не TDES ключове с двойна дължина, както е специфицирано в [ISO 16844-3]. Тези AES ключове могат да са с дължина 128, 192 или 256 бита. Тъй като размерът на AES блока е 16 байта, дължината на криптираното съобщение трябва да е кратна на 16 байта, докато при TDES тя трябва да е кратна на 8 байта. Също така, някои от тези съобщения ще бъдат използвани за маршрутизиране на AES ключове, чиято дължина може да е 128, 192 или 256 бита. Следователно, броят на байтовете данни за една инструкция, посочен в Таблица 5 от [ISO 16844-3], трябва да бъде променен, както е показано в таблица 6:

Таблица 6

Брой на байтовете данни в открит текст и на криптираните байтове данни за една инструкция, дефиниран в [ISO 16844-3]

Инструкция	Заявка / отговор	Описание на данните	# на байтовете данни в открит текст съгласно [ISO 16844-3]	# на байтовете данни в открит текст, използващи AES ключове	# на криптираните байтове данни, използващи AES ключове с дължина в битове		
					128	192	256
10	Заявка	Данни за автентифициране + номер на файла	8	8	16	16	16

([1]) Забележете, че ключовете за сдвояване от поколение 1, 2 и 3 могат реално да са един и същ ключ, или три различни ключа с различни дължини, както е изяснено в CSM_117.

Инструкция	Заявка / отговор	Описание на данните	# на байтовете данни в открит текст съгласно [ISO 16844-3]	# на байтовете данни в открит текст, използващи AES ключове	# на криптираните байтове данни, използващи AES ключове с дължина в битове		
					128	192	256
11	Отговор	Данни за автентифициране + номер на файла	16 или 32, зависи от файла	16 или 32, зависи от файла	16 / 32	16 / 32	16 / 32
41	Заявка	Сериен номер на MoS	8	8	16	16	16
41	Отговор	Ключ за сдвояване	16	16 / 24 / 32	16	32	32
42	Заявка	Сесиен ключ	16	16 / 24 / 32	16	32	32
43	Заявка	Информация за сдвояване	24	24	32	32	32
50	Отговор	Информация за сдвояване	24	24	32	32	32
70	Заявка	Данни за автентифициране	8	8	16	16	16
80	Отговор	Стойност на брояча на MoS + данни за автент.	8	8	16	16	16

CSM_219 Информацията за сдвояване, изпращана с инструкции номер 43 (заявка от бордовото устройство) и номер 50 (отговор от датчика за движение) трябва да бъде събрана, както е специфицирано в раздел 7.6.10 от [ISO 16844-3], с тази разлика, че в схемата за криптиране на данните за сдвояване се използва алгоритъмът AES вместо алгоритъма TDES, като по този начин се получават две криптирания AES и се възприема специфицираното в CSM_220 запълване, за да има съответствие с размера на AES блок. Използваният за това криптиране ключ K'_P трябва да бъде генериран както следва:

— В случай, че ключът за сдвояване K_P е с дължина 16 байта: $K'_P = K_P \text{ XOR } (N_s||N_s)$

— В случай, че ключът за сдвояване K_P е с дължина 24 байта: $K'_P = K_P \text{ XOR } (N_s||N_s||N_s)$

— В случай, че ключът за сдвояване K_P е с дължина 32 байта: $K'_P = K_P \text{ XOR } (N_s||N_s||N_s||N_s)$

където N_s е 8-байтовият сериен номер на датчика за движение.

CSM_220 В случай че дължината на данните в открит текст (при използване на AES ключове) не е кратна на 16 байта, трябва да се използва методът на запълване номер 2, дефиниран в [ISO 9797-1].

Забележка: В [ISO 16844-3] броят на байтовете данни в открит текст е винаги кратен на 8 и поради това когато се използва TDES не е необходимо да се прави запълване. С тази част на настоящото допълнение не се променя дефиницията на данни и съобщения от [ISO 16844-3] и поради това се появява необходимост да се прилага запълване.

CSM_221 За инструкция 11 и в случай, че трябва да бъде криптиран повече от един блок данни, трябва да бъде използван работният режим на свързване на блокове шифровани данни (Cipher Block Chaining), дефиниран в [ISO 10116], с параметър на редуване (interleave parameter) $m = 1$. Използваният инициализиращ вектор трябва да бъде както следва:

— За инструкция 11: 8-байтовият автентифициращ блок, специфициран в раздел 7.6.3.3 от [ISO 16844-3], запълнен с използване на метода за запълване номер 2, дефиниран в [ISO 9797-1]; вж. също раздели 7.6.5 и 7.6.6 от [ISO 16844-3].

— За всички други инструкции, при които се прехвърлят повече от 16 байта, както е специфицирано в таблица 6: '00' {16}, т.е. шестнадесет байта с бинарна стойност 0.

Забележка: Както е показано в раздел 7.6.5 и 7.6.6 от [ISO 16844-3], когато бордовото устройство криптира файлове с данни за включване в инструкция 11, автентифициращият блок едновременно:

— се използва като инициализиращ вектор за криптиране в режим CBC на файловете с данни

— се криптира и включва като първия блок с данни, който се изпраща на бордовото устройство.

12.4. **Сдвояване бордово устройство — датчик за движение при различни поколения на оборудването**

CSM_222 Както е изяснено в раздел 9.2.1, даден датчик за движение от второ поколение може да съдържа криптиране на база TDES на данните за сдвояване (както е дефинирано в част A от настоящото допълнение), което дава възможност този датчик за движение да бъде сдвоен с бордово устройство от първо поколение. Ако случаят е такъв, бордовото устройство от първо поколение и датчикът за движение от второ поколение трябва да бъдат сдвоени както е описано в част A от настоящото допълнение и в [ISO 16844-3]. За процеса на сдвояване може да бъде използвана карта за монтаж и настройки или от първо, или от второ поколение.

Забележки:

— Не е възможно сдвояване на бордово устройство от второ поколение с датчик за движение от първо поколение.

— Не е възможно да се използва карта за монтаж и настройки от първо поколение за куплиране към датчик за движение на бордово устройство от второ поколение.

13. СИГУРНОСТ ПРИ ВРЪЗКА ОТ РАЗСТОЯНИЕ ПО DSRC

13.1. **Общи положения**

Както е специфицирано в допълнение 14, бордовото устройство редовно генерира данни за дистанционен мониторинг на тахографа (Remote Tachograph Monitoring — RTM) и изпраща тези данни на (вътрешно или външно) устройство за връзка от разстояние (Remote Communication Facility — RCF). Устройството за връзка от разстояние има за задача да изпраща тези данни по описаната в допълнение 14 DSRC до дистанционното разпитващо устройство. В допълнение 1 е посочено, че RTM данните представляват конкатенация на:

Криптирани полезни данни от тахографа (криптирането на откритият текст на полезните данни от тахографа)

Данни за сигурността на DSRC (описани по-долу)

Форматът на тахографските полезни данни в открит текст е специфициран в допълнение 1 и доуточнен в допълнение 14. В настоящата секция е описана структурата на данните за сигурността на DSRC; официалната спецификация е в допълнение 1.

CSM_223 Данните `tachographPayload` в открит текст, които се съобщават от бордово устройство на устройство за връзка от разстояние (RCF — ако това устройство е външно за бордовото устройство) или от бордово устройство на дистанционно разпитващо устройство по DSRC интерфейс (ако RCF е вътрешно устройство в бордовото устройство) трябва да бъдат защитени в режим „криптиране с последващо автентифициране“, т.е. тахографските полезни данни първо се криптират за да се осигури поверителността на съобщението и след това се изчислява автентификационен код (MAC) за съобщението, за да се осигури автентичност и цялостност на данните.

CSM_224 Данните за сигурността на DSRC трябва да представляват конкатенация на следните елементи от данни в следния ред; вж. също фигура 12:

Текуща дата и час (текущата дата и час на бордовото устройство (тип данни `TimeReal`))

Брояч (3-байтов брояч, вж. CSM_225)

Сериен номер на бордовото устройство (серийният номер на бордовото устройство (тип данни `VuSerialNumber`))

номер на версията на главния ключ за DSRC (1-байтовият номер на версията на главния ключ за DSRC, от който са изведени специфични за бордовото устройство ключове за DSRC, вж. раздел 9.2.2.)

MAC (Стойността на MAC, изчислена върху всички предходни байтове в RTM данните).

CSM_225 3-байтовият брояч в данните за сигурността на DSRC трябва да бъде във формат с най-старшия байт на първо място (MSB-first format). Когато дадено бордово устройство за пръв път изчислява набор от RTM данни след неговото влизане в експлоатация, стойността в брояча му трябва да е настроена да е 0. Бордовото устройство трябва да увеличава стойността в брояча на данните с 1 преди всяко изчисление от него на нов набор от RTM данни.

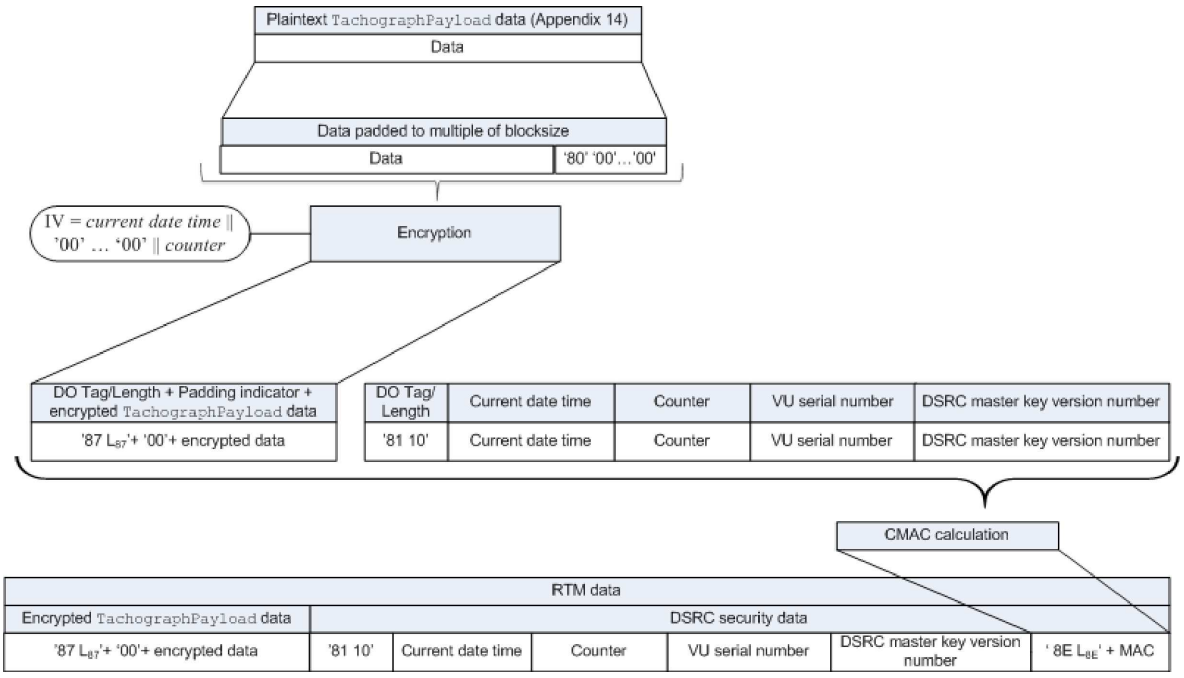
13.2. Криптиране на полезните тахографски данни и генериране на MAC

CSM_226 При даден елемент от данни в открит текст от типа `TachographPayload`, както е описан в допълнение 14, съответното бордово устройство трябва да криптира тези данни, както е показано на фигура 12: криптиращият DSRC ключ на бордовото устройство $K\_VU_{DSRC}\_ENC$ (вж. раздел 9.2.2) трябва да бъде използван с AES в работен режим на свързване на блокове шифровани данни (CBC), както е дефиниран в [ISO 10116], с параметър на редуване (interleave parameter) $m = 1$. Инициализиращият вектор трябва да бъде *IV = current date time || '00 00 00 00 00 00 00 00' || counter*, където *current date time* и *counter* са специфицирани в CSM_224. Данните за криптиране трябва да бъдат запълнени с използване на метод 2, дефиниран в [ISO 9797-1].

CSM_227 Бордовото устройство трябва да изчисли MAC за данните за сигурността на DSRC, както е показано във фигура 12: MAC трябва да бъде изчислен върху всички предходни байтове в RTM данните, до и включително с номера на версията на главния ключ за DSRC, както и включително с таговете и дължините на обектите от данни. Бордовото устройство трябва да използва своя DSRC ключ за автентификация $K\_VU_{DSRC}\_MAC$ (вж. раздел 9.2.2) с алгоритъма AES в режим CMAC, както е специфицирано в [SP 800-38B]. Дължината на MAC трябва да е свързана с дължината на специфичните за бордовото устройство DSRC ключове, както е специфицирано в CSM_50.

Фигура 12

Криптиране на полезните тахографски данни и генериране на MAC



13.3. **Проверка и декриптиране на полезни тахографски данни**

CSM_228 Когато дадено дистанционно разпитващо устройство получи от бордово устройство RTM данни, то трябва да изпрати всички тези данни на контролна карта в полето за данни на команда PROCESS DSRC MESSAGE, както е описано в допълнение 2. Тогава:

1. Контролната карта трябва да инспектира номера на версията на главния ключ за DSRC в данните за сигурността на DSRC. Ако контролната карта не познава посочения главен ключ за DSRC, тя трябва да върне съобщение за грешка, което е специфицирано в допълнение 2, и да прекрати процеса.

2. Контролната карта трябва да използва посочения главен ключ DSRC в комбинация със серийния номер на бордовото устройство в данните за сигурността на DSRC, за да изведе специфичните за бордовото устройство ключове K_VU_{DSRC}_ENC и K_VU_{DSRC}_MAC, както е специфицирано в CSM_124.

3. Контролната карта трябва да използва ключа K_VU_{DSRC}_MAC за да провери MAC в данните за сигурността на DSRC, както е специфицирано в CSM_227. Ако MAC не е верен, контролната карта трябва да върне съответното съобщение за грешка, специфицирано в допълнение 2 и да прекрати процеса.

4. Контролната карта трябва да използва ключа K_VU_{DSRC}_ENC за да декриптира криптираните тахографски полезни данни, както е специфицирано в CSM_226. Контролната карта трябва да отстрани запълването и да върне декриптираните тахографски полезни данни на дистанционното разпитващо устройство.

CSM_229 С цел предотвратяване на атаки с повторно възпроизвеждане (replay attacks) дистанционното разпитващо устройство трябва да проверява свежестта (freshness) на данните RTM чрез проверка дали стойността *current date time* в данните за сигурността на DSRC не се отклонява прекалено много от текущото време според дистанционното разпитващо устройство.

Забележки:

— За тази цел е необходимо дистанционното разпитващо устройство да разполага с точен и надежден източник за отчитане на времето.

— Като се има предвид, че в допълнение 14 има изискване бордовото устройство да изчислява нов набор от RTM данни на всеки 60 секунди и че за часовника на бордовото устройство е допустимо да се отклонява с 1 минута от действителното време, долната граница за свежест на данните RTM е 2 минути. Действителната стойност на свежестта зависи също от точността на часовника на дистанционното разпитващо устройство.

CSM_230 Когато даден завод/сервиз (workshop) проверява правилното действие на DSRC функционалността на дадено бордово устройство, той трябва да изпрати всички RTM данни, които е получил от бордовото устройство, до карта за монтаж и настройка в полето за данни на команда PROCESS DSRC MESSAGE, както е описано в допълнение 2. Картата за монтаж и настройки трябва да изпълни всички проверки и дейности, специфицирани в CSM_228.

14. ПОДПИСВАНЕ НА ИЗТЕГЛЕНИ ДАННИ И ПРОВЕРКА НА ПОДПИСИТЕ

14.1. **Общи положения**

CSM_231 Специализираното интелигентно устройство (IDE) трябва да записва в един физически файл данните, получени от бордово устройство или карта в рамките на една сесия на изтегляне на данни. Данните могат да бъдат съхранени върху външно запаметяващо устройство (ESM). Гореспоменатият файл съдържа електронни подписи върху блоковете данни, както е специфицирано в допълнение 7. Този файл трябва да съдържа също следните сертификати (вж. раздел 9.1):

— В случай на изтегляне на данни от бордово устройство:

— Сертификата VU_Sign

— Сертификата MSCA_VU-EGF, съдържащ публичния ключ, който се използва за проверяване на сертификата VU_Sign

— В случай на изтегляне на данни от карта:

— Сертификата Card_Sign

— Сертификата MSCA_Card, съдържащ публичния ключ, който се използва за проверяване на сертификата Card_Sign

CSM_232 Специализираното интелигентно устройство трябва да разполага също със следните сертификати в съответните случаи:

— В случай че използва контролна карта за проверка на подпис, както е показано във фигура 13 — със свързващият сертификат, който свързва последния EUR сертификат с този EUR сертификат, чийто период на валидност е непосредствено предхождащ, ако има такъв.

— В случай, че проверява самия подпис — с всички валидни европейски основни сертификати.

Забележка: В настоящото допълнение не е специфициран методът, който да се използва от IDE за придобиване на тези сертификати.

14.2. **Генериране на подпис**

CSM_233 Използваният от бордовото устройство алгоритъм за подписване при автентифицирането на бордовото устройство трябва да бъде ECDSA, както е специфициран в [DSS], с използване на алгоритъма за хеширане, свързан с размера на ключа на бордовото устройство или на картата, както е специфицирано в CSM_50. Форматът на подписа трябва да бъде открит (plain), както е специфицирано в [TR-03111].

14.3. **Проверка на подписа**

CSM_234 Дадено IDE може самото то да извършва проверка на подпис върху изтеглени данни, или да използва за тази цел контролна карта. В случай че използва контролна карта, проверката на подписа трябва да бъде направена както е показано във фигура 13. В случай че самото IDE прави проверките на подписа, то трябва да провери автентичността и валидността на всички сертификати в сертификационната верига във файла с данни и да провери подписа върху данните, следвайки схемата за подписване, дефинирана в [DSS].

Забележки към фигура 13:

— Оборудването, което е подписало подлежащите на анализ данни се означава с EQT.

— Упоменатите във фигурата сертификати и публични ключове EQT са тези, които се използват за подписване, т.е. VU_Sign или Card_Sign.

— Упоменатите във фигурата сертификати и публични ключове EQT.CA са тези, които се използват за подписване на сертификати на бордови устройства или карти, съобразно конкретния случай.

— Упоменатият във фигурата сертификат EQT.CA.EUR е европейският основен сертификат, който е посочен в референтното означение на сертифициращия орган (CAR) на сертификата EQT.CA.

— Упоменатият във фигурата сертификат EQT.Link е свързващият сертификат на EQT, ако има такъв. Както е посочено в раздел 9.1.2, това е свързващ сертификат за нова европейска двойка основни ключове, създадена от ERCA и подписана с предходния европейски частен ключ.

— Сертификатът EQT.Link.EUR е европейският основен сертификат, който е посочен в референтното означение на сертифициращия орган (CAR) на сертификата EQT.Link.

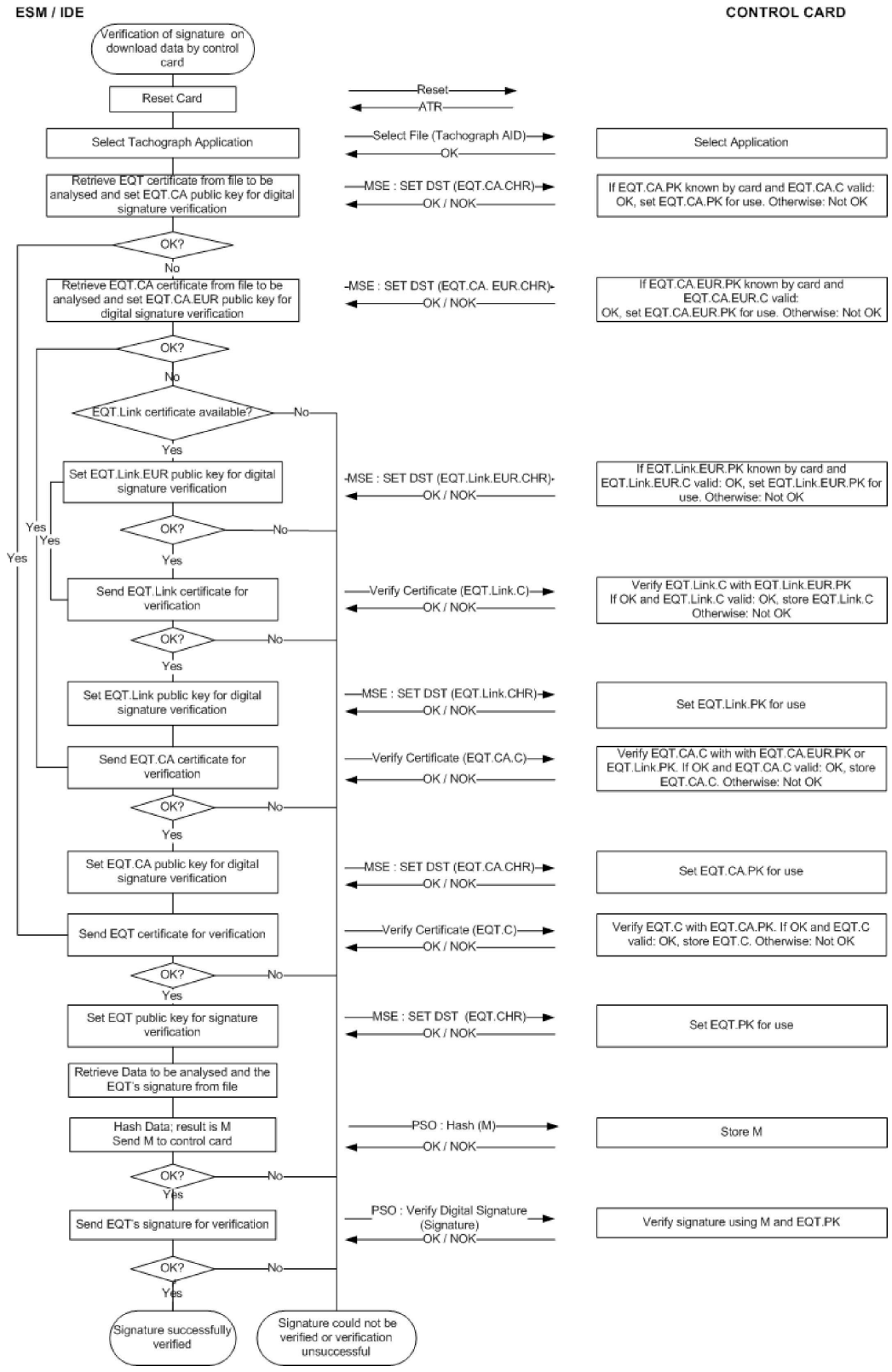
CSM_235 За изчисляването на хеш M, изпратено на контролната карта в командата PSO:Hash, IDE трябва да използва алгоритъма за хеширане, свързан с размера на ключа на бордовото устройство или на картата, от които се изтеглят данни, както е специфицирано в CSM_50.

CSM_236 За проверяване на подписа на EQT контролната карта трябва да следва схемата за подписване, дефинирана в [DSS].

Забележка: В настоящия документ не е специфицирано действие, което да се предприема, ако подписът върху изтеглени данни не може да бъде проверен или ако проверката е неуспешна.

Фигура 13

Протокол за проверка на подписа върху изтеглен файл с данни



Допълнение 12

ОПРЕДЕЛЯНЕ НА МЕСТОПОЛОЖЕНИЕТО ВЪЗ ОСНОВА НА ГЛОБАЛНА НАВИГАЦИОННА СПЪТНИКОВА СИСТЕМА (GNSS)

СЪДЪРЖАНИЕ

1. ВЪВЕДЕНИЕ

В настоящото допълнение са описани техническите изисквания за данните от GNSS, използвани от бордовото устройство, включително протоколите, които трябва да бъдат приложени за обезпечаване на сигурно и правилно прехвърляне на данни за местоположението.

Основните текстове в Регламент (ЕС) № 165/2014 във връзка с тези изисквания са в следните негови членове: „Член 8 Регистриране на местоположението на превозното средство на определени точки в рамките на дневното работно време“, „Член 10 Интерфейс с интелигентни транспортни системи“ и „Член 11 Подробни разпоредби за интелигентните тахографи“.

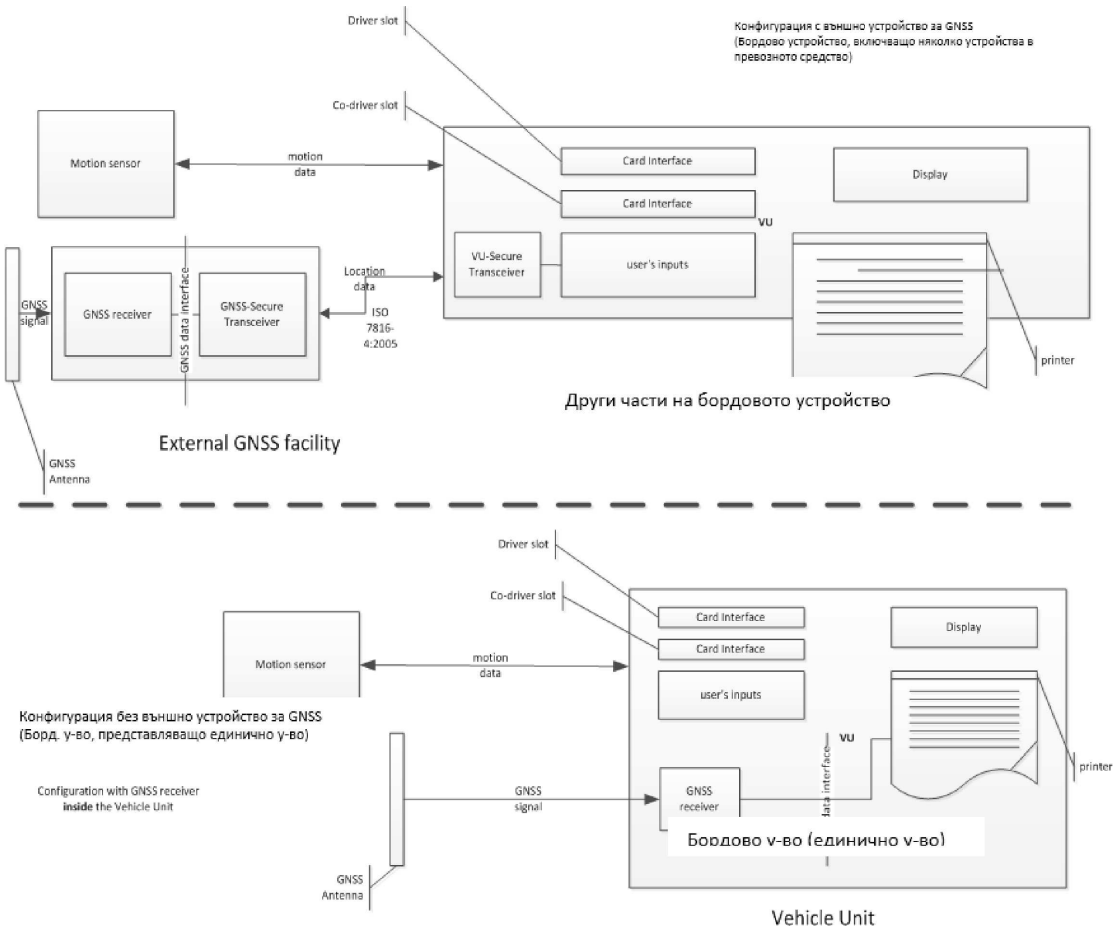
1.1. **Обхват**

GNS_1 Бордовото устройство трябва да събира данни за местоположението от поне една GNSS, които да служат за изпълнение на изискването по член 8.

Бордовото устройство може да бъде със или без външно устройство за GNSS, както е описано на Figure 1:

Фигура 1

Различни конфигурации за разположението на приемника на сигнали от GNSS.



1.2. **Съкращения и означения**

В настоящото допълнение се използват следните съкращения:

DOP Намаление на точността при определяне на местоположението

EGF Елементарен файл на устройството за GNSS

EGNOS Европейска геостационарна служба за навигационно покритие

GNSS Глобална навигационна спътникова система

GSA DOP и активни спътници на GPS

HDOP Хоризонтално намаление на точността при определяне на местоположението

ICD Документ за управление на интерфейса

NMEA National Marine Electronics Association (Национална асоциация за морска електроника, САЩ)

PDOP Position Dilution of Precision (позиционно намаление на точността при определяне на местоположението)

RMC Recommended Minimum Specific (препоръчан минимум от специфични [GNSS данни])

SIS Signal in Space (сигнал от геонавигационни спътници)

VDOP Вертикално намаление на точността при определяне на местоположението

VU Бордово устройство

2. СПЕЦИФИКАЦИЯ НА ПРИЕМНИКА НА СИГНАЛИ ОТ GNSS

Независимо дали конфигурацията на интелигентния тахограф е със или без външно GNSS устройство, осигуряването на точна и надеждна информация за местоположението е съществен елемент от функционирането на интелигентния тахограф. Следователно е целесъобразно да има изискване за съвместимост с услугите, предоставяни по програмата „Галилео“ и програмата за Европейската геостационарна служба за навигационно покритие (EGNOS), определени в Регламент (ЕС) № 1285/2013 на Европейския парламент и на Съвета ([1]). Системата, създадена в рамките на програмата „Галилео“, е независима глобална спътникова навигационна система, а системата, създадена в рамките на програмата EGNOS, е регионална спътникова навигационна система за подобряване на качеството на сигнала на Глобалната система за позициониране (GPS).

GNS_2 Производителите трябва да осигуряват съвместимост на приемниците на сигнали от GNSS с услугите за определяне на местоположението, предоставяни от системите „Галилео“ и EGNOS. Също така, производителите могат допълнително да изберат да има съвместимост и с други навигационни спътникови системи.

GNS_3 Приемникът на сигнали от GNSS трябва да има способност да поддържа автентифициране в рамките на отворените услуги на „Галилео“, когато такива услуги бъдат предоставяни от системата „Галилео“ и бъдат поддържани от производителите на приемници на сигнали от GNSS. От друга страна обаче, няма да се изисква обновяване на интелигентните тахографи, които са пуснати на пазара преди реализирането на горните условия и нямат способност да поддържат автентифициране в рамките на отворените услуги на „Галилео“.

3. ИЗРЕЧЕНИЯ НА NMEA

В настоящия раздел са описани изреченията на NMEA, използвани в областта на функционирането на интелигентните тахографи. Посоченото в настоящия раздел е валидно и за двата вида конфигурации на интелигентните тахографи — със или без външно устройство за GNSS.

GNS_4 Данните за местоположението се базират на изречението на NMEA Recommended Minimum Specific (RMC) GNSS Data (препоръчан минимум от специфични GNSS данни), което обхваща информацията за местоположението (географска ширина и дължина), за времето във формат UTC (hhmmss.ss) и за скоростта спрямо земната повърхност във възли, плюс допълнителни величини.

Форматът на изречението RMC е както следва (съгласно стандарта на NMEA V4.1):

([1]) Регламент (ЕС) № 1285/2013 на Европейския парламент и на Съвета от 11 декември 2013 г. за изграждане и експлоатация на европейските навигационни спътникови системи и за отмяна на Регламент (ЕО) № 876/2002 на Съвета и на Регламент (ЕО) № 683/2008 на Европейския парламент и на Съвета (ОВ L 347, 20.12.2013 г., стр. 1).

Фигура 2

Структура на изречение RMC

1) Time (UTC)
2) Status, A = Valid position, V = Warning
3) Latitude
4) N or S
5) Longitude
6) E or W
7) Speed over ground in knots
8) Track made good, degrees true
9) Date, ddmmyy
10) Magnetic Variation, degrees
11) E or W
12) Checksum

Състоянието (Status) показва дали има наличен GNSS сигнал. Докато стойността за състоянието не стане A, получените данни (например за времето или за географската ширина/дължина) не могат да се използват за записване в бордовото устройство на местоположението на превозното средство.

Разделителната способност за местоположението се базира на формата на гореописаното изречение RMC. Първата част от полета 3) и 5) (първите две числа) се използва за посочване на градусите. Останалото пространство се използва за посочване на минутите с три десетични знака. Следователно разделителната способност е 1/1000 от минутата или 1/60000 от градуса (защото 1 минута е 1/60 от градуса).

GNS_5 Бордовото устройство трябва да съхранява в своята база данни позиционната информация за географска ширина и дължина с разделителна способност 1/10 от минутата или 1/600 от градуса, както е описано в допълнение 1 за типа данни „географски координати“.

За определяне и записване на наличието и точността на сигнал бордовото устройство може да използва командата за DOP и активните спътници на GPS (командата GSA). По-специално, стойността на HDOP се използва като показател за степента на точност на записаните данни за местоположението (вж. 4.2.2). Бордовото устройство трябва да съхранява стойността на хоризонталното намаление на точността при определяне на местоположението (HDOP), изчислена като минималната измежду стойностите на HDOP, получени от наличните системи за GNSS.

Идентификаторът на системата за GNSS посочва дали системата е GPS, Глонасс, Galileo, Beidou или Спътниковата система за диференциална корекция (Satellite-Based Augmentation System, SBAS).

Фигура 3

Структура на изречение GSA

1) Selection mode (Режим на селекция)
2) Mode (Режим)
3) ID of 1st satellite used for fix (Идентификатор на първия спътник, използван за фиксиране)
4) ID of 2nd satellite used for fix (Идентификатор на втория спътник, използван за фиксиране)

...

14) ID of 12th satellite used for fix (Идентификатор на дванадесетия спътник, използван за фиксиране)
15) PDOP в метри
16) HDOP в метри
17) VDOP в метри
18) Идентификатор на система за GNSS
19) Checksum (Контролна сума)

Където Режимът (2-ра позиция) дава индикация, че няма налично фиксиране (Режим=1), или че има налично фиксиране за 2D (Режим=2) или за 3D (Режим=3).

GNS_6 Изречението *GSA* трябва да бъде съхранявано с номер на записа ‘06’.

GNS_7 Максималният размер на изреченията на NMEA (например за RMC, GSA или други), които могат да бъдат използвани във връзка с оразмеряването на командата „read record“, трябва да е 85 байта (вж. Table 1).

4. БОРДОВО УСТРОЙСТВО С ВЪНШНО УСТРОЙСТВО ЗА GNSS

4.1. **Конфигурация**

4.1.1 *Основни компоненти и интерфейси*

При тази конфигурация приемникът на сигнали от GNSS е част от външното устройство за GNSS.

GNS_8 Външното устройство за GNSS трябва да бъде захранвано чрез специфичен интерфейс на превозното средство.

GNS_9 Външното устройство за GNSS трябва да се състои от следните компоненти (вж. Figure 4):

а) Предлаган на пазара приемник на сигнали от GNSS за осигуряване на данни за местоположението чрез интерфейс за данни от GNSS. Например, интерфейсът за данни от GNSS може да бъде по стандарт V4.10 на NMEA, където GNSS приемникът действа като източник на съобщения (talker) и предава изречения на NMEA на защитен GNSS приемопредавател (трансивер) с честота 1 Hz за предварително дефинирания набор от изречения на NMEA, който трябва да съдържа поне изреченията RMC и GSA. Начинът на изпълнение на интерфейса за данни от GNSS се избира от производителите на външни устройства за GNSS.

б) приемопредавателен модул (защитен GNSS приемопредавател) със способност да поддържа стандарт ISO/IEC 7816-4:2013 (вж. 4.2.1) за да комуникира с бордовото устройство, както и да поддържа интерфейса за данни от GNSS към приемника на сигнали от GNSS. Модулът разполага с памет за съхранение на идентификационните данни на приемника на сигнали от GNSS и на външното устройство за GNSS.

в) Ограждаща система с функция за откриване на намеса (tamper detection function), която капсулира както приемника на сигнали от GNSS, така и защитения GNSS приемопредавател. Функцията за откриване на манипулиране трябва да изпълнява защитните мерки за сигурност, в съответствие с изискванията на защитния профил на интелигентния тахограф.

г) GNSS антена, инсталирана върху превозното средство и свързана с приемника на сигнали от GNSS през ограждащата система.

GNS_10 Външното устройство за GNSS разполага поне със следните външни интерфейси:

а) Интерфейс към GNSS антената, инсталирана върху корпуса на превозното средство, ако се използва външна антена.

б) Интерфейс към бордовото устройство.

GNS_11 Намиращият се в бордовото устройство защитен приемопредавател (трансивер) на бордовото устройство представлява другият край на защитената връзка със защитения GNSS приемопредавател и той трябва да поддържа стандарта ISO/IEC 7816-4:2013 за връзката към външното устройство за GNSS.

GNS_12 По отношение на физическия слой на връзката с външното устройство за GNSS, бордовото устройство трябва да поддържа стандарта ISO/IEC 7816-12:2005 или друг стандарт, който може да поддържа ISO/IEC 7816-4:2013. (вж. 4.2.1).

4.1.2 *Състоянието на външното устройство за GNSS при завършването на производството му*

GNS_13 При излизането си от завода външното устройство за GNSS трябва да съхранява следните стойности в енергонезависимата памет на защитения приемопредавател за GNSS:

— двойката ключове EGF_MA и съответния сертификат,

— сертификата MSCA_VU-EGF, съдържащ публичния ключ MSCA_VU-EGF.PK, който се използва за проверяване на сертификата EGF_MA,

— сертификата EUR, съдържащ публичния ключ EUR.PK, който се използва за проверяване на сертификата MSCA_VU-EGF,

— ако съществува, сертификата EUR, чийто период на валидност непосредствено предшества този сертификат EUR, който се използва за проверяване на сертификата MSCA_VU-EGF,

— ако съществува, свързващия сертификат, който дава връзка между тези два сертификата EUR,

— разширения сериен номер на външното устройство за GNSS,

— идентификатора на операционната система на устройството за GNSS,

— номера на одобрението на типа на външното устройство за GNSS,

— идентификатор на компонента за сигурност на външното устройство за GNSS.

4.2. **Връзка между външното устройство за GNSS и бордовото устройство**

4.2.1 *Протокол за връзка*

GNS_14 Протоколът за връзка между външното устройство за GNSS и бордовото устройство трябва да поддържа следните три функции:

1. Събиране и разпределяне на GNSS данни (например за местоположението, времето, скоростта),

2. Събиране на конфигурационните данни за външното устройство за GNSS,

3. Протокола за управление, който да поддържа куплирането, взаимното удостоверяване на автентичността и договарянето на сесийните ключове между външното устройство за GNSS и бордовото устройство.

GNS_15 Протоколът за връзка трябва да се базира на стандарта ISO/IEC 7816-4:2013, като защитеният приемопредавател на бордовото устройство играе ролята на главно устройство, а защитеният приемопредавател за GNSS играе ролята на подчинено устройство. Физическата връзка между външното устройство за GNSS и бордовото устройство се базира на стандарта ISO/IEC 7816-12:2005 или друг стандарт, който може да поддържа ISO/IEC 7816-4:2013.

GNS_16 В протокола за връзка не трябва да се поддържат полета с увеличена дължина.

GNS_17 Протоколът за връзка по стандартите ISO 7816 (съответно *-4:2013 и *-12:2005) между външното устройство за GNSS и бордовото устройство трябва да бъде зададен с T=1.

GNS_18 По отношение на функциите: 1) събиране и разпределяне на GNSS данни, 2) събиране на конфигурационните данни за външното устройство за GNSS и 3) протокол за за управление, защитеният приемопредавател за GNSS трябва да симулира карта с чип (smart card) с архитектура на файловата система, състояща се от главен файл (Master File, MF), файл за директориите (Directory File, DF) с идентификатор на приложенията, специфициран в допълнение 1, глава 6.2 (‘ FF 44 54 45 47 4D’), 3 елементарни файла, съдържащи сертификати и един единичен елементарен файл (EF.EGF) с идентификатор равен на ‘2F2F’, както е описано в Table 1.

GNS_19 Защитеният GNSS приемопредавател трябва да съхранява във файла EF.EGF данните, идващи от приемника на сигнали от GNSS, и конфигурацията. Този файл представлява линеен файл с променлива дължина и е с идентификатор равен на ‘2F2F’ в шестнадесетичен формат.

GNS_20 Паметта, използвана от защитения GNSS приемопредавател за съхраняване на данните, трябва да може да изпълни поне 20 милиона цикъла записване/четене. С изключение на този аспект, вътрешната конструкция и изпълнението на защитения GNSS приемопредавател е по усмотрение на производителите.

Разпределянето в паметта (mapping) на номерата на записите и данните е дадено в таблица 1. Забележете, че съществуват четири изречения GSA за четирите спътникови системи и спътниковата система за диференциална корекция (SBAS).

GNS_21 Файловата структура е дадена в Table 1. По отношение на условията за достъп (ALW, NEV, SM-MAC) вж. допълнение 2, глава 3.5.

Таблица 1

Файлова структура

		Условия за достъп		
Файл	Идентификатор на файла	Четене	Актуализация	Криптиран
MF	3F00			
EF.ICC	0002	ALW	NEV (чрез VU)	Не
DF GNSS Facility	0501	ALW	NEV	Не
EF EGF_MACertificate	C100	ALW	NEV	Не
EF CA_Certificate	C108	ALW	NEV	Не
EF Link_Certificate	C109	ALW	NEV	Не
EF.EGF	2F2F	SM-MAC	NEV (чрез VU)	Не

Файл / елемент от данни	Номер на записа	Размер (байтове)		Стойности по подразбиране
		Мин.	Макс.	
MF		552	1 031	
EF.ICC				
sensorGNSSSerialNumber		8	8	
DF GNSS Facility		*612*	*1 023*	
EF EGF_MACertificate		*204*	*341*	
EGFCertificate		204	341	{00..00}
EF CA_Certificate		*204*	*341*	
MemberStateCertificate		204	341	{00..00}
EF Link_Certificate		*204*	*341*	
LinkCertificate		204	341	{00..00}
EF.EGF				
изречение RMC NMEA	‘01’	85	85	
1-во RMC NMEA изречение	‘02’	85	85	
2-ро GSA NMEA изречение	‘03’	85	85	

Файл / елемент от данни	Номер на записа	Размер (байтове)		Стойности по подразбиране
		Мин.	Макс.	
3-то GSA NMEA изречение	‘04’	85	85	
4-то GSA NMEA изречение	‘05’	85	85	
5-то GSA NMEA изречение	‘06’	85	85	
Разширен сериен номер на външното устройство за GNSS, дефиниран в допълнение 1 като SensorGNSSSerialNumber.	‘07’	8	8	
Идентификатор на операционната система на защитения приемопредавател за GNSS, дефиниран в допълнение 1 като SensorOSIdentifier.	‘08’	2	2	
Номер на одобрението на типа на външното устройство за GNSS, дефиниран в допълнение 1 като SensorExternalGNSSApprovalNumber.	‘09’	16	16	
Идентификатор на компонента за сигурност на външното устройство за GNSS, дефиниран в допълнение 1 като SensorExternalGNSSSCIdentifier	‘10’	8	8	
RFU — Запазен за бъдещо използване	От ‘11’ до ‘FD’			

4.2.2 *Защитено прехвърляне на данни от GNSS*

GNS_22 Защитеното прехвърляне на получени от GNSS данни за местоположението трябва да се допуска само при следните условия:

1. Завършен процес на куплиране, както е описано в допълнение 11. Общи механизми за сигурност.

2. Периодично взаимно удостоверяване на автентичността и договаряне на сесийни ключове между бордовото устройство и външното устройство за GNSS, също описано в допълнение 11. Общите механизми за сигурност трябва да са изпълнени с посочената периодичност.

GNS_23 На всеки T секунди, където T е със стойност по-малка или равна на 10, освен когато се провежда куплиране или взаимно удостоверяване на автентичността и договаряне на сесийни ключове, бордовото устройство иска от външното устройство за GNSS информацията за местоположението въз основа на следния поток от данни:

1. Бордовото устройство иска от външното устройство за GNSS данни за местоположението, заедно с данни за намалението на точността (от изречението GSA NMEA). Защитеният приемопредавател на бордовото устройство използва командата SELECT and READ RECORD(S) по ISO/IEC 7816-4:2013 при защитен обмен на съобщения в режим „само с удостоверяване на автентичността“ (authentication-only mode), както е описано в допълнение 11, раздел 11.5, с идентификатор на файла „2F2F“ и RECORD номер равен на ‘01’ за изречение RMC NMEA и съответно ‘02’, ‘03’, ‘04’, ‘05’, ‘06’ за изречение GSA NMEA.

2. Последната получена информация за местоположението се съхранява в елементарния файл с идентификатор ‘2F2F’ и в записите в защитения GNSS приемопредавател, описани в таблица 1, като защитеният GNSS приемопредавател получава NMEA данни с честота поне 1 Hz от GNSS приемника посредством интерфейса за GNSS данни.

3. Защитеният GNSS приемопредавател изпраща отговора до защитения приемопредавател на бордовото устройство като използва ответно APDU съобщение при защитен обмен на съобщения в режим „само с удостоверяване на автентичността“, както е описано в допълнение 11, раздел 11.5.

4. Защитеният приемопредавател на бордовото устройство проверява автентичността и целостта на получения отговор. При положителен резултат от тази проверка данните за местоположението се прехвърлят в процесора на бордовото устройство посредством интерфейса за GNSS данни.

5. Процесорът на бордовото устройство проверява получените данни и извлича информация (например географска ширина, дължина, време) от изречението RMC NMEA. Изречението RMC NMEA включва информация дали местоположението е валидно. Ако местоположението не е валидно, данните за местоположението все още не са достъпни и не могат да се използват за записване на местоположението на превозното средство. Ако местоположението е валидно, процесорът на бордовото устройство извлича от изреченията GSA NMEA също стойностите на хоризонталното намаление на точността (HDOP) и изчислява средната стойност по наличните спътникови системи (т.е. когато има налично фиксиране).

6. Процесорът на бордовото устройство съхранява в бордовото устройство получената и обработена информация, например за географската ширина, дължина, време и скорост във формата, дефиниран в допълнение 1 Data Dictionary като GeoCoordinates заедно със стойността на HDOP, изчислена като минималната измежду стойностите на HDOP, получени от наличните системи за GNSS.

4.2.3 *Структура на командата Read Record*

В настоящия раздел е описана подробно структурата на командата Read Record. Добавя се защитен обмен на съобщения (в режим само с удостоверяване на автентичността), както е описан в допълнение 11 „Общи механизми за сигурност“.

GNS_24 Командата трябва да поддържа защитен обмен на съобщения (в режим само с удостоверяване на автентичността), вж. допълнение 11.

GNS_25 Командно съобщение

Байт	Дължина	Стойност	Описание
CLA	1	‘0Ch’	Поискан е защитен обмен на съобщения.
INS	1	‘B2h’	Read Record
P1	1	‘XXh’	Номер на записа (номерът ‘00’ е на текущия запис)
P2	1	‘04h’	Прочитане на записа с посочения в P1 номер.
Le	1	‘XXh’	Дължина на очакваните данни. Брой на байтовете, които трябва да се извлекат

GNS_26 Посоченият в P1 запис става текущ запис.

Байт	Дължина	Стойност	Описание
#1-#X	X	‘XX..XXh’	Извлечени данни
SW	2	‘XXXXh’	Байтове за състоянието (SW1, SW2)

— Ако командата бъде изпълнена успешно, защитеният GNSS приемопредавател отговаря с ‘**9000**’.

— Ако текущият файл не е предназначен за записи, защитеният GNSS приемопредавател отговаря с ‘**6981**’.

— Ако командата се използва с P1 = ‘00’ но няма текущ елементарен файл, защитеният GNSS приемопредавател отговаря с ‘**6986**’ (неразрешена команда).

— Ако записът не е намерен, защитеният GNSS приемопредавател отговаря с ‘**6A 83**’.

— Ако външното устройство за GNSS открие манипулиране, то трябва да отговори с израза за състояние ‘**66 90**’.

GNS_27 Защитеният GNSS приемопредавател трябва да поддържа следните команди за тахографи от поколение 2, специфицирани в допълнение 2:

Команда	Препратка
Select	Допълнение 2, глава 3.5.1
Read Binary	Допълнение 2, глава 3.5.2
Get Challenge	Допълнение 2, глава 3.5.4
PSO: Verify Certificate	Допълнение 2, глава 3.5.7
External Authenticate	Допълнение 2, глава 3.5.9
General Authenticate	Допълнение 2, глава 3.5.10
MSE:SET	Допълнение 2, глава 3.5.11

4.3. **Куплиране, взаимно удостоверяване на автентичността и договаряне на сесийни ключове на външното устройство за GNSS с бордовото устройство**

Куплирането, взаимно удостоверяване на автентичността и договарянето на сесийни ключове на външното устройство за GNSS с бордовото устройство са описани в допълнение 11 „Общи механизми за сигурност“, глава 11.

4.4. **Третиране на грешки**

В настоящия раздел е описано как се третират и записват в бордовото устройство потенциалните състояния на грешка от страна на външното устройство за GNSS.

4.4.1 *Грешка във връзката с външното устройство за GNSS*

GNS_28 Ако бордовото устройство не успее да установи връзка с куплираното външно устройство за GNSS в течение на повече от 20 последователни минути, бордовото устройство трябва да генерира и регистрира в себе си събитие от типа EventFaultType с изброена (enum) стойност ‘53’H *External GNSS communication fault* и с времеви печат (timestamp set), съответстващ на текущото време. Събитието се генерира само ако са изпълнени следните две условия: а) интелигентният тахограф не е в режим на калибриране и б) превозното средство се движи. В този контекст, регистрирането на грешка във връзката се задейства когато защитеният приемопредавател на бордовото устройство не получи съобщение-отговор след изпращането на съобщение със заявка, както е описано в 4.2.

4.4.2 *Нарушение на физическата цялост на външното устройство за GNSS*

GNS_29 Ако цялостта на външното устройство за GNSS бъде нарушена, защитеният GNSS приемопредавател трябва да изтрие цялата си памет, включително криптографския материал. Както е описано в GNS_25 и GNS_26, бордовото устройство трябва да констатира наличие на манипулиране (tampering) ако отговорът е със статус ‘6690’. В такъв случай бордовото устройство трябва да генерира събитие от типа EventFaultType с изброена (enum) стойност *‘55’H Tamper detection of GNSS*.

4.4.3 *Липса на информация за местоположението от приемник на сигнали от GNSS*

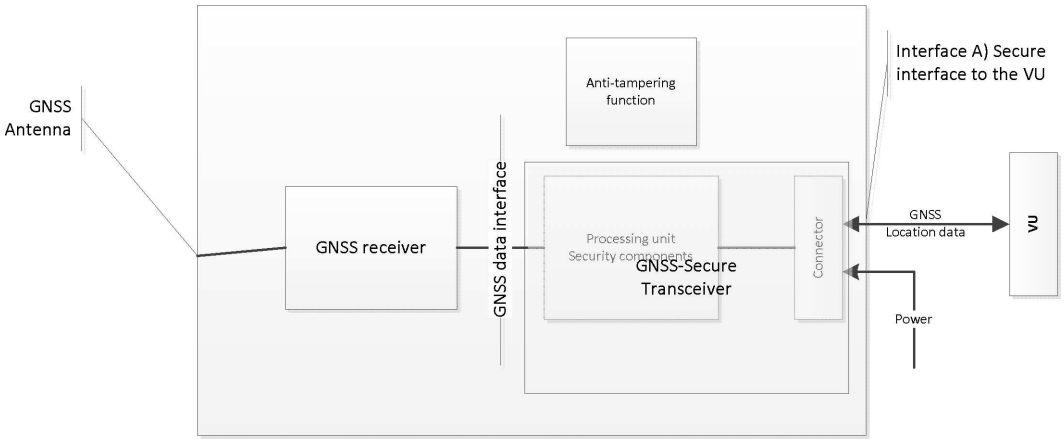
GNS_30 Ако защитеният GNSS приемопредавател не получава данни от приемника на сигнали от GNSS в течение на повече от 3 последователни часа, защитеният GNSS приемопредавател трябва да генерира съобщение-отговор на командата READ RECORD с номер на записа (RECORD) равен на ‘01’ и с поле за данни от 12 байта, всички със стойност 0xFF. При получаване на съобщението-отговор с тази стойност в полето за данни, бордовото устройство трябва да генерира и регистрира събитие от типа EventFaultType с изброена (enum) стойност ‘52’H *external GNSS receiver fault* с времеви печат, съответстващ на текущото време, само ако са изпълнени следните две условия: а) интелигентният тахограф не е в режим на калибриране и б) превозното средство се движи.

4.4.4 *Изтекъл сертификат на външното устройство за GNSS*

GNS_31 Ако бордовото устройство установи, че вече не е валиден сертификатът на външното устройство за GNSS, използван за взаимно удостоверяване на автентичността, бордовото устройство трябва да генерира и регистрира грешка от типа typeEventFaultType с изброена (enum) стойност *'56'H External GNSS facility certificate expired* с времеви печат, съответстващ на текущото време. При това бордовото устройство трябва да продължи да използва получаваните GNSS данни за местоположението.

Фигура 4

Схема на външно устройство за GNSS



5. БОРДОВО УСТРОЙСТВО БЕЗ ВЪНШНО УСТРОЙСТВО ЗА GNSS

5.1. **Конфигурация**

При този вид конфигурация приемникът за сигнали от GNSS е вътре в бордовото устройство, както е описано в Figure 1.

GNS_32 Приемникът за сигнали от GNSS действа като източник на съобщения (talker) и предава изречения NMEA на процесора на бордовото устройство, който действа като приемник (listener) с честота по-голяма или равна на 1/10 Hz на предварително дефинирания набор от изречения на NMEA, който трябва да съдържа поне изреченията RMC и GSA.

GNS_33 Към бордовото устройство се свързва външна GNSS антена, инсталирана върху превозното средство, или вътрешна GNSS антена.

5.2. **Третиране на грешки**

5.2.1 *Липса на информация за местоположението от приемник на сигнали от GNSS*

GNS_34 Ако бордовото устройство не получи данни от приемника на сигнали от GNSS в течение на повече от 3 последователни часа, бордовото устройство трябва да генерира и регистрира събитие от типа EventFaultType с изброена (enum) стойност '51'H *Internal GNSS receiver fault* с времеви печат, съответстващ на текущото време, само ако са изпълнени следните две условия: а) интелигентният тахограф не е в режим на калибриране и б) превозното средство се движи.

6. ПРОТИВОРЕЧИЕ С ВРЕМЕТО В ДАННИТЕ ОТ GNSS

Ако бордовото устройство установи несъответствие в размер на повече от 1 минута между показанията на функцията за измерване на времето на бордовото устройство и данните за времето, произхождащи от приемника на сигнали от GNSS, бордовото устройство трябва да регистрира събитие от типа EventFaultType с изброена (enum) стойност *'0B'H Time conflict (GNSS versus VU internal clock)*. Това събитие се регистрира заедно със стойността на вътрешния часовник на бордовото устройство и се придружава от автоматично сверяване на часовника. След задействане на събитие на противоречие на данните за времето, през следващите 12 часа бордовият блок не генерира други събития за подобно противоречие. Това събитие не трябва да се задейства в случай, че от приемника на сигнали от GNSS не е могъл да бъде открит валиден сигнал от GNSS през последните 30 дни. Когато обаче информацията за местоположението от приемника на сигнали от GNSS отново стане достъпна, трябва да бъде извършено автоматично сверяване на времето.

7. ПРОТИВОРЕЧИЕ В ДАННИТЕ ЗА ДВИЖЕНИЕТО НА ПРЕВОЗНОТО СРЕДСТВО

GNS_35 Бордовото устройство генерира и регистрира събитие за противоречие в данните за движението на превозното средство (вж. изискване 84 в настоящото допълнение) с времеви печат, съответстващ на текущото време, в случай че информацията за движението, изчислена от датчика за движение, противоречи на информацията за движението, изчислена от вътрешния приемник на сигнали от GNSS или съответно от външното устройство за GNSS. За целите по откриване на такива противоречия трябва да бъде използвана стойността на медианата на разликите в данните за скоростта от тези източници, както е посочено по-долу:

— Най-много на всеки 10 секунди трябва да се изчислява разликата между данните за скоростта на превозното средство, оценена от GNSS, и скоростта, оценена от датчика за движение.

— За изчисление на стойността на медианата трябва да се използват всички изчислени стойности във времеви прозорец, съдържащ последните пет минути от движението.

— Стойността на медианата трябва да се изчислява като средна стойност на 80 % от числата, оставащи след елиминиране на най-големите по абсолютна стойност числа.

Събитие за противоречие в данните за превозното средство трябва да се задейства ако стойността на медианата е над 10 км/час за пет последователни минути от движението на превозното средство. Като опционна възможност могат да се използват други независими източници на данни за движението на превозното средство, така че да се осигури по-надеждно разкриване на манипулации на тахографа. (Забележка: използването на стойността на медианата за последните 5 минути се прилага за смекчаване на риска от силно отличаващи се измерени резултати и преходни стойности). Този вид събитие не трябва да се задейства при следните условия: а) при преминаване с ферибот/влак, б) когато няма достъпна информация за местоположението от приемника на сигнали от GNSS и в) при режим на калибриране.

Допълнение 13

ИНТЕРФЕЙС С ITS

СЪДЪРЖАНИЕ

1. ВЪВЕДЕНИЕ

В настоящото допълнение се определят проектирането и процедурите, които трябва да се следват за осъществяването на интерфейса с интелигентни транспортни системи (ИТС, по-долу ITS от Intelligent Transport Systems), изисквана съгласно член 10 от Регламент (ЕС) № 165/2014 (*Регламентът*).

В *Регламента* е посочено, че тахографите на превозни средства могат да бъдат оборудвани със стандартни интерфейси, позволяващи регистрираните или генерираните от тахограф данни да се използват в работен режим от външно устройство, когато са изпълнени следните условия:

а) интерфейсът не засяга истинността и цялостността на данните от тахографа;

б) интерфейсът съответства на подробните разпоредби по член 11;

в) външното устройство, свързано с интерфейса, има достъп до лични данни, включително данни за местоположението, само след получаване на съгласието на водача, за когото се отнасят данните, като даването на съгласие трябва да може да се удостовери.

2. ОБХВАТ

В настоящото допълнение е определен начинът, по който приложения, поддържани от външни устройства, могат да получат чрез връзка Bluetooth® данни (*данните*) от даден тахограф.

Данните, предоставяни чрез този интерфейс, са описани в приложение 1 към настоящия документ. Този интерфейс не възпрепятства прилагането на други интерфейси (напр. чрез CAN bus) за предаване на данни от бордовото устройство (VU) към други бордови средства за обработка на данни.

В настоящото допълнение са определени:

— *Данните*, предоставяни чрез интерфейса с ITS

— Профилът на връзката Bluetooth®, която се използва за прехвърляне на данните

— Процедурите за запитване и изтегляне на данни и последователността на операциите

— Механизмът за „сдвояване“ (pairing) между тахографа и външното устройство

— Предоставяният на водача механизъм за даване на съгласие

Трябва да се поясни, че в настоящото приложение не са определени:

— Събирането и управлението на данните в рамките на VU (които са определени другаде в *Регламента* или в противен случай са в зависимост от проектирането на съответния продукт)

— Формата на представяне на събраните данни на приложенията, поддържани от външното устройство.

— Мерките за сигурност на данните извън предоставяните от Bluetooth® (като например криптиране), отнасящи се за съдържанието на *данните* (които се определят другаде в Регламента [в допълнение 10 относно общите механизми за сигурност])

— Протоколите за Bluetooth®, използвани от интерфейса с ITS

2.1. **Съкращения, определения и обозначения**

В настоящото допълнение са използвани следните съкращения и определения, които са специфични за него:

връзката	обменът на информация/данни между главно устройство (т.е. тахографа) и външно устройство чрез интерфейса с ITS по Bluetooth®.
данните	наборите данни, определени в приложение 1.
Регламентът	Регламент (ЕС) № 165/2014 на Европейския парламент и на Съвета от 4 февруари 2014 г. относно тахографите в автомобилния транспорт, за отмяна на Регламент (ЕИО) № 3821/85 на Съвета относно контролните уреди за регистриране на данните за движението при автомобилен транспорт и за изменение на Регламент (ЕО) № 561/2006 на Европейския парламент и на Съвета за хармонизиране на някои разпоредби от социалното законодателство, свързани с автомобилния транспорт
BR	Basic Rate (основна скорост)
EDR	Enhanced Data Rate (повишена скорост за предаване на данни)
GNSS	Global Navigation Satellite System („Глобална навигационна спътникова система“)
IRK	Identity Resolution Key
ITS	Intelligent Transport System (интелигентна транспортна система — ИТС)
LE	Low Energy (ниска енергия)
PIN (ПИН)	Personal Identification Number (персонален идентификационен номер)
PUC	Personal Unblocking Code („персонален код за деблокиране“)
SID	Service Identifier (идентификатор на услугата)
SPP	Serial Port Profile (профил на сериен порт)
SSP	Secure Simple Pairing (защитено опростено сдвояване)
TRTP	Transfer Request Parameter (параметър на заявката за прехвърляне на данни)
TREP	Transfer Response Parameter (параметър на отговора за прехвърляне на данни)
VU	Vehicle Unit (бордово устройство)

3. ПОЗОВАВАНИЯ НА РЕГЛАМЕНТИ И СТАНДАРТИ

Спецификацията, определена в настоящото допълнение, се отнася до и зависи от всички или части от посочените по-долу регламенти и стандарти. В разделите от настоящото допълнение са посочени относимите стандарти или относимите раздели на стандарти. В случай на противоречие разделите на настоящото допълнение имат предимство.

Настоящото допълнение съдържа позовавания на следните регламенти и стандарти:

— Регламент (ЕС) № 165/2014 на Европейския парламент и на Съвета от 4 февруари 2014 г. относно тахографите в автомобилния транспорт, за отмяна на Регламент (ЕИО) № 3821/85 на Съвета относно контролните уреди за регистриране на данните за движението при автомобилен транспорт и за изменение на Регламент (ЕО) № 561/2006 на Европейския парламент и на Съвета за хармонизиране на някои разпоредби от социалното законодателство, свързани с автомобилния транспорт

— Регламент (ЕО) № 561/2006 на Европейския парламент и на Съвета от 15 март 2006 г. за хармонизиране на някои разпоредби от социалното законодателство, свързани с автомобилния транспорт, за изменение на Регламенти (ЕИО) № 3821/85 и (ЕО) № 2135/98 на Съвета и за отмяна на Регламент (ЕИО) № 3820/85 на Съвета

— ISO 16844 — 4: Пътни превозни средства. Тахографски системи. Част 4: Интерфейс на CAN мрежа

— ISO 16844 — 7: Пътни превозни средства. Тахографски системи. Част 7: Параметри

— Bluetooth® — профил на сериен порт — V1.2

— Bluetooth® — основна версия 4.2

— Протокол NMEA 0183 V4.1

4. ПРИНЦИПИ НА ФУНКЦИОНИРАНЕ НА ИНТЕРФЕЙСА

4.1. **Предварителни условия за прехвърляне на данни чрез интерфейса с ITS**

От бордовото устройство (VU) се изисква да актуализира и да поддържа данните, които трябва да се съхраняват в него, без никакво участие на интерфейса с ITS. Средството, чрез което се постига това, е вътрешно за VU и е определено другаде в Регламента, а не в настоящото допълнение.

4.1.1 *Данни, предоставяни чрез интерфейса с ITS*

От VU се изисква да актуализира данните, които ще бъдат предоставяни чрез интерфейса с ITS, с честота, определена в рамките на процедурите на VU, без никакво участие на интерфейса с ITS. Данните във VU се използват като основа за получаване и актуализиране на *данните*, като начинът за постигане на това е определен другаде в *Регламента*, а ако не е определен там, се определя не в настоящото допълнение, а при проектирането на съответния продукт.

4.1.2 *Съдържание на данните*

Съдържанието на данните трябва да е съгласно приложение 1 към настоящото допълнение.

4.1.3 *Приложения за ITS*

Приложенията за ITS ще използват данни, предоставени чрез интерфейса с ITS — например за оптимизиране на управлението на дейностите на водача, като същевременно се спазва Регламентът, за откриване на евентуални неизправности в тахографа или за използване на данни от GNSS. Спецификацията на приложенията не попада в обхвата на настоящото допълнение.

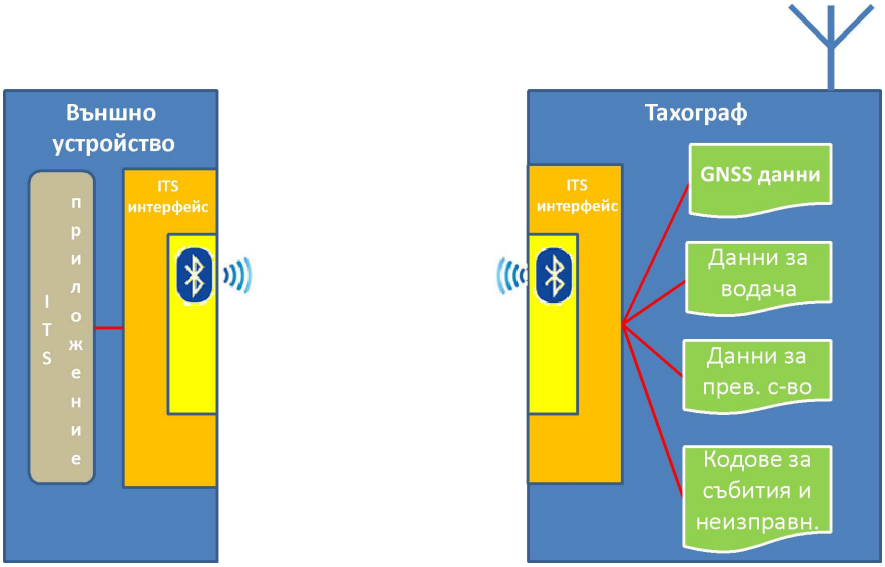
4.2. **Съобщителна технология**

Обменът на данни чрез интерфейса с ITS се извършва посредством интерфейс Bluetooth®, който е съвместим с версия 4.2 или по-късна. Bluetooth® функционира в нелицензираната радиочестотна лента от 2,4 до 2,485 GHz за промишлени, научни и медицински (ISM) цели. Bluetooth ® 4.2 осигурява усъвършенствани механизми за неприкосновеност на личния живот и сигурност, а също така повишава скоростта и надеждността на прехвърлянето на данни. За целите на настоящата спецификация се използва радиовръзка Bluetooth® клас 2 с обсег до 10 метра. Повече информация относно Bluetooth ® 4.2 е налична на www.bluetooth.com (https://www.bluetooth.org/en-us/specification/adopted-specifications?_ga=1.215147412.2083380574.1435305676).

Връзката със съобщителното оборудване се установява, след като главното устройство приключи процеса на сдвояване. Тъй като при Bluetooth® се използва модел главен/подчинен, за да се контролира кога и къде устройствата могат да изпращат данни, тахографът ще изпълнява ролята на главно устройство, а външното устройство — на подчинено.

Когато външно устройство попадне в обсега на VU за първи път, процесът на сдвояване за връзка Bluetooth® може да започне (виж също приложение 2). Устройствата споделят своите адреси, наименования и профили, както и общ таен ключ, който им позволява в бъдеще винаги да се съчетават, когато са в близост. След като бъде завършена тази стъпка, външното устройство придобива статут на доверено и е в състояние да отправи заявки за изтегляне на данни от тахографа. Не се предвижда да се добавят още механизми за криптиране извън предоставяното от Bluetooth®. Ако са необходими обаче допълнителни механизми за сигурност, те се осъществяват в съответствие с допълнение 10 относно общите механизми за сигурност.

Общият принцип на връзка е онагледен на следващата фигура.



За прехвърляне на данни от VU към външното устройство се използва профилът SPP (Serial Port Profile) на Bluetooth®.

4.3. **Разрешаване на достъпа чрез PIN**

От съображения за сигурност VU изисква система за разрешаване на достъпа чрез PIN код, която е отделена от сдвояването по Bluetooth. Всяко VU трябва да е в състояние да генерира PIN кодове, съставени от най-малко 4 цифри, за целите на удостоверяването на автентичността. Всеки път, когато външно устройство се сдвоява с VU, то трябва да подаде правилния PIN код, преди да получи каквито и да били данни.

Когато устройството подаде успешно PIN, то се включва в позитивен списък (whitelist). В позитивния списък трябва да се съхраняват данни за най-малко 64 устройства, сдвоени с конкретното VU.

Ако устройството три пъти подред подаде неправилен PIN код, то се включва временно в „черен списък“. Докато устройството е в черния списък, всеки нов опит от негова страна се отхвърля. Ако след това устройството подаде още три пъти подред неправилен PIN код, това води до все по-продължителна забрана на достъпа (виж таблица 1). Подаването на правилния PIN код нулира продължителността на забраната за достъп и броя на опитите. Във фигура 1 в приложение 2 е дадена диаграма на последователността при опит за валидиране на PIN.

Таблица 1

Продължителност на забраната в зависимост от броя на поредните неуспешни опити за подаване на правилния PIN код

Брой на поредните неуспешни опити	Продължителност на забраната
3	30 секунди
6	5 минути
9	1 час
12	24 часа
15	Постоянна

Ако ITS устройството петнадесет пъти (5 × 3) подред подаде неправилен PIN код, то се включва за постоянно в черния списък. Тази постоянна забрана се отменя само с подаването на правилния PUC код.

PUC кодът се състои от 8 цифри и се предоставя от производителя заедно с VU. Ако ITS устройството десет пъти подред подаде неправилен PUC код, то се включва неотменимо за постоянно в черния списък.

Производителят може да предлага възможност за промяна на PIN кода пряко чрез VU, но PUC кодът не може да се променя. Ако изменението на PIN кода е възможно, за целта се изисква текущият PIN код да бъде въведен пряко във VU.

Освен това всички устройства, данни за които се съхраняват в позитивния списък, се запазват, докато не бъдат заличени ръчно от ползвателя (напр. чрез интерфейса човек—машина на VU или с други средства). По този начин загубени или откраднати устройства на ITS могат да бъдат отстранени от позитивния списък. Също така всяко ITS устройство, напуснало обсега за връзка по Bluetooth за повече от 24 часа, автоматично се отстранява от позитивния списък на VU и трябва да подаде отново правилния PIN код, когато връзката се възстанови.

Форматът на съобщенията между интерфейса на VU и самото VU не се определя, а е по усмотрение на производителя. Въпросният производител трябва обаче да гарантира спазването на формата за съобщенията между ITS устройството и интерфейса на VU (виж спецификациите за ASN.1).

По този начин всяка заявка за прехвърляне на данни се посреща с надлежна проверка на пълномощията на подателя преди каквато и да била форма на обработване. Във фигура 2 в приложение 2 е дадена диаграма на последователността за тази процедура. Всяко устройство, включено в черния списък, се отхвърля автоматично, а всяко устройство, което не фигурира нито в черния, нито в позитивния списък, получава заявка за PIN, която трябва да изпълни преди да изпрати пак своята заявка за прехвърляне на данни.

4.4. **Формат на съобщенията**

Всички съобщения, разменяни между ITS устройството и VU, трябва да са форматирани със структура от следните три части: заглавна част (header), съставена от байт за целевото устройство (TGT), байт за източника (SRC) и байт за дължина (LEN);

поле за данни, съдържащо един байт за идентификатора на услугата (SID) и променлив брой байтове с данни (максимум 255);

байт за контролната сума (CS) — серия от еднобайтови суми по модул 256, които представляват всички байтове на съобщението с изключение на самата контролна сума.

Съобщението трябва да бъде във формат Big Endian.

Таблица 2

Общ формат на съобщенията

Заглавна част			Поле за данни					Контролна сума
TGT	SRC	LEN	SID	TRTP	CC	CM	DATA (ДАННИ)	CS
3 байта			Макс. 255 байта					1 байт

Заглавна част

TGT и SRC: идентификатор (ID) съответно на целевото (Target — TGT) и изходното (Source — SRC) устройство за съобщението. Интерфейсът на VU трябва по подразбиране да е с ID „EE“. Този ID не може да се променя. Устройството на ITS използва по подразбиране за ID „A0“ за своето първо съобщение от сесията на връзка. След това интерфейсът на VU присвоява уникален ID на ITS устройството и го уведомява за този ID с оглед на бъдещи съобщения по време на сесията.

Байтът LEN отчита само частта DATA на полето за данни (виж таблица 2), като първите 4 байта са имплицитни.

Интерфейсът на VU потвърждава автентичността на подателя на съобщението чрез кръстосана проверка на своя списък на идентификатори (IDList) с данните по Bluetooth, като проверява дали ITS устройството, фигуриращо в списъка за предоставения ID, понастоящем в обсега на връзката по Bluetooth.

Поле за данни

Освен SID полето за данни съдържа и други параметри: параметър на заявката за прехвърляне на данни (TRTP) и броячни байтове.

Ако данните, които трябва да се пренасят, са твърде дълги спрямо наличното пространство в едно съобщение, те се разделят в няколко подсъобщения. Всяко подсъобщение е с едни и същи заглавна част и SID, но съдържа брояч от 2 байта — Counter Current (CC) и Counter Max (CM), който посочва номера на подсъобщението. С цел осигуряване на контрол за грешки и евентуално прекратяване на обмена на данни, приемащото устройство потвърждава получаването на всяко подсъобщение. Приемащото устройство може да потвърди приемането на подсъобщението, да поиска повторното му предаване или да заяви възобновяване или прекратяване на предаването на данните от предаващото устройство.

Ако CC и CM не се използват, те получават стойността 0xFF.

Например следното съобщение

HEADER	SID	TRTP	CC	CM	DATA	TC
3 байта	Дължина, по-голяма от 255 байта					1 байт

се предават като:

HEADER	SID	TRTP	01	n	DATA	TC
3 байта	255 байта					1 байт

HEADER	SID	TRTP	02	n	DATA	TC
3 байта	255 байта					1 байт

…

HEADER	SID	TRTP	N	N	DATA	TC
3 байта	Макс. 255 байта					1 байт

Таблица 3 съдържа съобщенията, които VU и ITS устройството трябва да са в състояние да обменят. Съдържанието на всеки параметър е дадено в шестнадесетична бройна система. За яснота в таблицата не са представени CC и CM, виж по-горе за пълния формат.

Таблица 3

Подробно съдържание на съобщението

Съобщение	Заглавна част			DATA			Контролна сума
	TGT	SRC	LEN	SID	TRTP	DATA	
RequestPIN	*ITSID*	EE	00	01	FF		
SendITSID	*ITSID*	EE	01	02	FF	*ITSID*	
SendPIN	EE	*ITSID*	04	03	FF	4*INTEGER, т.е. цяло число (0..9)	
PairingResult	*ITSID*	EE	01	04	FF	BOOLEAN (T/F), т.е. булева стойност T за „вярно“ и F за „невярно“	
SendPUC	EE	*ITSID*	08	05	FF	8*INTEGER (0..9)	
BanLiftingResult	*ITSID*	EE	01	06	FF	BOOLEAN (T/F)	
RequestRejected	*ITSID*	EE	08	07	FF	Час	
RequestData							
standardTachData	EE	*ITSID*	01	08	01		
personalTachData	EE	*ITSID*	01	08	02		
gnssData	EE	*ITSID*	01	08	03		
standardEventData	EE	*ITSID*	01	08	04		
personalEventData	EE	*ITSID*	01	08	05		
standardFaultData	EE	*ITSID*	01	08	06		
manufacturerData	EE	*ITSID*	01	08	07		

Съобщение	Заглавна част			DATA			Контролна сума
	TGT	SRC	LEN	SID	TRTP	DATA	
ResquestAccepted	*ITSID*	EE	Len	09	TREP	Данни	
DataUnavailable							
Няма налични данни	*ITSID*	EE	02	0A	TREP	10	
Не се споделят лични данни	*ITSID*	EE	02	0A	TREP	11	
NegativeAnswer							
Общ отказ	*ITSID*	EE	02	0B	SID Req	10	
Несъвместима услуга	*ITSID*	EE	02	0B	SID Req	11	
Несъвместима подфункция	*ITSID*	EE	02	0B	SID Req	12	
Неправилна дължина на съобщението	*ITSID*	EE	02	0B	SID Req	13	
Неправилни условия или грешка в последователността на заявката	*ITSID*	EE	02	0B	SID Req	22	
Заявка извън обсега	*ITSID*	EE	02	0B	SID Req	31	
Изчакване на отговор	*ITSID*	EE	02	0B	SID Req	78	
Несъответствие на IT-SID	*ITSID*	EE	02	0B	SID Req	FC	
Неоткриваем ITSID	*ITSID*	EE	02	0B	SID Req	FB	

RequestPIN (SID 01)

Това съобщение се издава от интерфейса на VU, ако ITS устройство, което не фигурира в черния списък, но не фигурира и в позитивния списък, заяви данни.

SendITSID (SID 02)

Това съобщение се издава от интерфейса на VU винаги когато ново устройство изпрати заявка. Това устройство използва за ID „A0“ по подразбиране преди да му се присвои уникален ID за сесията на връзка.

SendPIN (SID 03)

Това съобщение се издава от ITS устройството, за да бъде включено в позитивния списък от интерфейса на VU. Съдържанието на това съобщение е код от 4 цели числа (INTEGER) между 0 и 9.

PairingResult (SID 04)

Това съобщение се издава от интерфейса на VU, за да уведоми ITS устройството, ако изпратеният от последното PIN код е верен. Съдържанието на това съобщение е булева стойност „True“ за верен PIN код и „False“ в противен случай.

SendPUC (SID 05)

Това съобщение се издава от ITS устройството, за да бъде изваден от черния списък от интерфейса на VU. Съдържанието на това съобщение е код от 8 цели числа (INTEGER) между 0 и 9.

BanLiftingResult (SID 06)

Това съобщение се издава от интерфейса на VU, за да уведоми ITS устройството, ако изпратеният от последното PUC код е верен. Съдържанието на това съобщение е булева стойност „True“ за верен PUC код и „False“ в противен случай.

RequestRejected (SID 07)

Това съобщение се издава от интерфейса на VU в отговор на всяко съобщение от включено в черния списък ITS устройство с изключение на съобщението „SendPUC“. В съобщението се посочва още колко време ITS устройството ще остане в черния списък, като се спазва форматът на последователността „Time“, определен в приложение 3.

RequestData (SID 08)

Това съобщение със заявка за достъп до данни се издава от ITS устройството. Еднобайтов параметър на заявката за прехвърляне на данни (TRTP) указва вида на заявените данни. Има няколко вида данни:

— standardTachData (TRTP 01): налични данни от тахографа, класифицирани като нелични.

— personalTachData (TRTP 02): налични данни от тахографа, класифицирани като лични.

— gnssData (TRTP 03): данни от GNSS, които винаги са лични.

— standardEventData (TRTP 04): записани данни за събития, класифицирани като нелични.

— personalEventData (TRTP 05): записани данни за събития, класифицирани като лични.

— standardFaultData (TRTP 06): записани данни за неизправности, класифицирани като нелични.

— manufacturerData (TRTP 07): данни, предоставени от производителя.

Вж. приложение 3 към настоящото допълнение за повече информация относно съдържанието на всеки вид данни.

Виж допълнение 12 за повече информация относно формата и съдържанието на данните от GNSS.

Вж. приложения IБ и IВ за повече информация за кодове на данни за събития и неизправности.

RequestAccepted (SID 09)

Това съобщение се издава от интерфейса на VU, ако се приеме съобщение „RequestData“ на ITS устройството. Това съобщение съдържа еднобайтов параметър на отговора за прехвърляне на данни (TREP), който представлява TRTP байтът на съответното съобщение RequestData, и всички данни от заявения вид.

DataUnavailable (SID 0A)

Това съобщение се издава от интерфейса на VU, ако по някаква причина заявените данни не са на разположение за изпращане на включено в позитивния списък ITS устройство. Съобщението съдържа еднобайтов TREP, който представлява TRTP на заявените данни, и еднобайтов код за грешка, определен в таблица 3. Прилагат се следните кодове:

— Няма налични данни (10): интерфейсът на VU няма достъп до данните на VU по неуточнени причини.

— Не се споделят лични данни (11): ITS устройството се опитва да извлече лични данни, когато те не са споделени.

NegativeAnswer (SID 0B)

Тези съобщения се издават от интерфейса на VU, ако дадена заявка не може да бъде изпълнена по причини, различни от липсата на данни. Тези съобщения обикновено се дължат на неправилен формат на заявката (по отношение на дължина, SID, ITSID…), но не само на това. TRTP в полето за данни съдържа SID на заявката. Полето за данни съдържа код, идентифициращ причината за отрицателния отговор. Прилагат се следните кодове:

— General Reject, т.е. общ отказ (код: 10)

— Действието не може да се изпълни по причина, която не е посочена по-долу, нито в раздел … (да се впише номерът на раздела за DataUnavailable).

— Service not supported, т.е. несъвместима услуга (код: 11)

— SID на заявката не е разпознат.

— Sub function not supported, т.е. несъвместима подфункция (код: 12)

— TRTP на заявката не е разпознат. Например той може да липсва или да е извън приетите стойности.

— Incorrect message length, т.е. неправилна дължина на съобщението (код: 13)

— Дължината на полученото съобщение е неправилна (несъответствие между байта LEN и действителната дължина на съобщение).

— Conditions not correct or request sequence error, т.е. неправилни условия или грешка в последователността на заявката (код: 22)

— Заявената услуга не е налична или последователността на съобщенията за заявката е неправилна.

— Request out of range, т.е. заявка извън обсега (код: 33)

— Записът за параметрите на заявката (полето за данни) не е валиден.

— Response pending, т.е. изчакване на отговор (код: 78)

— Заявеното действие не може да бъде изпълнено в определеното време и VU няма готовност да приеме друга заявка.

— *ITSID* Mismatch (код: FB)

— След сравнение с информацията по Bluetooth е установено несъответствие на ITSID на SRC с устройството, за което се отнася.

— *ITSID* Not Found (код: FC)

— ITSID на SRC не е свързан с никакво устройство.

Редове 1—72 (**FormatMessageModule**) на кода ASN. 1 в приложение 3 определят формата на съобщенията, както е описано в таблица 3. Повече подробности относно съдържанието на съобщенията се дава по-долу.

4.5. **Съгласие на водача**

Всички налични данни са класифицирани или като стандартни, или като лични. Личните данни са достъпни само ако водачът е дал своето съгласие личните данни от неговия тахограф да напускат мрежата на превозното средство за използване от приложения на трети страни.

Водачът дава съгласието си, когато при първото вкарване на своята карта на водач или на карта за монтаж и настройки, която към момента е неизвестна за бордовото устройство, титулярят на картата бъде приканен да изрази своето съгласие за подаване на лични данни от тахографа посредством незадължителния интерфейс с ITS (виж също приложение IB, точка 3.6.2).

Състоянието по отношение на даването на съгласие (дадено или не) се записва в паметта на тахографа.

В случай на екип от няколко водача, по интерфейса с ITS се споделят личните данни само на водачите, които са дали съгласието си за това. Например ако превозното средство е с двама водачи и само първият от тях се е съгласил да споделя личните си данни, не се споделят личните данни, отнасящи се за втория водач.

4.6. **Извличане на стандартни данни**

На фигура 3 от приложение 2 се дават диаграми на последователността на валидна заявка, изпратена от ITS устройството за достъп до стандартни данни. Ако ITS устройството надлежно фигурира в позитивния списък и заявката не е за лични данни, не е необходима по-нататъшна проверка. Диаграмите са с оглед, че вече е изпълнена правилната процедура, показана на фигура 2 от приложение 2. Те могат да бъдат отъждествени със сивата клетка *REQUEST TREATMENT* във фигура 2.

Измежду наличните данни за стандартни се считат следните:

— standardTachData (TRTP 01)

— StandardEventData (TRTP 04)

— standardFaultData (TRTP 06)

4.7. **Извличане на лични данни**

Във фигура 4 от приложение 2 е дадена диаграма на последователността за обработката на заявката за лични данни. Както вече беше посочено, интерфейсът на VU изпраща лични данни само ако водачът е дал своето изрично съгласие (виж също 4.5). В противен случай заявката трябва да бъде отхвърлена автоматично.

Измежду наличните данни за лични се считат следните:

— personalTachData (TRTP 02)

— gnssData (TRTP 03)

— personalEventData (TRTP 05)

— manufacturerData (TRTP 07)

4.8. **Извличане на данни за събития и неизправности**

ITS устройствата трябва да могат да заявяват данни относно събития със списък на всички неочаквани събития. Тези данни се считат за стандартна или за лични — виж приложение 3. Съдържанието на данните за всяко събитие е в съответствие с документацията, предоставена в приложение 1 към настоящото допълнение.

ПРИЛОЖЕНИЕ 1

СПИСЪК НА ДАННИТЕ, ПРЕДОСТАВЯНИ ЧРЕЗ ИНТЕРФЕЙСА С ITS

Data	Source	Data classification (personal/ not personal)
VehicleIdentificationNumber	Vehicle Unit	**not personal**
CalibrationDate	Vehicle Unit	**not personal**
TachographVehicleSpeed speed instant t	Vehicle Unit	personal
Driver1WorkingState Selector driver	Vehicle Unit	personal
Driver2WorkingState	Vehicle Unit	personal
DriveRecognize Speed Threshold detected	Vehicle Unit	**not personal**
Driver1TimeRelatedStates Weekly day time	Driver Card	personal
Driver2TimeRelatedStates	Driver Card	personal
DriverCardDriver1	Vehicle Unit	**not personal**
DriverCardDriver2	Vehicle Unit	**not personal**
OverSpeed	Vehicle Unit	personal
TimeDate	Vehicle Unit	**not personal**
HighResolutionTotalVehicleDistance	Vehicle Unit	**not personal**
ServiceComponentIdentification	Vehicle Unit	**not personal**
ServiceDelayCalendarTimeBased	Vehicle Unit	**not personal**
Driver1Identification	Driver Card	personal
Driver2Identification	Driver Card	personal
NextCalibrationDate	Vehicle Unit	**not personal**
Driver1ContinuousDrivingTime	Driver Card	personal
Driver2ContinuousDrivingTime	Driver Card	personal
Driver1CumulativeBreakTime	Driver Card	personal
Driver2CumulativeBreakTime	Driver Card	personal
Driver1CurrentDurationOfSelectedActivity	Driver Card	personal
Driver2CurrentDurationOfSelectedActivity	Driver Card	personal

Data	Source	Data classification (personal/ not personal)
SpeedAuthorised	Vehicle Unit	**not personal**
TachographCardSlot1	Driver Card	**not personal**
TachographCardSlot2	Driver Card	**not personal**
Driver1Name	Driver Card	personal
Driver2Name	Driver Card	personal
OutOfScopeCondition	Vehicle Unit	**not personal**
ModeOfOperation	Vehicle Unit	**not personal**
Driver1CumulatedDrivingTimePreviousAndCurrentWeek	Driver Card	personal
Driver2CumulatedDrivingTimePreviousAndCurrentWeek	Driver Card	personal
EngineSpeed	Vehicle Unit	personal
RegisteringMemberState	Vehicle Unit	**not personal**
VehicleRegistrationNumber	Vehicle Unit	**not personal**
Driver1EndOfLastDailyRestPeriod	Driver Card	personal
Driver2EndOfLastDailyRestPeriod	Driver Card	personal
Driver1EndOfLastWeeklyRestPeriod	Driver Card	personal
Driver2EndOfLastWeeklyRestPeriod	Driver Card	personal
Driver1EndOfSecondLastWeeklyRestPeriod	Driver Card	personal
Driver2EndOfSecondLastWeeklyRestPeriod	Driver Card	personal
Driver1CurrentDailyDrivingTime	Driver Card	personal
Driver2CurrentDailyDrivingTime	Driver Card	personal
Driver1CurrentWeeklyDrivingTime	Driver Card	personal
Driver2CurrentWeeklyDrivingTime	Driver Card	personal
Driver1TimeLeftUntilNewDailyRestPeriod	Driver Card	personal
Driver2TimeLeftUntilNewDailyRestPeriod	Driver Card	personal
Driver1CardExpiryDate	Driver Card	personal

Data	Source	Data classification (personal/ not personal)
Driver2CardExpiryDate	Driver Card	personal
Driver1CardNextMandatoryDownloadDate	Driver Card	personal
Driver2CardNextMandatoryDownloadDate	Driver Card	personal
TachographNextMandatoryDownloadDate	Vehicle Unit	**not personal**
Driver1TimeLeftUntilNewWeeklyRestPeriod	Driver Card	personal
Driver2TimeLeftUntilNewWeeklyRestPeriod	Driver Card	personal
Driver1NumberOfTimes9hDailyDrivingTimesExceeded	Driver Card	personal
Driver2NumberOfTimes9hDailyDrivingTimesExceeced	Driver Card	personal
Driver1CumulativeUninterruptedRestTime	Driver Card	personal
Driver2CumulativeUninterruptedRestTime	Driver Card	personal
Driver1MinimumDailyRest	Driver Card	personal
Driver2MinimumDailyRest	Driver Card	personal
Driver1MinimumWeeklyRest	Driver Card	personal
Driver2MinimumWeeklyRest	Driver Card	personal
Driver1MaximumDailyPeriod	Driver Card	personal
Driver2MaximumDailyPeriod	Driver Card	personal
Driver1MaximumDailyDrivingTime	Driver Card	personal
Driver2MaximumDailyDrivingTime	Driver Card	personal
Driver1NumberOfUsedReducedDailyRestPeriods	Driver Card	personal
Driver2NumberOfUsedReducedDailyRestPeriods	Driver Card	personal
Driver1RemainingCurrentDrivingTime	Driver Card	personal
Driver2RemainingCurrentDrivingTime	Driver Card	personal
GNSS position	Vehicle Unit	personal

2) НЕПРЕКЪСНАТИ ДАННИ ОТ GNSS, ПРЕДОСТАВЯНИ СЛЕД СЪГЛАСИЕТО НА ВОДАЧА

Виж допълнение 12 — GNSS.

3) ПРЕДОСТАВЯНИ БЕЗ СЪГЛАСИЕТО НА ВОДАЧА КОДОВЕ ЗА СЪБИТИЯ

Събитие	Правила за съхраняване на данните	Данни, които се регистрират при всяко събитие
Вкарване на невалидна карта	— десетте най-скорошни събития.	— дата и час на събитието, — тип на картата(ите), номер, държава членка, издала картата, и поколение на картата, предизвикваща събитието. — брой сходни събития, възникнали същия ден
Конфликт, предизвикан от карта	— десетте най-скорошни събития.	— дата и час на началото на събитието, — дата и час на края на събитието, — тип и номер на картата(ите), държава членка, издала картата(ите), и поколение на двете карти, предизвикващи събитието.
Неправилно приключване на последната картова сесия	— десетте най-скорошни събития.	— дата и час на вкарване на картата, — тип и номер на картата(ите), държава членка, издала картата(ите), поколение, — данни относно последната сесия така, както са прочетени от картата: — дата и час на вкарване на картата, — VRN, държава членка на регистрация и поколение на бордовото устройство.
Прекъсване на електрическото захранване (2)	— най-продължителното събитие за всеки от десетте последни дни на възникване на това събитие, — петте най-продължителни събития през последните 365 дни.	— дата и час на началото на събитието, — дата и час на края на събитието, — тип и номер на картата(ите), държава членка, издала картата(ите), както и поколение на всяка карта, вкарана в началото и/или в края на събитието, — брой сходни събития, възникнали същия ден.
Грешка в комуникацията с устройството за връзка от разстояние	— най-продължителното събитие за всеки от десетте последни дни на възникване на това събитие, — петте най-продължителни събития през последните 365 дни.	— дата и час на началото на събитие, — дата и час на края на събитието, — тип и номер на картата(ите), държава членка, издала картата(ите), както и поколение на всяка карта, вкарана в началото и/или в края на събитието, — брой сходни събития, възникнали същия ден.
Липса на информация за местоположението от приемник на сигнали от GNSS	— най-продължителното събитие за всеки от десетте последни дни на възникване на това събитие, — петте най-продължителни събития през последните 365 дни.	— дата и час на началото на събитие, — дата и час на края на събитието, — тип и номер на картата(ите), държава членка, издала картата(ите), както и поколение на всяка карта, вкарана в началото и/или в края на събитието, — брой сходни събития, възникнали същия ден.
Грешка в данните за движението	— най-продължителното събитие за всеки от десетте последни дни на възникване на това събитие, — петте най-продължителни събития през последните 365 дни.	— дата и час на началото на събитието, — дата и час на края на събитието, — тип и номер на картата(ите), държава членка, издала картата(ите), както и поколение на всяка карта, вкарана в началото и/или в края на събитието, — брой сходни събития, възникнали същия ден.

Събитие	Правила за съхраняване на данните	Данни, които се регистрират при всяко събитие
Противоречие в данните за движението на превозното средство	— най-продължителното събитие за всеки от десетте последни дни на възникване на това събитие, — петте най-продължителни събития през последните 365 дни.	— дата и час на началото на събитието, — дата и час на края на събитието, — тип и номер на картата(ите), държава членка, издала картата(ите), както и поколение на всяка карта, вкарана в началото и/или в края на събитието, — брой сходни събития, възникнали същия ден.
Опит за нарушаване на сигурността	десетте най-скорошни събития за всеки тип събитие.	— дата и час на началото на събитието, — дата и час на края на събитие (ако е от значение), — тип и номер на картата(ите), държава членка, издала картата(ите), както и поколение на всяка карта, вкарана в началото и/или в края на събитието, — тип събитие.
Времеви конфликт	— най-продължителното събитие за всеки от десетте последни дни на възникване на това събитие, — петте най-продължителни събития през последните 365 дни.	— -уред за регистриране на дата и час — дата и час по GNSS, — тип и номер на картата(ите), държава членка, издала картата(ите), както и поколение на всяка карта, вкарана в началото и/или в края на събитието, — брой сходни събития, възникнали същия ден.

4) ПРЕДОСТАВЯНИ СЪС СЪГЛАСИЕТО НА ВОДАЧА КОДОВЕ НА ДАННИ ЗА СЪБИТИЯ

Събитие	Правила за съхраняване на данните	Данни, които се регистрират при всяко събитие
Управление на МПС без съответната карта	— най-продължителното събитие за всеки от десетте последни дни на възникване на това събитие, — петте най-продължителни събития през последните 365 дни.	— дата и час на началото на събитието, — дата и час на края на събитието, — тип и номер на картата(ите), държава членка, издала картата(ите), както и поколение на всяка карта, вкарана в началото и/или в края на събитието, — брой сходни събития, възникнали същия ден.
Вкарване на карта по време на управление на МПС	— последното събитие за всеки от десетте последни дни на възникване на това събитие,	— дата и час на събитието, — тип и номер на картата(ите), държава членка, издала картата(ите), поколение, — брой сходни събития, възникнали същия ден
Превишаване на скоростта (1)	— най-сериозното събитие (т.е. събитието, при което е достигната най-висока средна скорост) през десетте последни дни на възникване на това събитие, — петте най-сериозни събития през последните 365 дни. — първото събитие, възникнало след последното калибриране	— дата и час на началото на събитието, — дата и час на края на събитието, — максимална скорост, измерена по време на събитието, — средноаритметична скорост, измерена по време на събитието, — тип и номер на картата, държава членка, издала картата, и поколение на картата на водач (ако е приложимо), — брой сходни събития, възникнали същия ден.

5) ПРЕДОСТАВЯНИ БЕЗ СЪГЛАСИЕТО НА ВОДАЧА КОДОВЕ НА ДАННИ ЗА НЕИЗПРАВНОСТИ

Неизправност	Правила за съхраняване на данните	Данни, които се регистрират при всяка неизправност
Неизправност на картата	— десетте последни неизправности на картата на водач.	— дата и час на началото на неизправността, — дата и час на края на неизправността, — тип и номер на картата(ите), държава членка, издала картата(ите), поколение.
неизправности в уредите за регистриране на данните за движението	— десетте последни неизправности за всеки тип неизправност, — първата неизправност след последното калибриране.	— дата и час на началото на неизправност, — дата и час на края на неизправност, — тип на неизправността, — тип и номер на картата(ите), държава членка, издала картата(ите), както и поколение на всяка карта, вкарана в началото и/или в края на неизправността,

Тази неизправност се предизвиква от следните нередности при режимите, различни от режима на калибриране:

— Неизправност вътре в бордовото устройство

— Неизправност в печатащото устройство

— Неизправност в дисплея

— Грешка при изтегляне на данни

— Неизправност на датчика

— Неизправност в приемника на сигнали от GNSS или външното устройство за GNSS

— Неизправност в устройството за връзка от разстояние

6) ПРЕДОСТАВЯНИ БЕЗ СЪГЛАСИЕТО НА ВОДАЧА ДАННИ ЗА СПЕЦИФИЧНИ ЗА ПРОИЗВОДИТЕЛЯ СЪБИТИЯ И НЕИЗПРАВНОСТИ

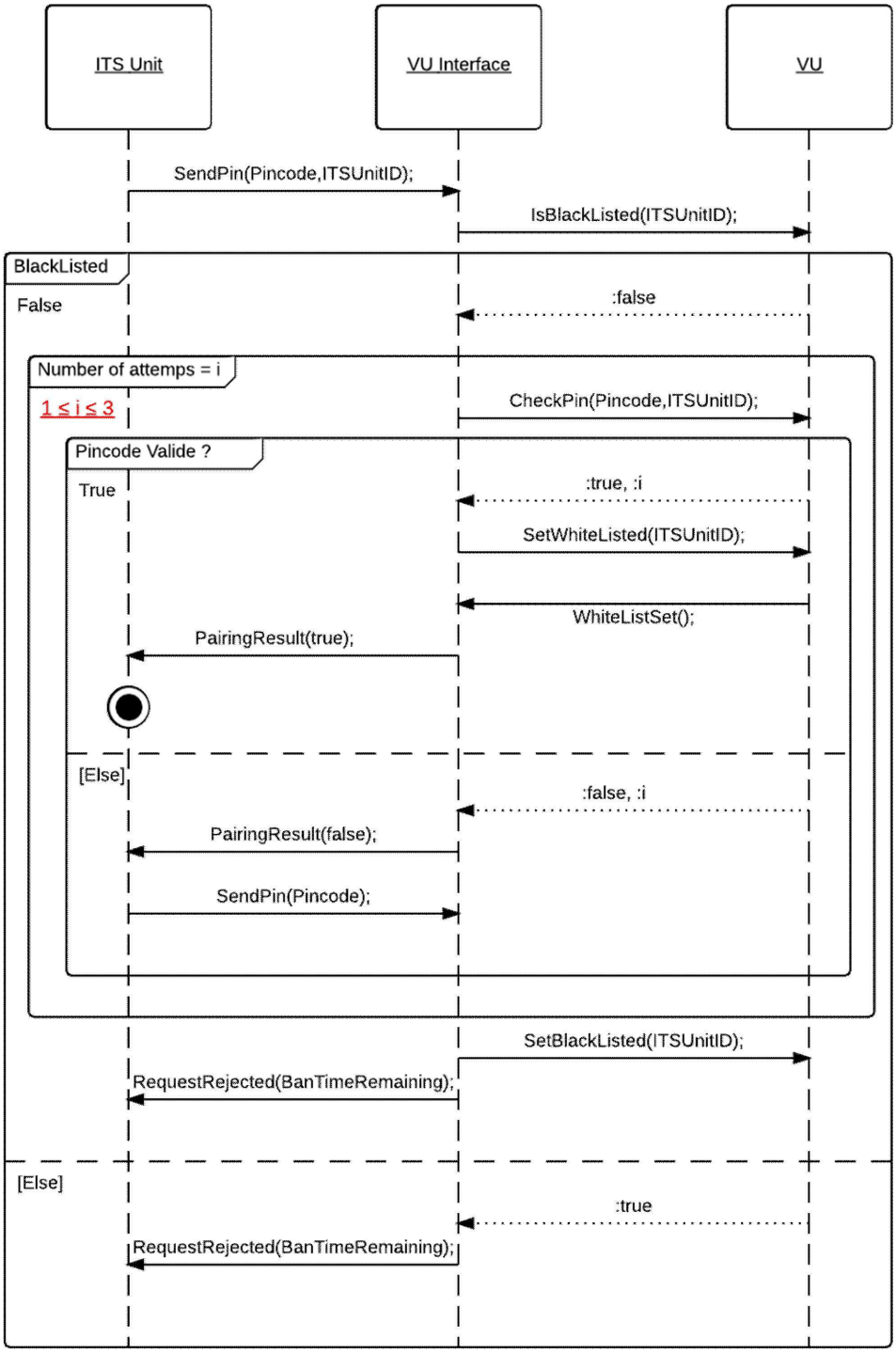
Събитие или неизправност	Правила за съхраняване на данните	Данни, които се регистрират при всяко събитие
Определят се от производителя	Определят се от производителя	Определят се от производителя

ПРИЛОЖЕНИЕ 2

ДИАГРАМИ НА ПОСЛЕДОВАТЕЛНОСТТА НА ОБМЕНА НА СЪОБЩЕНИЯ С ITS УСТРОЙСТВОТО

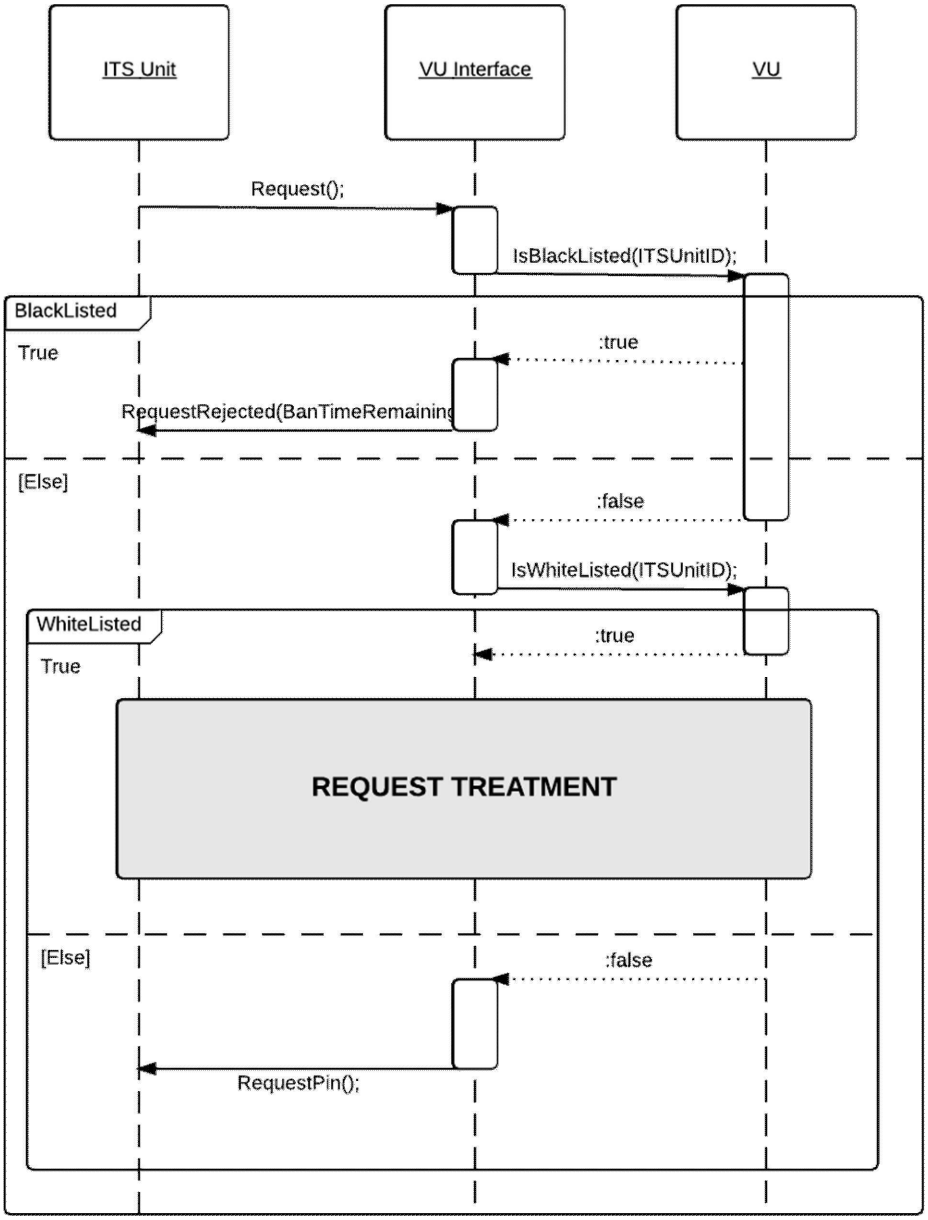
Фигура 1

Диаграма на последователността при опит за валидиране на PIN



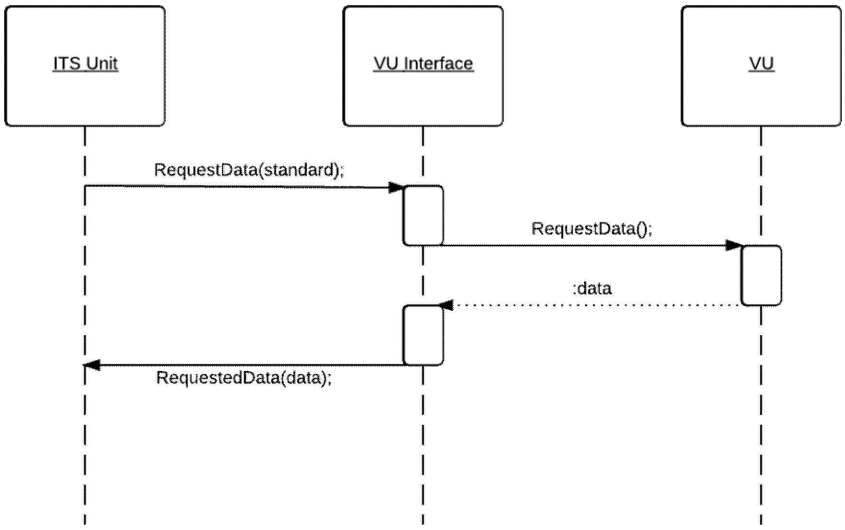
Фигура 2

Диаграма на последователността за проверката на разрешението на ITS устройството



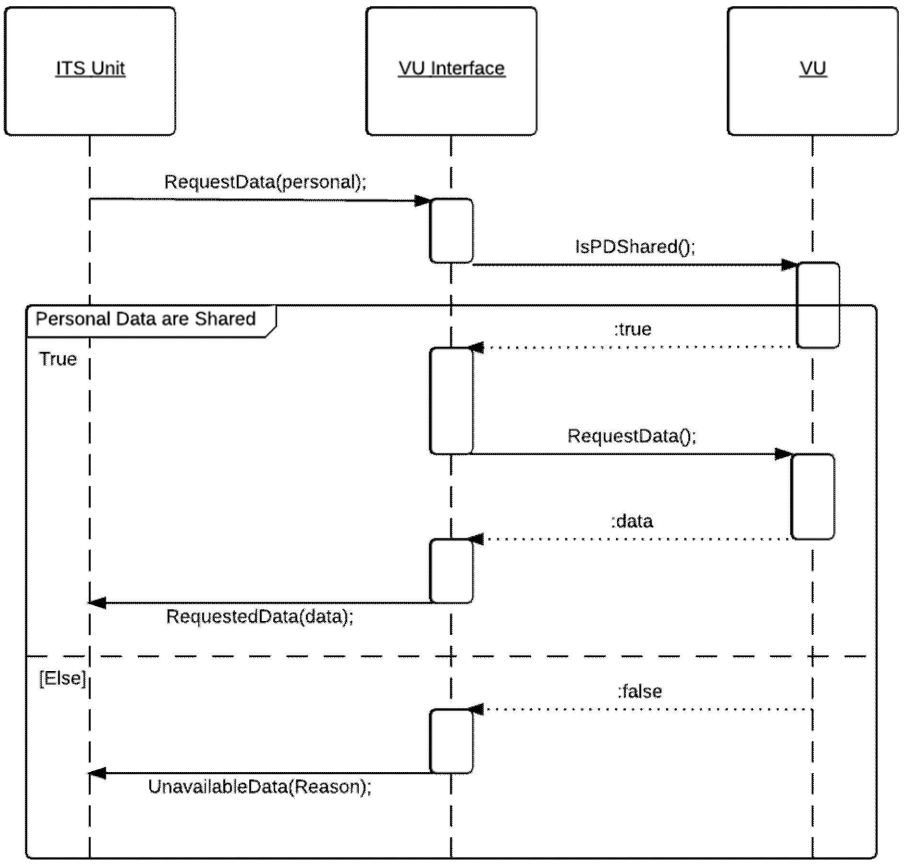
Фигура 3

Диаграма на последователността на обработката на заявка за данни, класифицирани като нелични (след правилен PIN за достъп)



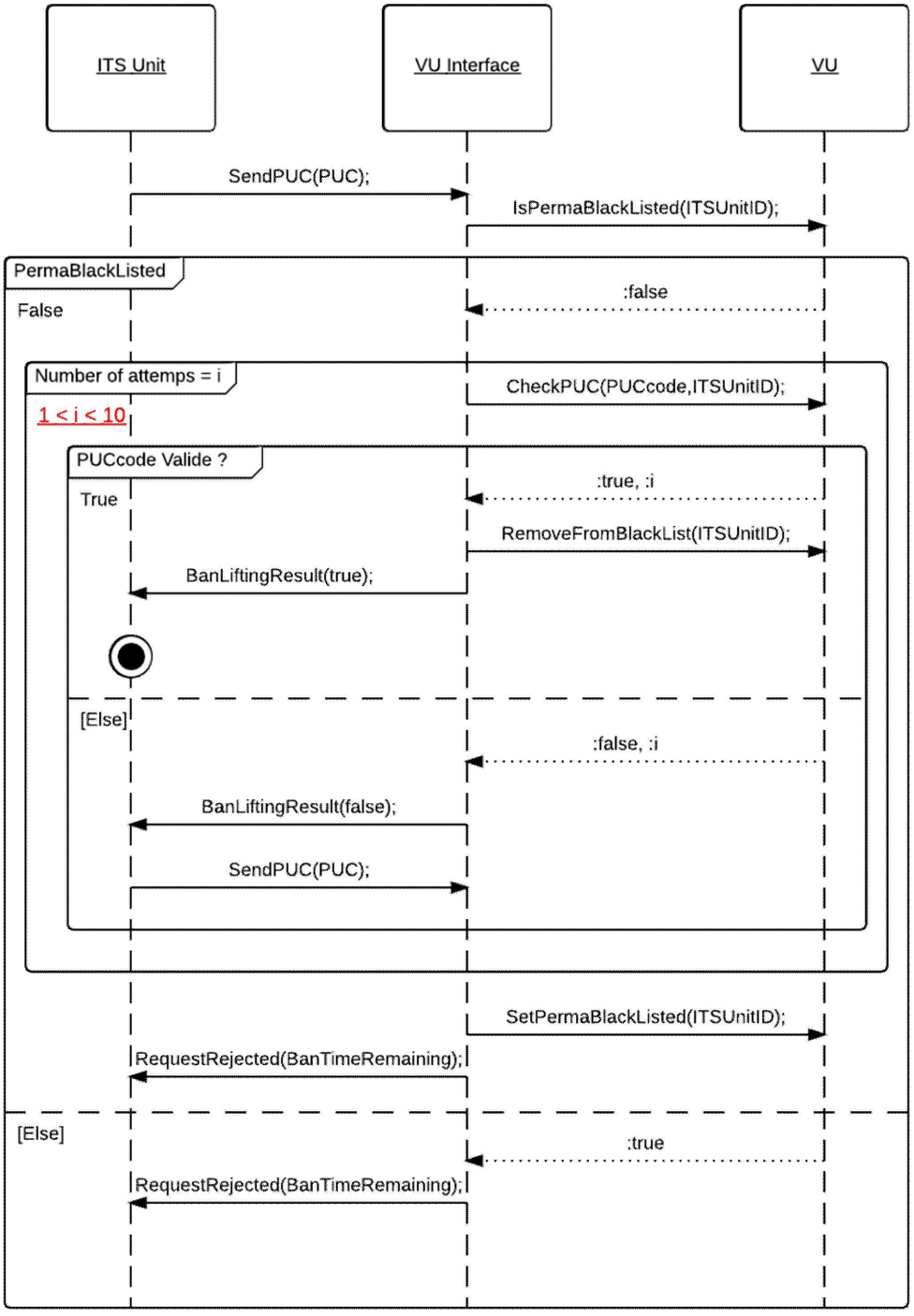
Фигура 4

Диаграма на последователността на обработката на заявка за данни, класифицирани като лични (след правилен PIN за достъп)



Фигура 5

Диаграма на последователността при опит за валидиране на PUC



ПРИЛОЖЕНИЕ 3

СПЕЦИФИКАЦИИ НА ASN.1

```
FormatMessageModule DEFINITIONS AUTOMATIC TAGS ::= BEGIN
EXPORTS ;
IMPORTS SendPIN, SendPUC, PairingResult, RequestPIN, RequestRejected,
        BanLiftingResult FROM PINPUCDataFieldsModule
        RequestAccepted,RequestData, DataUnavailable FROM
        RequestDataFieldsModule
        SendITSID, NegativeAnswer FROM OtherDataFieldsModule;

      CompleteMessage ::=SEQUENCE{
            header Header,
            data DataField,
            checksum Checksum
      }

      ----------------
      --HEADER TYPES--
      ----------------


      Header::=SEQUENCE{
            tgt IDList,
            src IDList,
            len BIT STRING (1..255)
      }

      vuID BIT STRING ::= 'EE'H
      IDList ::=CHOICE{
            vu BIT STRING (vuID),
            itsUnits SEQUENCE OF BIT STRING,
                  --Default hex Value:A0, redefined after first message exchange--
                  --Each ID will be linked to the Bluetooth ID of the device--
            ...
      }

      --------------------
      --DATAFIELDS TYPES--
      --------------------
      DataField ::=SEQUENCE{
            sid BIT STRING,
            trtp BIT STRING,
            subMBytes SubMessageBytes,
            dataField Content,
            ...
      }

      SubMessageBytes ::= SEQUENCE{
            currentSubM BIT STRING,
            totalSubM BIT STRING
      }

      Content ::= CHOICE{
            requestPIN RequestPIN,
            sendITSID SendITSID,
            sendPin SendPIN,
```

```
55                pairRslt PairingResult,
56                sendPUC SendPUC,
57                banlift BanLiftingResult,
58                requestRejected RequestRejected,
59                requestData RequestData,
60                requestOK RequestAccepted,
61                dataUnavailable DataUnavailable,
62                negAns NegativeAnswer
63          }
64
65          ------------------
66          --CHECKSUM TYPES--
67          ------------------
68
69          Checksum ::= SEQUENCE{
70                --SHA2 checksum
71          }
72    END
73
```

```
PINPUCDataFieldsModule DEFINITIONS AUTOMATIC TAGS ::= BEGIN
EXPORTS SendPIN, SendPUC, PairingResult, RequestPIN, RequestRejected,
BanLiftingResult;
IMPORTS ;

	----------
	---Utils--
	----------

	PUC ::= SEQUENCE (SIZE(8)) OF
	INTEGER (SIZE(0..9))

	PIN ::=	SEQUENCE (SIZE(4)) OF
		INTEGER (SIZE(0..9))

	--------------------------
	--Messages From ITS Unit--
	--------------------------

	SendPIN {PIN:pin} ::= SEQUENCE {
		sid BIT STRING ('03'H),
		pin PIN (pin)
	}

	SendPUC {PUC:puc} ::= SEQUENCE {
		sid BIT STRING ('05'H),
		puc PUC (puc)
	}
	--------------------
	--Messages From VU--
	--------------------

	PairingResult ::= SEQUENCE{
		sid BIT STRING ('04'H),
		result BOOLEAN
	}

	RequestPIN {MType:receivedRequest}::= SEQUENCE{
		sid BIT STRING ('01'H)
	}

	RequestRejected ::= SEQUENCE{
		sid BIT STRING ('07'H),
		banTimeRemaining GeneralizedTime, --PermaBan == 1k years-- }

	BanLiftingResult ::= SEQUENCE{
		sid BIT STRING ('06'H),
		result BOOLEAN
	}
END
```

```
RequestDataFields DEFINITIONS AUTOMATIC TAGS ::= BEGIN
	EXPORTS RequestAccepted,RequestData, DataUnavailable ;
	IMPORTS StandardEvent, PersonalEvent, StandardFault FROM EventsModule;

	------------------
	---From ITS Unit--
	------------------
	RequestData ::= SEQUENCE{
		sid BIT STRING ('08'H),
		requestedData DataTypeCode,
		...
	}

	-----------
	--From VU--
	-----------
	RequestAccepted ::=SEQUENCE{
		sid BIT STRING ('09'H),
		trtp DataTypeCode,
		dataSheet CHOICE{
			standardData StandardTachDataContent,
			personalData PersonalTachDataContent,
			gnss GNSSDataContent,
			standardEvent StandardEventContent,
			personalEvent PersonalEventContent,
			standardFault StandardFaultContent,
			manufacturerdata ManufacturerDataContent,
			...
		}
	}

	DataTypeCode ::=CHOICE{
		standardTachData BIT STRING ('01'H),
		personalTachData BIT STRING ('02'H),
		gnssData BIT STRING ('03'H),
		standardEventData BIT STRING ('04'H),
		personalEventData BIT STRING ('05'H),
		standardFaultData BIT STRING ('06'H),
		manufacturerData BIT STRING ('07'H),
		...
	}

	DataUnavailable ::=SEQUENCE{
		sid BIT STRING ('0A'H),
		trtp DataTypeCode,
		reason UnavailableDataCodes
	}

	UnavailableDataCodes ::= CHOICE{
		noDataAvailable BIT STRING ('10'H),
		personalDataNotShared BIT STRING ('11'H),
		...
	}
	----------------------------
	--Complete Tachograph Data--
	----------------------------
	--The format of the data was taken from the ISO16844-7 norm, more information
available in this ISO document–

```

```
Time ::= SEQUENCE{
	seconds INTEGER (0..59.75), --increment: 0.25s--
	minutes INTEGER (0..59), --increment: 1min--
	hours INTEGER (0..23), --increment: 1h--
	day INTEGER (0.25.. 31.75), --increment: 0.25d--
	month INTEGER (1..12), --increment: 1month--
	year INTEGER (1985..2235), --increment: 1year--
	locMinOffset INTEGER (-59..59), --increment: 1min--
	locHouroffset INTEGER (-23..23)--increment: 1h--
}

Date ::= SEQUENCE{
	month INTEGER (1..12), --increment: 1month--
	day INTEGER (0.25.. 31.75), --increment: 0.25d--
	year INTEGER (1985..2235) --increment: 1year--
}

DriverName ::=SEQUENCE{
	codePageSurname UTF8String, --See ISO/IEC 8859--
	surname UTF8String,
	codePageFirstname UTF8String, --See ISO/IEC 8859--
	firstname UTF8String,
}

--------------------
--Message Content--
--------------------

StandardTachDataContent ::= SEQUENCE{
	trtp DataTypeCode (DataTypeCode.&standardTachData),
	personal BOOLEAN (FALSE),
	data StandardTachyDataSheet,
}

PersonalTachDataContent ::= SEQUENCE{
	trtp DataTypeCode (DataTypeCode.&personalTachData),
	personal BOOLEAN (TRUE),
	data PersonalTachyDataSheet
}

GNSSDataContent ::= SEQUENCE{
	trtp DataTypeCode (DataTypeCode.&gnssData),
	personal BOOLEAN (TRUE),
	data GNSSDataSheet
}

StandardEventContent ::= SEQUENCE{
	trtp DataTypeCode (DataTypeCode.&standardEventData),
	personal BOOLEAN (FALSE),
	data StandardEventDataSheet
}

PersonalEventContent ::= SEQUENCE{
	trtp DataTypeCode (DataTypeCode.&personalEventData),
	personal BOOLEAN (TRUE),
	data PersonalEventDataSheet
}

StandardFaultContent ::= SEQUENCE{
```

```
243                 trtp DataTypeCode (DataTypeCode.&standardFaultData),
244                 personal BOOLEAN (FALSE),
245                 data StandardFault
246         }
247
248         ManufacturerDataContent ::= SEQUENCE{
249                 trtp DataTypeCode (DataTypeCode.&manufacturerData),
250                 personal BOOLEAN (TRUE),
251                 ...
252         }
253
254         ---------------
255         --DATA SHEETS--
256         ---------------
257
258         --Data sheet format follows ISO 16844-7.--
259         StandardTachyDataSheet ::= SEQUENCE{
260                 vin UTF8String (SIZE(17)),
261                 calibrationDate Date,
262                 driveRecognize INTEGER (2 UNION 12),
263                 driverCardDriver1 INTEGER (2 UNION 12),
264                 driverCardDriver2 INTEGER (2 UNION 12),
265                 timeDate Time,
266                 highResolutionTotalVehicleDistance INTEGER (0..21055406), --increment:
267   5m--
268                 serviceComponentIdentification INTEGER (0..255),
269                 serviceDelayCalendarTimeBased INTEGER (-125..125), --increment: 1week-
270   -
271                 nextCalibrationDate Date,
272                 speedAuthorised INTEGER (0..250.996), --increment 1/256km/h--
273                 tachographCardSlot1 INTEGER (0..4...), --Maximum 250--
274                 tachographCardSlot2 INTEGER (0..4...), --Maximum 250--
275                 outOfScopeCondition INTEGER(2 UNION 12),
276                 modeOfOperation INTEGER (0..4...), --Maximum 250--
277                 registeringMemberState UTF8String,
278         vehicleRegistrationNumber SEQUENCE {
279                         codePageVRN INTEGER (0..255),
280                         vrn OCTET STRING (SIZE(13)),
281                 },
282                 tachographNextMandatoryDownloadDate Date,
283                 ...
284         }
285
286         PersonalTachyDataSheet ::= SEQUENCE{
287                 tachographVehicleSpeed INTEGER (0..250.996), --increment 1/256km/h--
288                 driver1WorkingState INTEGER (2 UNION 12 UNION 102 UNION 112 UNION 1002
289   UNION 1012...),
290                 driver2WorkingState INTEGER (2 UNION 12 UNION 102 UNION 112 UNION 1002
291   UNION 1012...),
292
293                 driver1TimeRelatedStates INTEGER(2 UNION 12 UNION 102 UNION 112 UNION
294   1002 UNION
295                                                  1012 UNION 1102 UNION 1112 UNION
296   10002 UNION 10012 UNION
297                                                  10102 UNION 10112 UNION 11002 UNION
298   11012...),
299                 driver2TimeRelatedStates INTEGER(2 UNION 12 UNION 102 UNION 112 UNION
300   1002 UNION
```

```
                                                    1012 UNION 1102 UNION 1112 UNION
10002 UNION 10012 UNION
                                                    10102 UNION 10112 UNION 11002 UNION
11012...),

             overSpeed INTEGER (2 UNION 12),
             driver1Identification INTEGER (SIZE(19)), --TODO NEED FURTHER SPECS
FROM TACHO REGULATION--
             driver2Identification INTEGER (SIZE(19)), --TODO NEED FURTHER SPECS
FROM TACHO REGULATION--
             driver1ContinuousDrivingTime INTEGER (0.. 64255), --increment: 1min--
             driver2ContinuousDrivingTime INTEGER (0.. 64255), --increment: 1min--
             driver1CurrentDurationOfSelectedActivity INTEGER (0.. 64255), --
increment: 1min--
             driver2CurrentDurationOfSelectedActivity INTEGER (0.. 64255), --
increment: 1min--
             driver1Name DriverName,
             driver2Name DriverName,
             driver1CumulatedDrivingTimePreviousAndCurrentWeek INTEGER (0.. 64255),
--increment: 1min--
             driver2CumulatedDrivingTimePreviousAndCurrentWeek INTEGER (0.. 64255),
--increment: 1min--
             engineSpeed INTEGER(0..8031.875), --increment: 0,125r/min--
             driver1EndOfLastDailyRestPeriod Time,
             driver2EndOfLastDailyRestPeriod Time,
             driver1EndOfLastWeeklyRestPeriod Time,
             driver2EndOfLastWeeklyRestPeriod Time,
             driver1EndOfSecondLastWeeklyRestPeriod Time,
             driver2EndOfSecondLastWeeklyRestPeriod Time,
             driver1CurrentDailyDrivingTime INTEGER (0.. 64255), --increment: 1min-
-
             driver2CurrentDailyDrivingTime INTEGER (0.. 64255), --increment: 1min-
-
             driver1CurrentWeeklyDrivingTime INTEGER (0.. 64255), --increment:
1min--
             driver2CurrentWeeklyDrivingTime INTEGER (0.. 64255), --increment:
1min--
             driver1TimeLeftUntilNewDailyRestPeriod INTEGER (0.. 64255), --
increment: 1min--
             driver2TimeLeftUntilNewDailyRestPeriod INTEGER (0.. 64255), --
increment: 1min--
             driver1CardExpiryDate Date,
             driver2CardExpiryDate Date,
             driver1CardNextMandatoryDownloadDate Date,
             driver2CardNextMandatoryDownloadDate Date,
             driver1TimeLeftUntilNewWeeklyRestPeriod INTEGER (0.. 64255), --
increment: 1min--
             driver2TimeLeftUntilNewWeeklyRestPeriod INTEGER (0.. 64255), --
increment: 1min--
             driver1NumberOfTimes9hDailyDrivingTimesExceeded INTEGER (0..13),
             driver2NumberOfTimes9hDailyDrivingTimesExceeced INTEGER (0..13),
             driver1CumulativeUninterruptedRestTime INTEGER (0.. 64255), --
increment: 1min--
             driver2CumulativeUninterruptedRestTime INTEGER (0.. 64255), --
increment: 1min--
             driver1MinimumDailyRest INTEGER (0.. 64255), --increment: 1min--
             driver2MinimumDailyRest INTEGER (0.. 64255), --increment: 1min--
             driver1MinimumWeeklyRest INTEGER (0.. 64255), --increment: 1min--
             driver2MinimumWeeklyRest INTEGER (0.. 64255), --increment: 1min--
```

```
360                driver1MaximumDailyPeriod INTEGER (0..250), --increment: 1h--
361                driver2MaximumDailyPeriod INTEGER (0..250), --increment: 1h--
362                driver1MaximumDailyDrivingTime INTEGER (910 UNION 1010),
363                driver2MaximumDailyDrivingTime INTEGER (910 UNION 1010),
364                driver1NumberOfUsedReducedDailyRestPeriods INTEGER (0..13),
365                driver2NumberOfUsedReducedDailyRestPeriods INTEGER (0..13),
366                driver1RemainingCurrentDrivingTime INTEGER (0.. 64255), --increment:
367   1min--
368                driver2RemainingCurrentDrivingTime INTEGER (0.. 64255), --increment:
369   1min--
370                ...
371          }
372
373          GNSSDataSheet ::=  SEQUENCE {
374          gnssPosition GeoCoordinates
375                --See Appendix 1 for definition of GeoCoordinates--
376          }
377
378          StandardEventDataSheet ::= SEQUENCE{
379                events SEQUENCE OF StandardEvent
380          }
381
382          PersonalEventDataSheet ::= SEQUENCE{
383                events SEQUENCE OF PersonalEvent
384          }
385   END
386
387   EventsModule DEFINITIONS AUTOMATIC TAGS ::= BEGIN
388          EXPORTS ALL;
389          IMPORTS NationAlpha FROM Appendix1; --See Appendix 1 for more information
390   about NationAlpha--
391
392                SecurityBreachEvent ::=SEQUENCE{
393                      --See Annex 1B for more information--
394                }
395
396                RecordingEquipmentFaultType ::= SEQUENCE{
397                      --See Annex 1B for more information--
398                }
399
400                StandardEvent::= CHOICE{
401                      insertionInvalidCard InsertionOfANonValidCard,
402                      cardConflict CardConflict,
403                      timeOverlap TimeOverlap,
404                      previousSessionNotClosed LastCardSessionNotCorrectlyClosed,
405                      overSpeeding OverSpeeding,
406                      powerSupplyInterruption PowerSupplyInterruption,
407                      comErrorWithRemoteFacility
408   CommunicationErrorWithTheRemoteCommunicationFacility,
409                      absenceGNSSPosition
410   AbsenceOfPositionInformationFromGNSSReceiver,
411                      positionDataError PositionDataError,
412                      motionDataError MotionDataError,
413                      vehicleMotionConflict VehicleMotionConflict,
414                      securityBreachAttempt SecurityBreachAttempt,
415                      timeConflict TimeConflict,
416                      ...
417                }
418
```

```
PersonalEvent ::= CHOICE{
	lackOfAppropriateCard DrivingWithoutAnAppropriateCard,
	cardInsertionWhileDriving CardInsertionWhileDriving,
	overSpeeding OverSpeeding,
	...
}

StandardFault ::= CHOICE{
	cardFault CardFault,
	recordingEquipementFault RecordingEquipmentFault,
...
}

---------------
--EVENTS LIST--
---------------

InsertionOfANonValidCard::=SEQUENCE{
	beginDate GeneralizedTime,
	endDate GeneralizedTime,
	carsdType SEQUENCE OF UTF8String,
	cardsNumber SEQUENCE OF INTEGER,
	issuingMemberState SEQUENCE OF NationAlpha,
	cardsGeneration SEQUENCE OF INTEGER
}

CardConflict ::= SEQUENCE{
	beginDate GeneralizedTime,
	endDate GeneralizedTime,
	carsdType SEQUENCE OF UTF8String,
	cardsNumber SEQUENCE OF INTEGER,
	issuingMemberState SEQUENCE OF NationAlpha,
	cardsGeneration SEQUENCE OF INTEGER
}

TimeOverlap ::=SEQUENCE{
	beginDate GeneralizedTime,
	endDate GeneralizedTime,
	carsdType SEQUENCE OF UTF8String,
	cardsNumber SEQUENCE OF INTEGER,
	issuingMemberState SEQUENCE OF NationAlpha,
	cardsGeneration SEQUENCE OF INTEGER,
	numberSimilarEvent INTEGER
}

DrivingWithoutAnAppropriateCard ::= SEQUENCE{
	beginDate GeneralizedTime,
	endDate GeneralizedTime,
	carsdType SEQUENCE OF UTF8String,
	cardsNumber SEQUENCE OF INTEGER,
	issuingMemberState SEQUENCE OF NationAlpha,
	cardsGeneration SEQUENCE OF INTEGER,
	numberOfSimilarEvent INTEGER
}

CardInsertionWhileDriving ::= SEQUENCE{
	date GeneralizedTime,
	carsdType SEQUENCE OF UTF8String,
	cardsNumber SEQUENCE OF INTEGER,
```

```
478                     issuingMemberState SEQUENCE OF NationAlpha,
479                     numberOfSimilarEvents INTEGER
480             }
481
482             LastCardSessionNotCorrectlyClosed ::=SEQUENCE{
483                     beginDate GeneralizedTime,
484                     endDate GeneralizedTime,
485                     carsdType SEQUENCE OF UTF8String,
486                     cardsNumber SEQUENCE OF INTEGER,
487                     issuingMemberState SEQUENCE OF NationAlpha,
488                     cardsGeneration SEQUENCE OF INTEGER,
489                     oldSession SEQUENCE{
490                             beginDate GeneralizedTime,
491                             endDate GeneralizedTime,
492                             vrn UTF8String,
493                             issuingMemberState NationAlpha,
494                             cardsGeneration INTEGER,
495                     }
496             }
497
498             OverSpeeding ::=SEQUENCE{
499                     beginDate GeneralizedTime,
500                     endDate GeneralizedTime,
501                     maximumSpeed INTEGER,
502                     averageSpeed INTEGER,
503                     cardType UTF8String,
504                     cardNumber INTEGER,
505                     issuingMemberState NationAlpha,
506                     cardGeneration INTEGER,
507                     numberOfSimilarEvents INTEGER
508             }
509
510             PowerSupplyInterruption ::=SEQUENCE{
511                     beginDate GeneralizedTime,
512                     endDate GeneralizedTime,
513                     carsdType SEQUENCE OF UTF8String,
514                     cardsNumber SEQUENCE OF INTEGER,
515                     issuingMemberState SEQUENCE OF NationAlpha,
516                     cardsGeneration SEQUENCE OF INTEGER,
517                     numberOfSimilarEvent INTEGER
518             }
519
520             CommunicationErrorWithTheRemoteCommunicationFacility ::=SEQUENCE{
521                     beginDate GeneralizedTime,
522                     endDate GeneralizedTime,
523                     carsdType SEQUENCE OF UTF8String,
524                     cardsNumber SEQUENCE OF INTEGER,
525                     issuingMemberState SEQUENCE OF NationAlpha,
526                     cardsGeneration SEQUENCE OF INTEGER,
527                     numberOfSimilarEvent INTEGER
528             }
529
530             AbsenceOfPositionInformationFromGNSSReceiver ::= SEQUENCE{
531                     beginDate GeneralizedTime,
532                     endDate GeneralizedTime,
533                     carsdType SEQUENCE OF UTF8String,
534                     cardsNumber SEQUENCE OF INTEGER,
535                     issuingMemberState SEQUENCE OF NationAlpha,
536                     cardsGeneration SEQUENCE OF INTEGER,
```

```
537                 numberOfSimilarEvent INTEGER
538           }
539
540           PositionDataError ::= SEQUENCE{
541                 beginDate GeneralizedTime,
542                 endDate GeneralizedTime,
543                 carsdType SEQUENCE OF UTF8String,
544                 cardsNumber SEQUENCE OF INTEGER,
545                 issuingMemberState SEQUENCE OF NationAlpha,
546                 cardsGeneration SEQUENCE OF INTEGER,
547                 numberOfSimilarEvent INTEGER
548           }
549
550           MotionDataError ::= SEQUENCE{
551                 beginDate GeneralizedTime,
552                 endDate GeneralizedTime,
553                 carsdType SEQUENCE OF UTF8String,
554                 cardsNumber SEQUENCE OF INTEGER,
555                 issuingMemberState SEQUENCE OF NationAlpha,
556                 cardsGeneration SEQUENCE OF INTEGER,
557                 numberOfSimilarEvent INTEGER
558           }
559
560           VehicleMotionConflict ::= SEQUENCE{
561                 beginDate GeneralizedTime,
562                 endDate GeneralizedTime,
563                 carsdType SEQUENCE OF UTF8String,
564                 cardsNumber SEQUENCE OF INTEGER,
565                 issuingMemberState SEQUENCE OF NationAlpha,
566                 cardsGeneration SEQUENCE OF INTEGER,
567                 numberOfSimilarEvent INTEGER
568           }
569
570           SecurityBreachAttempt ::= SEQUENCE{
571                 beginDate GeneralizedTime,
572                 endDate GeneralizedTime OPTIONAL,
573                 carsdType SEQUENCE OF UTF8String,
574                 cardsNumber SEQUENCE OF INTEGER,
575                 issuingMemberState SEQUENCE OF NationAlpha,
576                 numberOfSimilarEvent INTEGER,
577                 typeOfEvent SecurityBreachEvent
578           }
579
580
581           TimeConflict ::= SEQUENCE{
582                 beginDate GeneralizedTime,
583                 endDate GeneralizedTime,
584                 carsdType SEQUENCE OF UTF8String,
585                 cardsNumber SEQUENCE OF INTEGER,
586                 issuingMemberState SEQUENCE OF NationAlpha,
587                 cardsGeneration SEQUENCE OF INTEGER,
588                 numberOfSimilarEvent INTEGER
589           }
590
591           ---------------
592           --FAULTS LIST--
593           ---------------
594
595           CardFault ::= SEQUENCE{
```

```
596                     beginDate GeneralizedTime,
597                     endDate GeneralizedTime,
598                     carsdType SEQUENCE OF UTF8String,
599                     cardsNumber SEQUENCE OF INTEGER,
600                     issuingMemberState SEQUENCE OF NationAlpha,
601                     cardsGeneration SEQUENCE OF INTEGER,
602             }
603
604             RecordingEquipmentFault ::= SEQUENCE{
605                     beginDate GeneralizedTime,
606                     endDate GeneralizedTime,
607                     faultType RecordingEquipmentFaultType,
608                     carsdType SEQUENCE OF UTF8String,
609                     cardsNumber SEQUENCE OF INTEGER,
610                     issuingMemberState SEQUENCE OF NationAlpha,
611                     cardsGeneration SEQUENCE OF INTEGER,
612             }
613 END
```

Допълнение 14

ФУНКЦИЯ ЗА ВРЪЗКА ОТ РАЗСТОЯНИЕ

СЪДЪРЖАНИЕ

1 ВЪВЕДЕНИЕ

Настоящото допълнение определя проектирането и процедурите, които трябва да се следват за осъществяването на функцията за връзка от разстояние („връзката“), изисквана съгласно член 9 от Регламент (ЕС) № 165/2014 („Регламентът“).

DSC_1 В Регламент (ЕС) № 165/2014 се определя, че тахографът трябва да притежава функция за връзка от разстояние, която да дава възможност на представители на компетентните контролни органи да четат информация от тахографа на преминаващи превозни средства, използвайки оборудване за разпитване от разстояние (четеца за връзка с цел ранно откриване от разстояние [REDCR]), като това оборудване осъществява по-конкретно безжична връзка на честота 5,8 GHz по интерфейси CEN към специализирани съобщителни системи с малък обсег на действие (Dedicated Short Range Communication — DSRC).

Важно е да се разбере, че тази функция е предназначена да служи само като предварителен филтър, за да се подбират превозни средства за по-щателна проверка, и не заменя формалния процес на контрол, определен в разпоредбите на Регламент (ЕС) № 165/2014. Виж съображение 9 в преамбюла към този регламент, което гласи, че връзката от разстояние за целите на пътните проверки между тахографите и контролните органи улеснява извършването на целеви пътни проверки.

DSC_2 *Данните* се обменят чрез *връзката*, която трябва да бъде безжична на честота 5,8 GHz с използване на DSRC съгласно настоящото допълнение и изпитана спрямо съответните параметри по EN 300 674-1, {Electromagnetic compatibility and Radio spectrum Matters (ERM), т.е. въпроси по електромагнитната съвместимост и радиочестотния спектър; Road Transport and Traffic Telematics (RTTT), т.е. телематика за автомобилния транспорт и пътното движение (RTTT); Dedicated Short Range Communication (DSRC) transmission equipment (500 kbit/s / 250 kbit/s) operating in the 5,8 GHz Industrial, Scientific and Medical (ISM) band, т.е. специализирани съобщителни системи с малък обсег на действие (DSRC) (500 kbit/s / 250 kbit/s), работещи в честотната лента 5,8 GHz за промишлени, научни и медицински (ISM) цели; Part 1, т.е. част 1: General characteristics and test methods for Road Side Units (RSU) and On -Board Units (OBU), т.е. общи характеристики и методи за изпитване на крайпътни устройства (RSU) и бордови устройства (OBU)}.

DSC_3 *Връзката* със съобщителните системи се осъществява само когато това е заявено от оборудването на компетентния контролен орган, използвайки отговарящи на изискванията радиосъобщителни средства (*четеца за връзка с цел ранно откриване от разстояние (REDCR)*.

DSC_4 *Данните* се защитават, за да се гарантира цялостността им.

DSC_5 Достъпът до съобщените *данни* се ограничава до компетентните контролни органи, оправомощени да проверяват за нарушенията на Регламент (ЕО) № 561/2006 и Регламент (ЕС) № 165/2014, и до сервизите, доколкото това е необходимо, за да се провери правилното функциониране на тахографа.

DSC_6 Съобщените при осъществяване на *връзката данни* се ограничават до данните, необходими за извършване на целеви пътни проверки на превозни средства, при които е възможно манипулиране или злоупотреба с тахографа.

DSC_7 Цялостността и сигурността на данните се постига чрез защита на *данните* в бордовото устройство (VU) и чрез предаването само на защитените полезни данни и данни, свързани със сигурността (виж 5.4.4), по безжичната връзка от разстояние на честота 5,8 GHz с DSRC, което означава, че само оправомощени представители на компетентните контролни органи разполагат с нужните средства, за да разбират данните, предадени по *връзката*, и да проверяват тяхната автентичност. Виж допълнение 11 относно общите механизми за сигурност.

DSC_8 Данните трябва да съдържат времеви печат, посочващ момента на последното им актуализиране.

DSC_9 Съдържанието на данните, свързани със сигурността, трябва да е известно и да е под контрола на компетентните контролни органи и на страните, с които те споделят тази информация, като то е извън обхвата на разпоредбите относно *връзката*, която е предмет на настоящото допълнение, освен ако при *връзката* се предвижда с всеки пакет от полезни данни да се предава и пакет от данни, свързани със сигурността.

DSC_10 Трябва да е възможно използването на същата архитектура и оборудване за получаването на други концепти на данни (като например от бордово устройство за претегляне) чрез определената тук архитектура.

DSC_11 Трябва да се поясни, че в съответствие с член 9 от Регламент (ЕС) № 165/2014 (член 7) по *връзката* не се предават данни за самоличността на водача.

2 ОБХВАТ

Настоящото допълнение обхваща определянето на начина, по който представители на компетентните контролни органи използват специфицирана безжична DSRC връзка на честота 5,8 GHz, за да получат от разстояние данни (*данните*) от целево превозно средство, които удостоверяват, че е възможно това превозно средство да нарушава разпоредбите на Регламент (ЕС) №165/2014 и следва да бъде набелязано за спиране с оглед на по-нататъшно разследване.

Съгласно Регламент (ЕС) №165/2014 събраните данни се ограничават до данните, които удостоверяват възможно нарушение, или са свързани с тези данни, както е определено в член 9 от Регламент (ЕС) № 165/2014.

В този сценарий наличното време за връзка е ограничено, понеже връзката е *целева* и е разчетена за малък обсег. Освен това същите съобщителни средства за наблюдение на тахографа от разстояние (RTM) могат да бъдат използвани от компетентните контролни органи и за други приложения (например за максимално допустимите маси и размери на тежкотоварни превозни средства, определени в Директива 2015/719/ЕС) и тези действия могат да бъдат отделни или последователни по преценка на компетентните контролни органи.

В настоящото допълнение се определя:

— Съобщителното оборудване, процедури и протоколи, които да се използват за *връзката*

— Стандартите и регламентите, на които трябва да отговаря радиотехническото оборудване

— Представянето на *данните* на оборудването за *връзката*

— Процедурите за запитване и изтегляне на данни и последователността на операциите

— *Данни*, които трябва да бъдат предадени

— Възможно тълкуване на *данните*, предадени по *връзката*

— Разпоредби за свързаните със сигурността данни, отнасящи се до *връзката*

— Предоставянето на данните на компетентните контролни органи

— Как четецът за връзка с цел ранно откриване от разстояние може да заяви различни концепти на данни за теглото и други характеристики на превозните средства

Трябва да се поясни, че в настоящото допълнение не се определят:

— събирането на *данни* за функционирането и управлението в рамките на бордовото устройство (което се определя при проектирането на съответния продукт, освен ако е посочено друго в Регламент (ЕС) № 165/2014)

— формата на представяне на събраните данни на представителя на компетентните контролни органи, нито критериите, които да се използват от тези органи при вземането на решение кои превозни средства да бъдат спрени (което се определя при проектирането на продукта, освен ако е посочено друго в Регламент (ЕС) № 165/2014 или в решение за политиката на компетентните контролни органи). За пояснение: *данните* се предоставят по *връзката* на компетентните контролни органи само за да могат те да вземат информирани решения

— мерките за сигурност на данните (като например криптиране), отнасящи се до съдържанието на *данните* (които се определят в допълнение 11 относно общите механизми за сигурност)

— подробности за концепти на данни, различни от тези при RTM, които могат да бъдат получени, използвайки същата архитектура и оборудване

— подробности за поведението и управлението между бордовото устройство (VU) и неговото средство за DSRC (DSRC-VU), нито за поведението в рамките на DSRC-VU (освен във връзка с предоставянето на *данните*, когато е заявено така от REDCR).

3 СЪКРАЩЕНИЯ, ОПРЕДЕЛЕНИЯ И ОБОЗНАЧЕНИЯ

В настоящото допълнение се използват следните съкращения и определения, които са специфични за него:

Антената електрическо устройство, което преобразува електрическата енергия в радиовълни и обратно, използвано в съчетание с радиопредавател или радиоприемник. Когато радиопредавателят е в действие, той подава трептящ на радиочестота електрически ток към клемите на антената, която излъчва енергията от електрическия ток под формата на електромагнитни вълни (радиовълни). В режим на приемане антената прехваща част от енергията на електромагнитните вълни, за да генерира много ниско напрежение върху своите клеми, което се подава към приемник за усилване.

Връзката обмен на информация/данни между DSRC-REDCR и DSRC-VU съгласно раздел 5 във взаимоотношение „главен/подчинен“ (master-slave) с цел получаване на данните

Данните защитени данни в определен формат (виж 5.4.4), заявени от *DSRC-REDCR* и предоставени на *DSRC-REDCR* от *DSRC-VU* по DSRC връзка на честота 5,8 GHz link, както е определено в 5 по-долу

Регламент (ЕС) № 165/2014
Регламент (ЕС) № 165/2014 на Европейския парламент и на Съвета от 4 февруари 2014 г. относно тахографите в автомобилния транспорт, за отмяна на Регламент (ЕИО) № 3821/85 на Съвета относно контролните уреди за регистриране на данните за движението при автомобилен транспорт и за изменение на Регламент (ЕО) № 561/2006 на Европейския парламент и на Съвета за хармонизиране на някои разпоредби от социалното законодателство, свързани с автомобилния транспорт

AID Application Identifier („идентификатор на приложение“)

BLE Bluetooth Low Energy („Bluetooth с ниска енергия“)

BST Beacon Service Table („таблица за навигационните услуги“)

CIWD	Card insertion while driving („вкарване на карта по време на управление на МПС“)
CRC	cyclic redundancy check („циклична контролна сума“)
DSC (n)	идентификатор на изискване за конкретно допълнение за DSRC
DSRC	Dedicated Short Range Communication (специализирана връзка или специализирана съобщителна система с малък обсег на действие)
DSRC-REDCR	DSRC — Remote Early Detection Communication Reader (DSRC — четец за връзка с цел ранно откриване от разстояние)
DSRC-VU	DSRC — Vehicle Unit (DSRC — бордово устройство) Това е „устройството за ранно откриване от разстояние“, определено в приложение 1B.
DWVC	Driving without valid card („управление на МПС без валидна карта“)
EID	Element Identifier („идентификатор на елемент“)
LLC	Logical Link Control („управление на логическата връзка“)
LPDU	LLC Protocol Data Unit („единица данни по протокола LLC“)
OWS	Onboard Weighing System („бордова система за претегляне“)
PDU	Protocol Data Unit („единица данни по протокола“)
REDCR	Remote early detection communication reader („четец за връзка с цел ранно откриване от разстояние“) Това е „четящото устройство за връзка с цел ранно откриване от разстояние“, определение за което се дава в приложение 1B.
RTM	Remote Tachograph Monitoring („наблюдение на тахографа от разстояние“)
SM-REDCR	Security Module-Remote early detection communication reader („модул за сигурност на четеца за връзка с цел ранно откриване от разстояние“)
TARV	Telematics Applications for Regulated Vehicles (ISO 15638 series of Standards) („Телематични приложения за регулирани превозни средства“ — серия от стандарти ISO 15638)
VU	Vehicle Unit („бордово устройство“)
VUPM	Vehicle Unit Payload Memory („памет на бордовото устройство за полезни данни“)
VUSM	Vehicle Unit Security Module („модул за сигурност на бордовото устройство“)
VST	Vehicle Service Table (таблица за услуги във връзка с превозното средство)
WIM	Weigh in motion („претегляне в движение“)
WOB	Weigh on board („бордово претегляне“)

Спецификацията, определена в настоящото допълнение, се отнася до и зависи от всички или части от следните регламенти и стандарти. В разделите от настоящото допълнение са посочени относимите стандарти или относимите раздели на стандарти. В случай на противоречие разделите на настоящото допълнение имат предимство. В случай на противоречие, когато в настоящото допълнение липсва ясно определена спецификация, действието в рамките на ERC 70-03 (изпитано по отношение на съответните параметри по EN 300 674-1) има предимство, последвано в низходяща последователност от EN 12795, EN 12253, EN 12834 и EN 13372, 6.2, 6.3, 6.4 и 7.1.

Настоящото допълнение съдържа позовавания на следните регламенти и стандарти:

[1] Регламент (ЕС) № 165/2014 на Европейския парламент и на Съвета от 4 февруари 2014 г. относно тахографите в автомобилния транспорт, за отмяна на Регламент (ЕИО) № 3821/85 на Съвета относно контролните уреди за регистриране на данните за движението при автомобилен транспорт и за изменение на Регламент (ЕО) № 561/2006 на Европейския парламент и на Съвета за хармонизиране на някои разпоредби от социалното законодателство, свързани с автомобилния транспорт.

[2] Регламент (ЕО) № 561/2006 на Европейския парламент и на Съвета от 15 март 2006 г. за хармонизиране на някои разпоредби от социалното законодателство, свързани с автомобилния транспорт, за изменение на Регламенти (ЕИО) № 3821/85 и (ЕО) № 2135/98 на Съвета и за отмяна на Регламент (ЕИО) № 3820/85 на Съвета (текст от значение за ЕИП).

[3] ERC 70-03 CEPT: ECC Recommendation 70-03: Relating to the Use of Short Range Devices (SRD)

[4] ISO 15638 Intelligent transport systems — Framework for cooperative telematics applications for regulated commercial freight vehicles (TARV).

[5] EN 300 674-1 Electromagnetic compatibility and Radio spectrum Matters (ERM); Road Transport and Traffic Telematics (RTTT); Dedicated Short Range Communication (DSRC) transmission equipment (500 kbit/s / 250 kbit/s) operating in the 5,8 GHz Industrial, Scientific and Medical (ISM) band; Part 1: General characteristics and test methods for Road Side Units (RSU) and On-Board Units (OBU).

[6] EN 12253 Road transport and traffic telematics — Dedicated short-range communication — Physical layer using microwave at 5.8 GHz.

[7] EN 12795 Road transport and traffic telematics — Dedicated short-range communication — Data link layer: medium access and logical link control.

[8] EN 12834 Road transport and traffic telematics — Dedicated short-range communication — Application layer.

[9] EN 13372 Road transport and traffic telematics — Dedicated short-range communication — Profiles for RTTT applications.

[10] ISO 14906 Electronic fee collection — Application interface definition for dedicated short- range communication (Електронно събиране на такси. Определяне на приложния интерфейс за обмен на информация на близки разстояния).

4 ОПЕРАТИВНИ СЦЕНАРИИ

4.1 **Преглед**

Регламент (ЕС) № 165/2014 предоставя конкретни и контролирани сценарии, в рамките на които да се използва *връзката*.

Поддържат се следните сценарии:

„*Communication Profile 1:(Профил 1 за връзката:) Roadside inspection using a short range wireless communication Remote Early Detection Communication Reader instigating a physical roadside inspection (master-:-slave) (Пътна проверка, използвайки четец за връзка с цел ранно откриване от разстояние чрез съобщителна система с малък обсег на действие, която да предизвика физическа пътна проверка (главен-:-подчинен)*

Reader Profile 1a: (Профил 1а за четеца:) via a hand aimed or temporary roadside mounted and aimed Remote Early Detection Communication (чрез ръчно насочен или временно монтиран край пътя четец за връзка с цел ранно откриване)

Reader Profile 1b: (Профил 1б за четеца:) via a vehicle mounted and directed Remote Early Detection Communication Reader (чрез монтиран на превозно средство и насочен четец за връзка с цел ранно откриване)“.

4.1.1 *Условия за прехвърляне на данни чрез интерфейса към DSRC на 5,8 GHz*

ЗАБЕЛЕЖКА: за разбиране на контекста за предварителните условия трябва да се направи справка с фигура 14.3 по-долу.

4.1.1.1 Данни, съхранявани в бордовото устройство (VU)

DSC_12 От бордовото устройство се изисква да актуализира на всеки 60 секунди и да поддържа данните, които трябва да се съхраняват в него, без никакво участие на функцията за специализирана връзка с малък обсег на действие (DSRC). Това се постига по вътрешен за бордовото устройство начин, който е определен не в настоящото допълнение, а в раздел 3.19 „*Връзка от разстояние за целеви пътни проверки*“ от приложение 1В към Регламент (ЕС) № 165/2014.

4.1.1.2 Данни, предоставяни на средството за DSRC на бордовото устройство (DSRC-VU)

DSC_13 От бордовото устройство се изисква да актуализира предаваните по DSRC тахографски данни (*данните*) всеки път когато съхраняваните в него данни се актуализират през интервала, определен в точка 4.1.1.1 (DSC_12), без никакво участие на функцията за DSRC.

DSC_14 Данните в бордовото устройство се използват като основа за получаване и актуализиране на полезните данни (*данните*), като начинът за постигане на това е определен в раздел 3.19 „*Връзка от разстояние за целеви пътни проверки*“ от приложение 1B, а ако не е определен там, се определя не в настоящото допълнение, а при проектирането на съответния продукт. Проектирането на връзката между средството за DSRC на бордовото устройство и самото бордово устройство се разглежда в раздел 5.6.

4.1.1.3 Съдържание на данните

DSC_15 Съдържанието и форматът на данните трябва да бъдат такива, че след тяхното декриптиране да са структурирани и налични във форма и формат, определен в раздел 5.4.4 от настоящото допълнение („Структури на данните“).

4.1.1.4 Представяне на данните

DSC_16 Данните, които се актуализират често в съответствие с процедурите, определени в точка 4.1.1.1, се защитават, преди да бъдат представени на *DSRC-VU*, и се представят като защитена стойност на концепта на данните за временно съхранение в *DSRC-VU* като текуща версия на *данните*. Тези данни се прехвърлят от *VUSM* (модула за сигурност на бордовото устройство) към DSRC-функцията *VUPM* (паметта на бордовото устройство за полезни данни). *VUSM* и *VUPM* представляват функции, а не непременно физически обекти. Формата на физическо изпълнение на тези функции се определя при проектирането на съответния продукт, ако не е определена другаде в Регламент (ЕС) № 165/2014.

4.1.1.5 Данни, свързани със сигурността

DSC_17 Данните, свързани със сигурността (*securityData*), включително данните, изисквани от REDCR, за да придобие пълна способност да декриптира *данните*, се предоставят съгласно допълнение 11 относно общите механизми за сигурност и се представят като стойност на концепта на данните за временно съхранение в *DSRC-VU* като текуща версия на *securityData* във формата, определена в раздел 5.4.4 от настоящото допълнение.

4.1.1.6 Данни във VUPM, които са на разположение за прехвърляне по интерфейса към DSRC

DSC_18 Концептът на данните, който трябва винаги да е на разположение в DSRC-функцията VUPM за незабавно прехвърляне по заявка от *REDCR*, е определен в раздел 5.4.4 за пълните спецификации на модула ASN.1.

Общ преглед на профил 1 за връзката

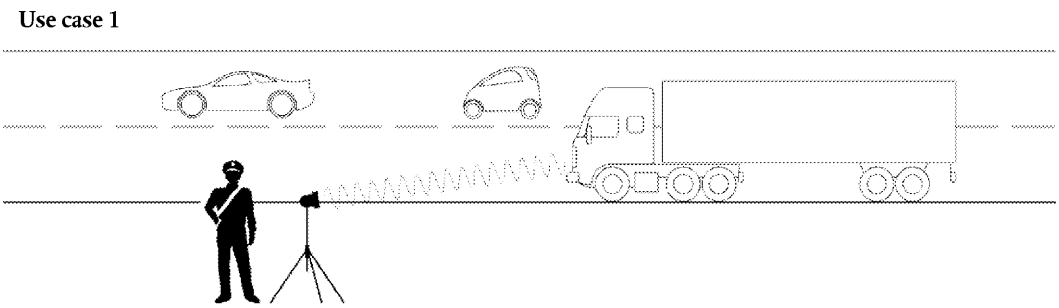
Този профил обхваща случаите на употреба, когато представител на компетентните контролни органи използва четец за връзка с цел ранно откриване от разстояние чрез съобщителна система с малък обсег на действие (с DSRC интерфейси на 5,8 GHz, функциониращи в рамките на ERC 70-03 и изпитани по отношение на съответните параметри по EN 300 674-1, както е описано в раздел 5) (*REDCR*), за да идентифицира от разстояние превозно средство, което евентуално нарушава разпоредбите на Регламент (ЕС) №165/2014. След като контролиращият разпитването за данни представител на компетентните контролни органи идентифицира превозното средство, той решава дали това превозно средство следва да бъде спряно.

4.1.2 *Профил 1a: чрез ръчно насочен или временно монтиран край пътя четец за връзка с цел ранно откриване*

В този случай представителят на компетентните контролни органи се намира край пътя и насочва от там държан с ръка, монтиран върху триножник или подобен преносим *REDCR* към центъра на предното стъкло на целевото превозно средство. За разпитването се използват DSRC интерфейси на 5,8 GHz, функциониращи в рамките на ERC 70-03 и изпитани по отношение на съответните параметри по EN 300 674-1, както е описано в раздел 5. Виж фигура 14.1 (случай № 1 на употреба).

Фигура 14.1

Крайпътно разпитване за данни чрез DSRC на 5,8 GHz



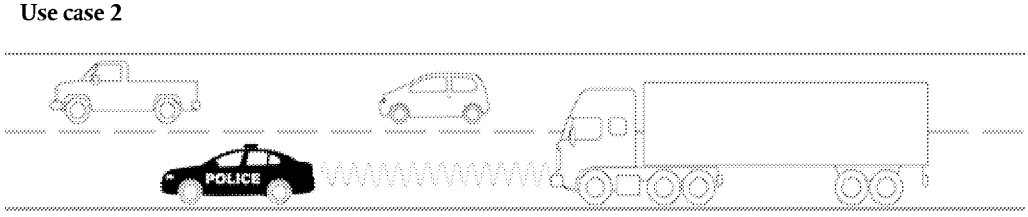
Крайпътен REDCR

4.1.3 *Профил 1б: чрез монтиран на превозно средство и насочен четец за връзка с цел ранно откриване (REDCR)*

В този случай представителят на компетентните контролни органи се намира в движещо се превозно средство и насочва държан с ръка *REDCR* към центъра на предното стъкло на целевото превозно средство или *REDCR* е монтиран вътре в превозното средство или върху него така, че да сочи към центъра на предното стъкло на целевото превозно средство, когато превозното средство с четеца за връзка с цел ранно откриване се намира в определено положение спрямо целевото превозно средство (например непосредствено пред него в пътния поток). За разпитването се използват DSRC интерфейси на 5,8 GHz, функциониращи в рамките на ERC 70-03 и изпитани по отношение на съответните параметри по EN 300 674-1, както е описано в раздел 5. Виж фигура 14.2 (случай № 2 на употреба).

Фигура 14.2

Разпитване за данни с монтиран в превозно средство четец чрез DSRC на 5,8 GHz



Мобилен REDCR

4.2 **Сигурност и цялост на данните**

С цел да се даде възможност за проверка на автентичността и цялостността на данните, изтеглени по връзката от разстояние, защитените данни се проверяват и декриптират съгласно допълнение 11 относно общите механизми за сигурност.

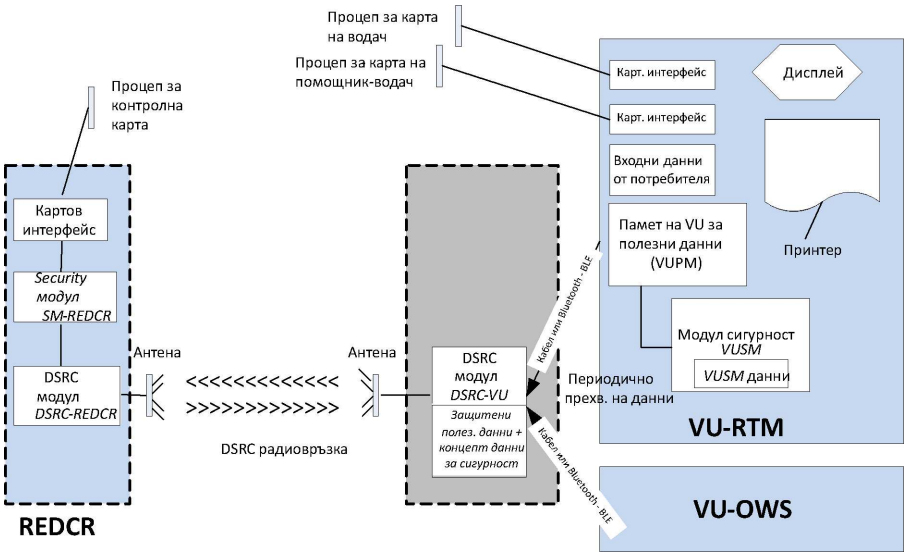
5 СТРУКТУРА И ПРОТОКОЛИ ЗА ВРЪЗКАТА ОТ РАЗСТОЯНИЕ

5.1 **Структура**

Структурата за реализиране на функцията за връзка от разстояние в интелигентния тахограф е показана на фигура 14.3.

Фигура 14.3

Структура за реализиране на функцията за връзка от разстояние



DSC_19 Бордовото устройство осъществява следните функции:

— Модул за сигурност (*VUSM*). Тази функция на бордовото устройство отговаря за защитата на *данните*, които трябва да се предадат от *DSRC-VU* на представителя на компетентните контролни органи по връзката от разстояние.

— Защитените данни се съхраняват в паметта на VUSM. През интервали, определени в 4.1.1.1 (DSC_12), бордовото устройство криптира и подава наново концепта на данните за RTM (който включва стойностите на концептите на полезните данни и на свързаните със сигурността данни, определени по-долу в настоящото допълнение), съхранявани в паметта на DSRC-VU. Функциониране на модула за сигурност е определено в допълнение 11 относно общите механизми за сигурност и е извън обхвата на настоящото допълнение, освен ако от него се изисква да предоставя актуализация на средството за връзка на бордовото устройство (VU Communication facility) при всяка промяна на данните във VUSM.

— Връзката между VU и DSRC-VU може да бъде жична или Bluetooth Low Energy (BLE), а DSRC-VU може да е обединено физически с антената върху предното стъкло на целевото превозно средство, да е вътре в бордовото устройство или да е разположено някъде между тях.

— DSRC-VU трябва да разполага по всяко време с надежден източник на електроенергия. Начинът на неговото електрическо захранване се определя при проектирането му.

— Паметта на DSRC-VU трябва да бъде енергонезависима с цел запазване на данните в DSRC-VU дори когато електрическата система на превозното средство е изключена.

— Ако връзката между VU и DSRC-VU се осъществява чрез BLE и електроенергийният източник не е акумулаторна батерия, електроенергийният източник на DSRC-VU се подменя при всеки периодичен технически преглед, а производителят на DSRC-VU гарантира, че електрическото захранване е в състояние да издържи от един периодичен технически преглед до следващия, като осигурява нормален достъп до данните чрез REDCR през целия период без неизправност или прекъсване.

— Функция „памет за полезните данни“ (payload memory) на VU (*VUPM*) за RTM. Тази функция на VU служи за предоставяне и актуализиране на *данните*. Съдържанието на *данните* („Tachograph-Payload“) е определено в 5.4.4/5.4.5 и се актуализира през интервала, определен в 4.1.1.1 (DSC_12).

— DSRC-VU. Това е функцията, осъществявана в рамките на антената или свързано с нея и чрез комуникация с VU посредством жична или безжична (BLE) връзка, която поддържа текущите данни (*VUPM-data*) и управлява отговарянето на разпитване по DSRC на 5,8 GHz. Прекъсването на специализираната връзка с малък обсег на действие (DSRC) или намесата по време на нормалната експлоатация на превозното средство във функционирането на тази връзка се счита за нарушение на Регламент (ЕС) № 165/2014.

— Модулът за сигурност на REDCR (*SM-REDCR*) е функцията, използвана за декриптиране и проверка на цялостността на данните, произхождащи от VU. Начинът за постигане на това се определя в допълнение 11 относно общите механизми за сигурност, а не в настоящото допълнение.

— Функцията DSRC на REDCR (*DSRC-REDCR*) се осъществява от приемопредавател на честота 5,8 GHz и съответен фърмуер и софтуер, който управлява *връзката* с *DSRC-VU* съгласно настоящото допълнение.

— *DSRC-REDCR* разпитва *DSRC-VU* на целевото превозно средство и получава *данните* (текущите *данни* от *VUPM* на целевото превозно средство) по DSRC, обработва и съхранява получените данни в своя *SM-REDCR*.

— Антената на DSRC-VU (*антената*) трябва да е разположена в центъра или близо до центъра на предното стъкло на превозното средство на височина от около 1,5—2,2 m. За тежкотоварни превозни средства тя трябва да бъде във или близо до долната част на предното стъкло. За леки превозни средства е подходящо монтиране в горната част на предното стъкло.

— Пред антената или в близост до нея не трябва да има никакви метални предмети (напр. поименни служебни карти, стикери, противоотразяващи (затъмняващи) ленти, слънчеви козирки или чистачки в покой на предното стъкло), които могат да влияят върху връзката.

— Антената се монтира така, че нейната диаграма на насоченост да е приблизително успоредна на повърхността на пътя.

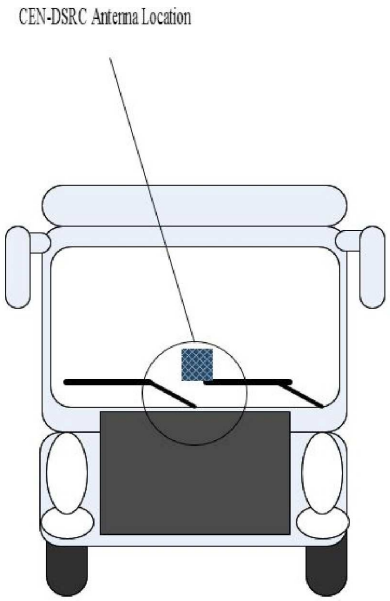
DSC_20 Антената и връзката трябва да функционират в рамките на ERC 70-03 и да са изпитани по отношение на съответните параметри по EN 300 674-1, както е описано в раздел 5. Антената и връзката могат да прилагат техники за ограничаване на смущенията в безжичната връзка, както е описано в доклад № 228 на ECC, като например се използват филтри.

DSC_21 Антената за DSRC се свързва със средството за DSRC на VU или пряко в модула, монтиран на предното стъкло или в близост до него, или посредством специален кабел, конструиран така, че да затруднява неправомерно разкачване. Разкачването на *антената* или намесата в нейното функциониране се счита за нарушение на Регламент (ЕС) № 165/2014. Умишленото екраниране на *антената* или отрицателното въздействие по друг начин върху нейните работни характеристики се счита за нарушение на Регламент (ЕС) № 165/2014.

DSC_22 Форм-факторът на антената не е определен и е предмет на търговско решение, стига монтираното DSRC-VU да отговаря на изискванията за съответствие, посочени в раздел 5 по-долу. Антената се разполага, както е определено в DSC_19 и показано на фигура 14.4 (овалната линия), като тя трябва да е ефикасна за случаите на употреба, описани в 4.1.2 и 4.1.3.

Фигура 14.4

Пример за разполагането на антената за DSRC на 5,8 GHz на предното стъкло на регулирани превозни средства



Форм-факторът на четеца *REDCR* и неговата антена може да е различен в зависимост от обстоятелствата по четеца (дали той е монтиран върху триножник, държан с ръка, монтиран в превозно средство и т.н.) и от начина на работа на представителя на компетентните контролни органи.

Използва се функция за показване и/или уведомяване, за да се дадат на представителя на компетентните контролни органи резултатите от функцията за връзка от разстояние. Показването може да бъде върху екран, като разпечатка, звуков сигнал или комбинация от тези различни форми на уведомяване. Формата на това показване и/или уведомяване зависи от изискванията на представителите на компетентните контролни органи и от конструкцията на оборудването и не е определена в настоящото допълнение.

DSC_23 Конструкцията и форм-факторът на *REDCR* се определят от производителя в рамките на ERC 70-03 и от спецификациите за конструкцията и работните характеристики, дадени в настоящото допълнение (раздел 5.3.2), като по този начин се предоставя максимална свобода на участниците в пазара да проектират и доставят оборудване, което да покрива специфичните сценарии за разпитване на конкретния компетентен контролен орган.

DSC_24 Конструкцията и форм-факторът на *DSRC-VU*, както и неговото разполагане във или извън VU, се определят от производителя в рамките на ERC 70-03 и от спецификациите за конструкцията и работните характеристики, дадени в настоящото допълнение(раздел 5.3.2) и в рамките на настоящия раздел (5.1).

DSC_25 *DSRC-VU* обаче трябва да е в състояние в приемлива степен да възприема стойности на концепти на данни от друго интелигентно оборудване на превозни средства посредством връзка и протоколи по отворен отраслови стандарт (например от бордово оборудване за претегляне), стига тези концепти на данни да се идентифицират от уникални и известни идентификатори на приложения / имена на файлове, а инструкциите за прилагане на такива протоколи трябва да се представят на Европейската комисия и да се предоставят безплатно на производителите на съответното оборудване.

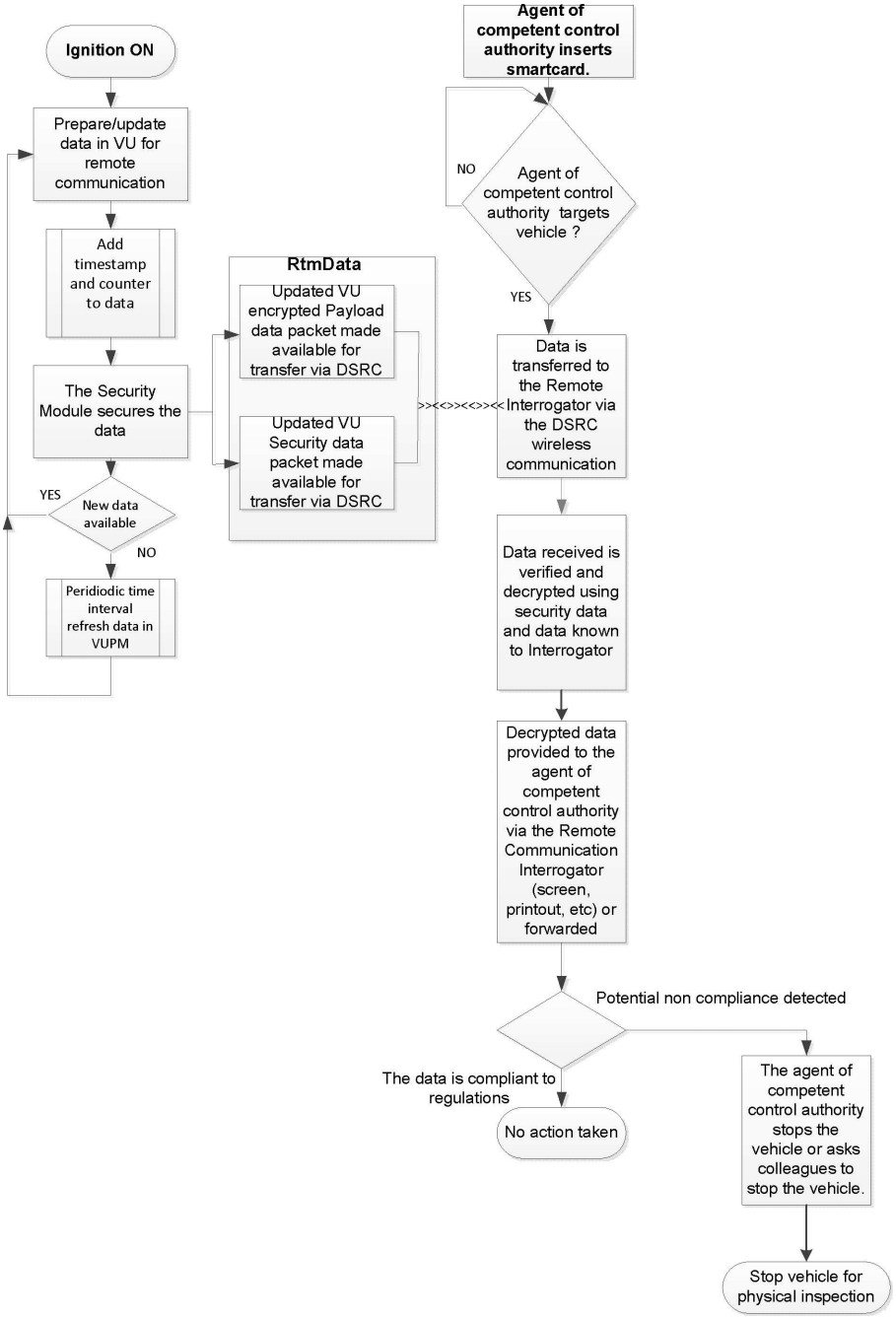
5.2 **Блоксхема**

5.2.1 *Действия*

Блоксхемата на действията е показана на фигура 14.5.

Фигура 14.5

Блоксхема на функцията за връзка от разстояние



Стъпките са описани по-долу:

а) Когато превозното средство е в действие (т.е. контактният ключ е в положение „включено“), тахографът подава данни на функцията VU. Функцията VU подготвя *данните* за функцията за връзка от разстояние (криптира ги) и актуализира *VUPM*, съдържаща се в паметта на *DSRC-VU* (както е определено в 4.1.1.1—4.1.1.2). Събраните *данни* се актуализират съгласно 5.4.4—5.4.5 по-долу.

б) При всяка актуализация на *данните* се актуализира и времевият печат, определен в концепта на данните, свързани със сигурността.

в) Функцията *VUSM* осигурява защитата на данните в съответствие с процедурите, определени в допълнение 11.

г) При всяка актуализация на *данните* (виж 4.1.1.1—4.1.1.2), те се прехвърлят към *DSRC-VU*, където заместват предишните данни, така че винаги да са налични актуализирани текущи данни (*данните*), които да бъдат предоставени в случай на разпитване от четец *REDCR*. Когато *данните* се предоставят от VU на DSRC-VU, трябва да е възможно тяхното идентифициране по името на файла *RTMData или* по идентификатори на приложението (ApplicationID) и атрибута (Attribute).

д) Ако представител на компетентния контролен орган желае да получи *данни* от целево превозно средство, той най-напред вкарва своята карта с чип в *REDCR*, за да се установи *връзката* и да се даде възможност на *SM-REDCR* да провери нейната автентичност и да декриптира данните.

е) След това представителят на компетентния контролен орган насочва четеца към превозното средство и изисква данните по връзката от разстояние. *REDCR* открива сесия по интерфейса за DSRC на 5,8 GHz с *DSRC-VU* на целевото превозно средство и заявява *данните*. *Данните* се прехвърлят към *REDCR* по безжичната съобщителна система като DSRC атрибут, използвайки услугата GET на приложението, както е определено 5.4. Атрибутът съдържа криптираните стойности на полезните данни и данните, свързани със сигурността на DSRC.

ж) Данните се анализират от четеца *REDCR* и се подават на представителя на компетентния контролен орган.

з) Представителят на компетентния контролен орган използва данните, за да реши дали превозното средство да бъде спряно за задълбочена проверка и, ако вземе такова решение, се обръща към друг представител на компетентния контролен орган с искане за спирането на превозното средство.

5.2.2 *Тълкуване на данните, получени по връзката DSRC*

DSC_26 Данните, получени по интерфейса на честота 5,8 GHz, трябва да бъдат със смисъла и значението, определени в 5.4.4 и 5.4.5 по-долу, и единствено с този смисъл и значение, и трябва да се тълкуват съобразно целите, определени там. В съответствие с разпоредбите на Регламент (ЕС) № 165/2014 *данните* се използват единствено за предоставяне на относима информация на компетентен контролен орган с оглед той да бъде подпомогнат при подбора на превозни средства, които следва да бъдат спрени за физическа проверка, и впоследствие те се унищожават съгласно член 9 от Регламент (ЕС) № 165/2014.

5.3 **Параметри на физическия DSRC интерфейс за връзка от разстояние**

5.3.1 *Ограничения за местоположението*

DSC_27 Разпитването на превозни средства от разстояние, използвайки DSRC интерфейс на 5,8GHz, следва да се извършва на не по-малко от 200 метра от функциониращ DSRC портал.

5.3.2 *Параметри на предаването на данни в права и обратна посока*

DSC_28 Оборудването, използвано за наблюдение на тахограф от разстояние, трябва да бъде в съответствие с ERC70-03 и да функционира в неговите рамки, както и с параметрите, определени в таблици 14.1 и 14.2 по-долу.

DSC_29 Освен това оборудването, използвано за наблюдение на тахограф от разстояние, трябва да бъде в съответствие с параметрите от EN 12253 и EN 13372, за да се гарантира оперативна съвместимост с работните параметри на други стандартизирани системи за DSRC на 5,8 GHz.

Това са именно:

Таблица 14.1.

Параметри на предаването на данни в права посока

Позиция №	Параметър	Стойност(и)	Забележка
D1	Носещи честоти за предаване в права посока	Има четири алтернативи, които могат да бъдат използвани от REDCR: 5,7975 GHz 5,8025 GHz 5,8075 GHz 5,8125 GHz	В рамките на ERC 70-03. Носещите честоти може да бъдат избрани от изпълнителя на крайпътната система и не е нужно те да са известни в DSRC-VU (в съответствие с EN 12253 и EN 13372)
D1a (*)	Допустимо отклонение на носещите честоти	до 5 ppm	(в съответствие с EN 12253)
D2 (*)	Спектрална маска на радиопредавателя на крайпътното устройство (RSU, т.е. на REDCR)	В рамките на ERC 70-03. REDCR трябва да е в съответствие с клас B,C съгласно EN 12253. Няма други специфични изисквания в рамките на настоящото приложение	Параметри, използвани за контролиране на смущенията между близки разпитващи устройства (както е определено в EN 12253 и EN 13372).
D3	Минимален честотен обхват на бордовото устройство (DSRC-VU)	5,795—5,815 GHz	(в съответствие с EN 12253)
D4 (*)	Максимална еквивалентна изотропно излъчена мощност (E.I.R.P.)	В рамките на ERC 70-03 (нелицензирано) и на националното законодателство Максимум + 33 dBm	(в съответствие с EN 12253)
D4a	Ъглова маска за E.I.R.P.	Съгласно обявената и публикувана спецификация на проектанта на разпитващото устройство	(в съответствие с EN 12253)
D5	Поляризация	Ляво въртяща се кръгова поляризация	(в съответствие с EN 12253)
D5a	Напречна поляризация	XPD: В диаграмата на насоченост: (REDCR) RSU t ≥ 15 δB (DSRC-VU) OBU r ≥ 10 δB В зоната − 3 dB: (REDCR) RSU t ≥ 10 δB (DSRC-VU) OBU r ≥ 6 δB	(в съответствие с EN 12253)
D6 (*)	Модулация	Амплитудна модулация на две нива.	(в съответствие с EN 12253)
D6a (*)	Индекс на модулация	0,5 … 0,9	(в съответствие с EN 12253)

Позиция №	Параметър	Стойност(и)	Забележка
D6b	Диаграма Eye Pattern	≥ 90 % (време) / ≥ 85 % (амплитуда)	
D7 (*)	Кодиране на данните	FM0 Бит „1“ има преходи само в началото и края на интервала на бита. Бит „0“ има допълнителен преход в средата на интервала на бита в сравнение с бита „1“.	(в съответствие с EN 12253)
D8 (*)	Скорост на предаване на данните	500 kBit/s	(в съответствие с EN 12253)
D8a	Допустимо отклонение на такта за бит (Bit Clock)	по-малко от ± 100 ppm	(в съответствие с EN 12253)
D9 (*)	Честота на грешните битове (B.E.R.) при връзката	≤ 10^{-6} когато падащата мощност върху бордовото устройство (OBU, т.е. DSRC-VU) е в диапазона, посочен в [D11a до D11b].	(в съответствие с EN 12253)
D10	Тригер за „събуждане“ на OBU (DSRC-VU)	OBU (DSRC-VU) се събужда при получаване на какъвто и да е фрейм с 11 или повече октета (включително преамбюл)	Не е необходим специален модел за събуждане. DSRC-VU може да се събуди при получаването на фрейм с по-малко от 11 октета. (в съответствие с EN 12253)
D10a	Максимално стартово време	≤ 5 ms	(в съответствие с EN 12253)
D11	Съобщителна зона	Пространствената област, в рамките на която е постигната B.E.R. съгласно D9a	(в съответствие с EN 12253)
D11a (*)	Гранична стойност на мощността за връзката (горна).	– 24dBm	(в съответствие с EN 12253)
D11b (*)	Гранична стойност на мощността за връзката (долна).	Падаща мощност: – 43 dBm (диаграма на насоченост) – 41 dBm (в границите от – 45° до + 45° в съответствие с равнината, успоредна на повърхността на пътя, когато DSRC-VU по-късно е монтирано в превозното средство (Azimuth)	(в съответствие с EN 12253) Разширено изискване за хоризонтални ъгли до ±45° поради случаите на употреба, определени в настоящото приложение.
D12 (*)	Гранично ниво на мощността (на DSRC-VU)	– 60 dBm	(в съответствие с EN 12253)
D13	Преамбюл	Преамбюлът е задължителен.	(в съответствие с EN 12253)
D13a	Дължина и модел на преамбюла	16 бита ± 1 бит, кодирани по FM0 битове „1“	(в съответствие с EN 12253)

Позиция №	Параметър	Стойност(и)	Забележка
D13b	Форма на вълната на преамбюла	Редуваща се поредица от ниско ниво и високо ниво с времетраене на импулса 2 μs. Допустимото отклонение се дава от D8a	(в съответствие с EN 12253)
D13c	Изоставащи (trailing) битове	На крайпътното устройство (т.е. REDCR) е разрешено да предаде максимум 8 бита след флага за край. Не се изисква бордовото устройство (DSRC-VU) да отчита тези допълнителни битове.	(в съответствие с EN 12253)

(*) Параметрите на предаването на данни в права посока подлежат на изпитване за съответствие съгласно относимото изпитване на параметри по EN 300 674-1

Таблица 14.2.

Параметри на предаването на данни в обратна посока

Позиция №	Параметър	Стойност(и)	Забележка
U1 (*)	Подносещи честоти	OBU (DSRC-VU) трябва да поддържа 1,5 MHz и 2,0 MHz RSU (REDCR) трябва да поддържа 1,5 MHz или 2,0 MHz, или и двете честоти U1-0: 1,5 MHz U1-1: 2,0 MHz	Изборът на подносещата честота (1,5 MHz или 2,0 MHz) зависи от избрания профил по EN 13372.
U1a (*)	Допустимо отклонение на подносещите честоти	в рамките на ± 0,1 %	(в съответствие с EN 12253)
U1b	Използване на странични ленти	Едни и същи данни за двете страни	(в съответствие с EN 12253)
U2 (*)	Спектрална маска на радиопредавателя на бордовото устройство (OBU, т.е. на DSRC-VU)	В съответствие с EN 12253 1) Мощност извън лентата: виж ETSI EN 300674-1 2) Мощност в лентата: [U4a] dBm в 500 kHz 3) Емисия в който и да е друг канал в обратна посока: U2(3)-1 = – 35 dBm в 500 kHz	(в съответствие с EN 12253)
U4a (*)	Максимална E.I.R.P. за единична странична лента (диаграма на насоченост)	Две възможности: U4a-0: – 14 dBm U4a-1: – 21 dBm	Съгласно обявената и публикувана спецификация на проектанта на оборудването
U4b (*)	Максимална E.I.R.P. за единична странична лента (35°)	Две възможности — неприложимо — – 17 dBm	Съгласно обявената и публикувана спецификация на проектанта на оборудването
U5	Поляризация	Ляво въртяща се кръгова поляризация	(в съответствие с EN 12253)

Позиция №	Параметър	Стойност(и)	Забележка
U5a	Напречна поляризация	XPD: В диаграмата на насоченост: (REDCR) RSU r ≥ 15 dB (DSRC-VU) OBU t ≥ 10 dB При -3 dB: (REDCR) RSU r ≥ 10 dB (DSRC-VU) OBU t ≥ 6 dB	(в съответствие с EN 12253)
U6	Модулация на подносещата	2-PSK Кодирани данни, синхронизирани с подносещата: преходите на кодираните данни съвпадат с преходите на подносещата.	(в съответствие с EN 12253)
U6b	Коефициент на запълване	Коефициент на запълване: 50 % ± α, α ≤ 5 %	(в съответствие с EN 12253)
U6c	Модулация на носещата	Мултиплексиране на модулираната подносеща с носещата.	(в съответствие с EN 12253)
U7 (*)	Кодиране на данните	NRZI (без преход към началото на бит „1“, преход в началото на бит „0“, без преход в рамките на бита)	(в съответствие с EN 12253)
U8 (*)	Скорост на предаване на данните	250 kbit/s	(в съответствие с EN 12253)
U8a	Допустимо отклонение на такта за бит (Bit Clock)	в рамките на ± 1 000 ppm	(в съответствие с EN 12253)
U9	Честота на грешните битове (B.E.R.) за връзката	≤ 10^{-6}	(в съответствие с EN 12253)
U11	Съобщителна зона	Пространствената област, в рамките на която DSRC-VU е разположено така, че предадените данни са получени от REDCR с по-малка B.E.R. от посочената в U9a.	(в съответствие с EN 12253)
U12a (*)	Усилване при преобразуването (долна граница)	1 dB за всяка странична лента Ъглов диапазон: кръгово симетричен между диаграмата на насоченост и ± 35° и	
		в границите от – 45° до + 45° в съответствие с равнината, успоредна на повърхността на пътя, когато DSRC-VU по-късно е монтирано в превозното средство (Azimuth)	По-голямо от специфицирания диапазон на стойности за хоризонтални ъгли до ± 45° поради случаите на употреба, определени в настоящото приложение.
U12b (*)	Усилване при преобразуването (горна граница)	10 dB за всяка странична лента	По-малко от специфицирания диапазон на стойностите за всяка странична лента в кръгъл конусовиден около диаграмата на насоченост на ± 45° ъгъл на отваряне
U13	Преамбюл	Преамбюлът е задължителен.	(в съответствие с EN 12253)

Позиция №	Параметър	Стойност(и)	Забележка
U13a	Преамбюл Дължина и модел	32 to 36 μs модулиран само с подносещата, после 8 бита „0“, кодирани по NRZI.	(в съответствие с EN 12253)
U13b	Изоставащи (trailing) битове	На DSRC-VU е разрешено да предаде максимум 8 бита след флага за край. Не се изисква RSU (REDCR) да отчита тези допълнителни битове.	(в съответствие с EN 12253)

(*) Параметрите на предаването на данни в обратна посока подлежат на изпитване за съответствие съгласно относимото изпитване на параметри по EN 300 674-1.

5.3.3 *Конструкция на антената*

5.3.3.1 Антена на четеца (REDCR)

DSC_30 Конструкцията на антената на *REDCR* зависи от производителя при спазване на ограниченията, определени в 5.3.2, и оптимизация на характеристиките на *DSRC-REDCR* за четене на данни съобразно специфичното предназначение и условията за четене, за които е проектиран *REDCR*.

5.3.3.2 Антена на бордовото устройство (VU)

DSC_31 Конструкцията на антената на *DSRC-VU* зависи от производителя при спазване на ограниченията, определени в 5.3.2, и оптимизация на характеристиките на *DSRC-REDCR* за четене на данни съобразно специфичното предназначение и условията за четене, за които е проектиран *REDCR*.

DSC_32 Антената на VU се закрепва върху предното стъкло на превозното средство, както е определено в 5.1 по-горе.

DSC_33 При изпитването в сервиз (виж раздел 6.3) антената на DSRC-VU, закрепена съгласно 5.1 по-горе, трябва успешно да осъществява стандартна изпитателна връзка и транзакция за RTM, както е определено в настоящото допълнение, на разстояние между 2 и 10 метра през повече от 99 % от времето — осреднено за 1 000 разпитвания за данни.

5.4 **Изисквания по протокола DSRC за RTM**

5.4.1 *Преглед*

DSC_34 Протоколът за транзакцията по изтегляне на *данните* по интерфейса за DSRC на 5,8 GHz трябва да бъде съгласно следните стъпки. В настоящия раздел се описва протичането на транзакцията при идеални условия без повторни предавания на данни или прекъсвания на връзката.

ЗАБЕЛЕЖКА Целта на етапа на инициализиране (стъпка № 1) е да се установи връзката между *REDCR* и DSRC-VU, които са навлезли в зоната на транзакцията за DSRC на 5,8 GHz (главен/подчинен), но все още не са установили връзката между *REDCR*, и да се уведомят приложните процеси.

— **Стъпка № 1.** Инициализиране. Четецът *REDCR* изпраща фрейм, съдържащ таблица за навигационните услуги (Beacon Service Table — BST), която включва идентификаторите на приложения (AID) в списъка на услугите, поддържани от него. В приложението RTM това ще бъде услугата със стойност на AID = 2 (Freight&Fleet). *DSRC-VU* оценява получената BST и отговаря (виж по-долу) със списъка на поддържаните приложения в домейна Freight&Fleet, или не отговаря въобще, ако не се поддържа никое от тези приложения. Ако *REDCR* не предлага AID=2, DSRC-VU не отговаря на REDCR.

— **Стъпка № 2.** *DSRC-VU* изпраща фрейм, съдържащ заявка за разпределяне на частен прозорец (private window allocation).

— **Стъпка № 3.** *REDCR* изпраща фрейм, съдържащ разпределение на частен прозорец.

— **Стъпка № 4.** *DSRC-VU* използва разпределения частен прозорец, за да изпрати фрейм, съдържащ неговата таблица за услуги във връзка с превозното средство (Vehicle Service Table — VST). Тази VST включва списък на всички инстанциирания на различните услуги, поддържани от това *DSRC-VU* в рамките на AID=2. Различните инстанциирания се идентифицират посредством уникални идентификатори на елементи (Element Identifiers — EIDs), всеки от които е свързан със стойност на параметъра Application Context Mark, указваща приложението и стандарта, които се поддържат.

— **Стъпка № 5.** След това четецът *REDCR* анализира предложената VST и или прекъсва връзката (RELEASE) поради липса на интерес към каквото и да било, предложено от VST (т.е. той получава VST от *DSRC-VU*, което не поддържа транзакцията за RTM), или започва инстанциирането на приложение, ако получи подходяща VST.

— **Стъпка № 6.** За целта REDCR изпраща фрейм, съдържащ команда за извличане на данните за RTM, като идентифицира инстанциирането на приложението за RTM чрез указване на съответния идентификатор (посочен от DSRC-VU във VST), и разпределя частен прозорец.

— **Стъпка № 7.** *DSRC-VU* използва новоразпределения частен прозорец, за да изпрати фрейм, който съдържа адресирания идентификатор, съответстващ на инстанциирането на приложението за RTM съгласно VST, следван от атрибута *RtmData* (елемент на полезните данни + елемент на данните, свързани със сигурността).

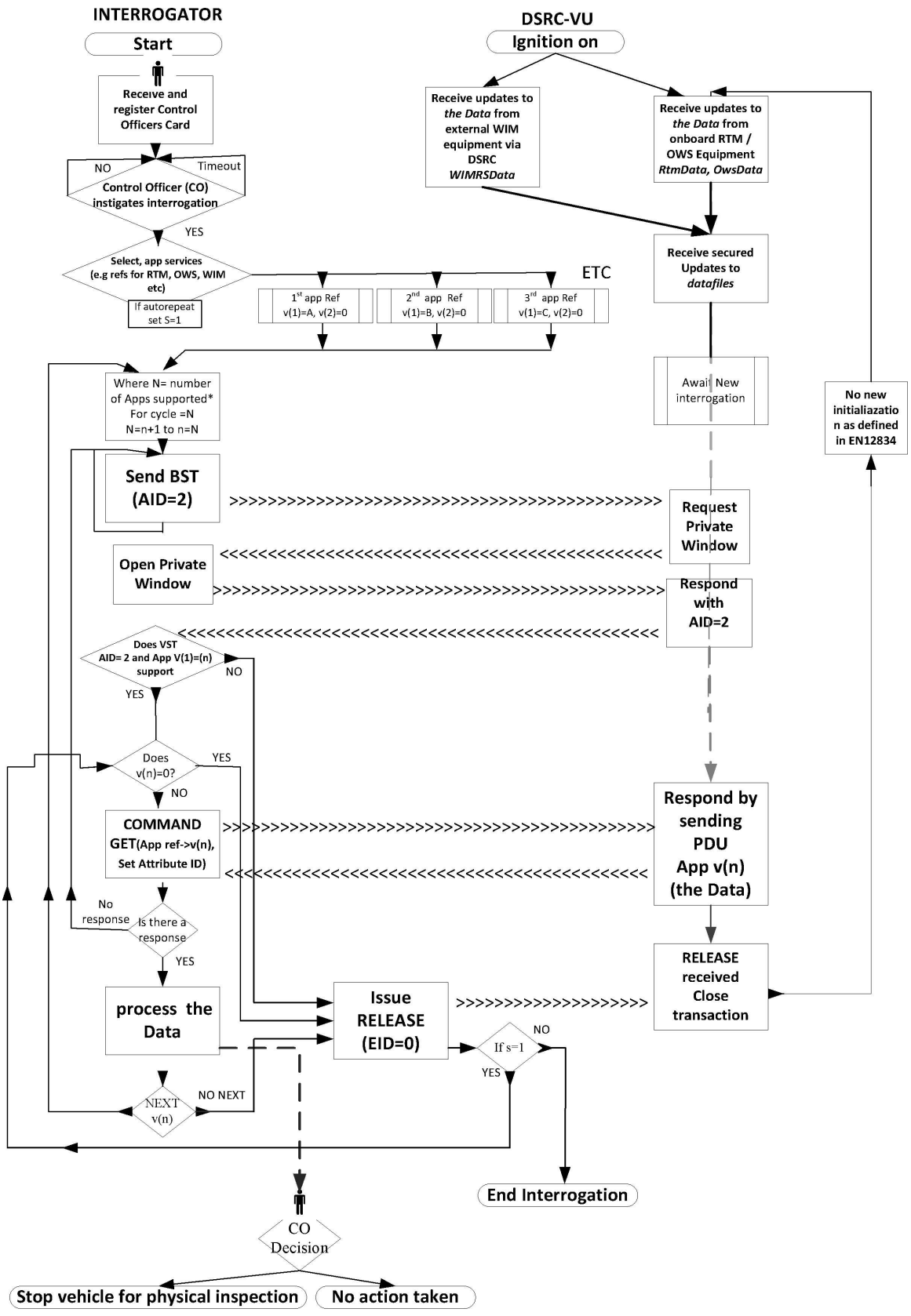
— **Стъпка № 8.** Ако са заявени няколко услуги, стойността „n“ се променя на референтния номер на следващата услуга и процесът се повтаря.

— **Стъпка № 9.** *REDCR* потвърждава приемането на данните, като изпраща на *DSRC-VU* фрейм, съдържащ командата RELEASE, за да приключи сесията, ИЛИ се връща на стъпка № 6, ако не е успял да валидира успешното приемане на LDPU.

Виж фигура 14.6 за схематично описание на протокола за транзакцията.

Фигура 14.6

Последователност на процеса на RTM по DSRC на 5,8 GHz



5.4.2 *Команди*

DSC_35 На етапа на транзакцията за RTM се използват само функциите, осъществявани от следните команди:

— **INITIALISATION.request**: Излъчвана от REDCR команда с определение за приложенията, поддържани от REDCR.

— **INITIALISATION.response**: Отговор от DSRC-VU, потвърждаващ връзката и съдържащ списък на инстанции на поддържаните приложения с характеристики и информация за начина на обръщане към тях (EID).

— **GET.request**: Команда, издадена от *REDCR* на *DSRC-VU*, указваща инстанциирането на приложението, към което трябва да се обърне посредством определен EID, получен във VST, с която *DSRC-VU* се инструктира да изпрати избрания(те) атрибут(и) с *данните*. Целта на командата GET е *REDCR* да получи *данните* от *DSRC-VU*.

— **GET.response**: Отговор от *DSRC-VU*, който съдържа заявените *данни*.

— **ACTION.request ECHO**: Команда към *DSRC-VU* да изпрати обратно данни от *DSRC-VU* на *REDCR*. Целта на командата ECHO е да даде възможност на сервизи или изпитателни пунктове за одобрение на типа да проверят дали DSRC функционира, без да е нужен достъп до сертификати за сигурност.

— **ACTION**.response ECHO: Отговор от DSRC-VU на командата ECHO.

— **EVENT_REPORT.request** RELEASE: Команда към *DSRC-VU*, че транзакцията е приключила. Целта на командата RELEASE е да приключи сесията с *DSRC-VU*. При получаване на RELEASE *DSRC-VU* не отговаря повече на по-нататъшни разпитвания по текущата връзка. Следва да се отбележи, че съгласно EN 12834 едно *DSRC-VU* не се свързва два пъти с едно и също разпитващо устройство, освен ако е било извън съобщителната зона в продължение на 255 секунди или ако е променен навигационният идентификационен номер (Beacon ID) на разпитващото устройство.

5.4.3 *Последователност на командите за разпитване*

DSC_36 По отношение на последователността от команди и отговори транзакцията се описва, както следва:

Пореден номер	Предавател		Приемник	Описание	Действие
1	REDCR	>	DSRC-VU	Инициализиране на връзката — заявка	REDCR излъчва BST
2	*DSRC-VU*	>	*REDCR*	*Инициализиране на връзката — отговор*	*Ако BST поддържа AID=2,тогава DSRC-VU заявява частен прозорец*
3	REDCR	>	DSRC-VU	Предоставя частен прозорец	Изпраща фрейм, съдържащ разпределение за частен прозорец
4	*DSRC-VU*	>	*REDCR*	*Изпраща VST*	*Изпраща фрейм, включващ VST*
5	REDCR	>	DSRC-VU	Изпраща GET.request за данни в Attribute за конкретен EID	
6	*DSRC-VU*	>	*REDCR*	*Изпраща GET.response със заявения Attribute за конкретен EID*	*Изпраща Attribute (RTMData, OWSData…) с данни за конкретен EID*

Пореден номер	Предавател		Приемник	Описание	Действие
7	REDCR	>	DSRC-VU	Изпраща GET.request за данни, различни от Attribute (ако е уместно)	
8	*DSRC-VU*	>	*REDCR*	*Изпраща GET.response със заявения Attribute*	*Изпраща Attribute с данни за конкретен EID*
9	REDCR	>	DSRC-VU	Потвърждава успешното приемане на данните	Изпраща команда RELEASE за приключване на транзакцията
10	*DSRC-VU*			*Приключва транзакцията*	

Пример за последователността на транзакцията и съдържанието на разменяните фреймове се дава в раздели 5.4.7 и 5.4.8.

5.4.4 *Структура на данните*

DSC_37 Семантичната структура на *данните*, когато преминават през интерфейса за DSRC на 5,8 GHz, трябва да е в съответствие с описаната в настоящото допълнение. Начинът на структуриране на тези данни е определен в настоящия раздел.

DSC_38 Полезните данни (RTM data) се състоят от конкатенацията на:

1. данните EncryptedTachographPayload, които представляват криптираните данни Tachograph-Payload, определени в ASN.1 в раздел 5.4.5. Методът на криптиране е описан в допълнение 11;
2. данните DSRCSecurityData, определени в допълнение 11.

DSC_39 Данните за RTM (RTM Data) се адресират като RTM Attribute=1 и се прехвърлят в RTM контейнер =10.

DSC_40 RTM Context Mark идентифицира поддържаната част от стандарта в серията TARV от стандарти (RTM съответства на част 9)

Модулът ASN.1 за DSRC данните в рамките на приложението RTM е определен, както следва:

```
   TarvRtm {iso(1) standard(0) 15638 part9(9) version1(1)}
   DEFINITIONS AUTOMATIC TAGS
   ::= BEGIN
   IMPORTS
   -- Imports data attributes and elements from EFC which are used for RTM
   LPN
   FROM EfcDsrcApplication {iso(1) standard(0) 14906 application(0) version5(5)}

   -- Imports function parameters from the EFC Application Interface Definition
   SetMMIRq
   FROM EfcDsrcApplication {iso(1) standard(0) 14906 application(0) version5(5)}

   -- Imports the L7 DSRCData module data from the EFC Application Interface Definition
   Action-Request, Action-Response, ActionType, ApplicationList, AttributeIdList, AttributeList,
   Attributes,
   BeaconID, BST, Dsrc-EID, DSRCApplicationEntityID, Event-Report-Request, Event-Report- Response,
   EventType, Get-Request, Get-Response, Initialisation-Request, Initialisation-Response,
   ObeConfiguration, Profile, ReturnStatus, Time, T-APDUs, VST
   FROM EfcDsrcGeneric {iso(1) standard(0) 14906 generic(1) version5(5)};


   -- Definitions of the RTM functions:
   RTM-InitialiseComm-Request ::= BST
   RTM-InitialiseComm-Response::= VST
   RTM-DataRetrieval-Request::= Get-Request (WITH COMPONENTS {fill (SIZE(1)), eid, accessCredentials ABSENT,iid
   ABSENT,  attrIdList})
   RTM-DataRetrieval-Response::= Get-Response {RtmContainer} (WITH COMPONENTS {..., eid, iid ABSENT})
   RTM-TerminateComm::= Event-Report-Request {RtmContainer}(WITH COMPONENTS {mode (FALSE), eid (0),
   eventType (0)})

   RTM-TestComm-Request::= Action-Request {RtmContainer} (WITH COMPONENTS {..., eid (0), actionType
   (15), accessCredentials ABSENT, iid ABSENT})

   RTM-TestComm-Response::= Action-Response {RtmContainer} (WITH COMPONENTS {..., fill (SIZE(1)), eid
   (0), iid ABSENT})

   -- Definitions of the RTM attributes:
   RtmData ::= SEQUENCE {
        encryptedTachographPayload OCTET STRING (SIZE(67)) (CONSTRAINED BY { -- calculated encrypting
   TachographPayload as per Appendix 11 --}),
        DSRCSecurityData OCTET STRING
        }
   TachographPayload ::= SEQUENCE {
             tp15638VehicleRegistrationPlate LPN -- Vehicle Registration Plate as per EN 15509.
             tp15638SpeedingEvent            BOOLEAN,  -- 1= Irregularities in speed (see Annex 1C)
             tp15638DrivingWithoutValidCard  BOOLEAN,     -- 1= Invalid card usage (see Annex 1C)
             tp15638DriverCard               BOOLEAN,-- 0= Indicates a valid driver card  (see Annex 1C)
             tp15638CardInsertion            BOOLEAN, -- 1= Card insertion while driving (see Annex 1C)
             tp15638MotionDataError          BOOLEAN, -- 1= Motion data error (see Annex 1C)
             tp15638VehicleMotionConflict    BOOLEAN, -- 1= Motion conflict (see Annex 1C)
             tp156382ndDriverCard            BOOLEAN, -- 1= Second driver card inserted (see Annex 1C)
             tp15638CurrentActivityDriving   BOOLEAN, -- 1= other activity selected;
                                                       -- 0= driving selected
             tp15638LastSessionClosed        BOOLEAN, -- 1= improperly, 0= properly, closed
             tp15638PowerSupplyInterruption  INTEGER (0..127), -- Supply interrupts in the last 10 days
             tp15638SensorFault              INTEGER (0..255),-- eventFaultType as per data dictionary
   -- All subsequent time related types as defined in Annex 1C.
             tp15638TimeAdjustment           INTEGER(0..4294967295), -- Time of the last time adjustment
             tp15638LatestBreachAttempt      INTEGER(0..4294967295), -- Time of last breach attempt
             tp15638LastCalibrationData      INTEGER(0..4294967295), -- Time of last calibration data
             tp15638PrevCalibrationData      INTEGER(0..4294967295), -- Time of previous calibration data
             tp15638DateTachoConnected       INTEGER(0..4294967295), -- Date tachograph connected
             tp15638CurrentSpeed             INTEGER (0..255), -- Last current recorded speed
             tp15638Timestamp                INTEGER(0..4294967295) -- Timestamp of current record[2]
             }
Rtm-ContextMark ::= SEQUENCE {
  standardIdentifier    StandardIdentifier, -- identifier of the TARV part and its version

  RtmCommProfile          INTEGER {
                                C1 (1),
                                C2 (2)
                                } (0..255) DEFAULT 1
  }
RtmTransferAck ::= INTEGER {
                  Ok (1),
                  NoK (2)
                  } SIZE (1..255)
```

```
StandardIdentifier ::= OBJECT IDENTIFIER
RtmContainer ::= CHOICE {
        integer                         [0]    INTEGER,
        bitstring                       [1]    BIT STRING,
        octetstring                     [2]    OCTET STRING (SIZE (0..127, ...)),
        universalString                 [3]    UniversalString,
        beaconId                        [4]    BeaconID,
        t-apdu                          [5]    T-APDUs,
        dsrcApplicationEntityId         [6]    DSRCApplicationEntityID,
        dsrc-Ase-Id                     [7]    Dsrc-EID,
        attrIdList                      [8]    AttributeIdList,
        attrList                        [9]    AttributeList{RtmContainer},
        rtmData                         [10]   RtmData,
        rtmContextmark                  [11]   Rtm-ContextMark,
        reserved12                      [12]   NULL,
        reserved13                     [13]   NULL,
        reserved14                      [14]   NULL,
        time                            [15]   Time,
-- values from 16 to 255 reserved for ISO/CEN usage
        }}

END
```

5.4.5 *Елементи на RtmData, извършени действия и определения*

DSC_41 Стойностите на данните, които трябва да бъдат изчислени от бордовото устройство (VU) и използвани за актуализиране на защитените данни в DSRC-VU, се изчисляват съгласно правилата, определени в таблица 14.3:

Таблица 14.3.

Елементи на RtmData, извършени действия и определения

(1) Елемент на RTM Data	(2) Действие, извършено от VU		(3) ASN.1 определение на данните
RTM1 **Регистрация на превозното средство Регистрационен номер**	VU задава стойността на елемента *tp15638VehicleRegistrationPlate* на данните RTM1 от регистрираната стойност на данните тип *VehicleRegistrationIdentification* както е определено в допълнение 1 *VehicleRegistrationIdentification*	Регистрационен номер на превозното средство, изразен като низ от символи	`tp15638VehicleRegstrationPlate LPN, --Регистрация на превозното средство Регистрационен номер, импортиран от ISO 14906 с ограничението, определено в EN 15509, т.е. ПОСЛЕДОВАТЕЛНОСТ, съдържаща код на държавата, следван от буквен показател и после от самия регистрационен номер, който винаги е 14 октета (допълнени с нули), така че дължината за типа LPN по EN 15509 винаги е 17 октета, от които 14 са „същинският" регистрационен номер.`

(1) Елемент на RTM Data	(2) Действие, извършено от VU		(3) ASN.1 определение на данните
RTM2 **Превишаване на допустимата скорост**	VU генерира булева стойност на елемента RTM2 на данните tp15638SpeedingEvent. Стойността на tp15638SpeedingEvent се изчислява от VU от броя на събитията Over Speeding Events, регистрирани във VU през последните 10 дни на възникването им, както е определено в приложение 1B. Ако има поне едно събитие tp15638SpeedingEvent през последните 10 дни на възникване, за стойността на tp15638SpeedingEvent се задава TRUE, т.е. „ВЯРНО“. В ПРОТИВЕН СЛУЧАЙ, ако не е имало такива събития през последните 10 дни на възникване, за стойността на tp15638SpeedingEvent се задава FALSE, т.е. „НЕВЯРНО“.	1 (TRUE) — указва нередности по отношение на скоростта през последните 10 дни на възникване	`tp15638speedingEvent BOOLEAN,`
RTM3 **Управление на МПС без валидна карта**	VU генерира булева стойност на елемента RTM3 на данните tp15638DrivingWithoutValidCard. VU присвоява стойност TRUE на променливата tp15638DrivingWithoutValidCard, ако през последните 10 дни на възникване VU е регистрирало поне едно събитие от типа „Управление на МПС без съответна карта“ съгласно определението в приложение 1B. В ПРОТИВЕН СЛУЧАЙ, ако не е имало такива събития през последните 10 дни на възникване, за стойността на tp15638DrivingWithoutValidCard се задава FALSE.	1 (TRUE) = указва използване на невалидна карта	`tp15638DrivingWithoutValidCard` `BOOLEAN,`
RTM4 **Валидна карта на водач**	VU генерира булева стойност на елемента RTM4 на данните tp15638DriverCard въз основа на данните, съхранени във VU и определени в допълнение 1. Ако не е налице валидна карта на водач, VU задава за променливата стойност TRUE. В ПРОТИВЕН СЛУЧАЙ, ако е налице валидна карта на водач, VU задава за променливата стойност FALSE.	0 (FALSE) = указва валидна карта на водач	`tp15638DriverCard BOOLEAN,`
RTM5 **Вкарване на карта по време на управлението на МПС**	VU генерира булева стойност на елемента RTM5 на данните. VU присвоява стойност TRUE на променливата tp15638CardInsertion, ако през последните 10 дни на възникване VU е регистрирало поне едно събитие от типа „Вкарване на карта по време на управлението на МПС“ съгласно определението в приложение 1B. В ПРОТИВЕН СЛУЧАЙ, ако не е имало такива събития през последните 10 дни на възникване, за стойността на tp15638CardInsertion се задава FALSE.	1 (TRUE) = указва вкарване на карта по време на управлението на МПС през последните 10 дни на възникване на това събитие	`tp15638CardInsertion BOOLEAN,`
RTM6 **Грешка в данните за движението**	VU генерира булева стойност на елемента RTM6 на данните. VU присвоява стойност TRUE на променливата tp15638MotionDataError, ако през последните 10 дни на възникване VU е регистрирало поне едно събитие от типа „Грешка в данните за движението“ съгласно определението в приложение 1B. В ПРОТИВЕН СЛУЧАЙ, ако не е имало такива събития през последните 10 дни на възникване, за стойността на tp15638MotionDataError се задава FALSE.	1 (TRUE) = указва грешка в данните за движението през последните 10 дни на възникване	`tp15638motionDataError BOOLEAN,`

(1) Елемент на RTM Data	(2) Действие, извършено от VU		(3) ASN.1 определение на данните
RTM7 **Противоречие в данните за движението на превозното средство**	VU генерира булева стойност на елемента RTM7 на данните. VU присвоява стойност TRUE на променливата tp15638vehicleMotionConflict, ако VU през последните 10 дни VU е регистрирало поне едно събитие от типа „противоречие в данните за движението на превозното средство“ съгласно определението в приложение 1B (стойност ‘0A’H). В ПРОТИВЕН СЛУЧАЙ, ако не е имало такива събития през последните 10 дни на възникване, за стойността на tp15638vehicleMotionConflict се задава FALSE.	1 (TRUE) = указва противоречие в данните за движението през последните 10 дни на възникване	`tp15638vehicleMotionConflict` `BOOLEAN,`
RTM8 **Карта на втория водач**	VU генерира булева стойност на елемента RTM8 на данните въз основа на приложение 1B („Данни за дейността на водача“ ЕКИП и ВТОРИ ВОДАЧ). Ако е налице валидна карта на втория водач, VU задава за променливата стойност TRUE. В ПРОТИВЕН СЛУЧАЙ, ако не е налице валидна карта на втория водач, VU задава за променливата стойност FALSE.	1 (FALSE) = указва, че е вкарана карта на втория водач	`tp156382ndDriverCard BOOLEAN,`
RTM9 **Текуща дейност**	VU генерира булева стойност на елемента RTM9 на данните. Ако текущата дейност е записана във VU като дейност, различна от „УПРАВЛЕНИЕ НА МПС“ (DRIVING) съгласно определението в приложение 1B, VU задава за променливата стойност TRUE В ПРОТИВЕН СЛУЧАЙ, ако текущата дейност е записана във VU като „Управление на МПС“, VU задава за променливата стойност FALSE	1 (TRUE) = друга дейност е избрана 0 (FALSE) = избрано е управление на МПС	`tp15638currentActivityDriving` `BOOLEAN`
RTM10 **Последната сесия е приключена**	VU генерира булева стойност на елемента RTM10 на данните. Ако последната картова сесия не е приключена правилно съгласно определението в приложение 1B, VU задава за променливата стойност TRUE. В ПРОТИВЕН СЛУЧАЙ, ако последната картова сесия е приключена правилно, VU задава за променливата стойност FALSE.	1 (TRUE) = приключена неправилно 0 (FALSE) = приключена правилно	`tp15638lastSessionClosed` `BOOLEAN`
RTM11 **Прекъсване на електрическото захранване**	VU генерира цяло число като стойност на елемента RTM11 на данните. VU присвоява на променливата tp15638PowerSupplyInterruption стойност, която е равна на най-дългото прекъсване на електрическото захранване, съгласно член 9 от Регламент (ЕС) № 165/2014 от типа „Прекъсване на електрическото захранване“, както е определено в приложение 1B. В ПРОТИВЕН СЛУЧАЙ, ако през последните 10 дни на възникване на събитието „Прекъсване на електрическото захранване“ не е имало такова, за стойността на това цяло число се задава 0.	— Брой на прекъсванията на електрическото захранване през последните 10 дни на възникване	`tp15638powerSupplyInterruption` `INTEGER (0..127),`

(1) Елемент на RTM Data	(2) Действие, извършено от VU		(3) ASN.1 определение на данните
RTM12 **Неизправност на датчика**	VU генерира целочислена стойност за елемента RTM12 на данните. VU присвоява на променливата sensorFault стойността: — 1 ако за датчика събитие от типа ‘35’H за неизправност е било записано през последните 10 дни, — 2 ако за приемника за GNSS събитие за неизправност (вътрешно или външно с изброени (enum) стойности ‘51’H или ‘52’H) е било записано през последните 10 дни, — 3 ако събитие от типа ‘53’H за външна неизправност във връзката с GNSS е било записано през последните 10 дни на възникване, — 4 ако през последните 10 дни на възникване са били регистрирани неизправности както по датчика, така и по приемника за GNSS, — 5 ако през последните 10 дни на възникване са били регистрирани неизправности както по датчика, така и външна неизправност във връзката с GNSS, — 6 ако през последните 10 дни на възникване са били регистрирани неизправности както по приемника за GNSS, така и външна неизправност във връзката с GNSS, — 7 ако през последните 10 дни на възникване са били регистрирани всички три вида неизправности по датчика и GNSS. В ПРОТИВЕН СЛУЧАЙ се присвоява стойност 0, ако през последните 10 дни на възникване не са били регистрирани събития.	— за неизправност на датчика — един байт съгласно речника на данните	`tp15638SensorFault INTEGER (0..255),`
RTM13 **Сверяване на часовника**	VU генерира целочислена стойност (timeReal от допълнение 1) за елемента RTM13 на данните въз основа на наличните данни за сверяването на часовника (Time Adjustment) съгласно определението в приложение 1B. VU присвоява като стойност момента, в който е станало последното събитие „Сверяване на часовника“. В ПРОТИВЕН СЛУЧАЙ, ако в данните във VU липсва събитие „Сверяване на часовника“ съгласно определението в приложение 1B, VU задава стойност 0.	Момент на последното сверяване на часовника	`tp15638TimeAdjustment INTEGER(0..4294967295),`
RTM14 **Опит за нарушаване на сигурността**	VU генерира целочислена стойност (timeReal от допълнение 1) за елемента RTM14 на данните въз основа на наличието на събитие „Опит за нарушаване на сигурността“ съгласно определението в приложение 1B. VU присвоява като стойност момента, в който е възникнало последното събитие „Опит за нарушаване на сигурността“, регистрирано от VU. В ПРОТИВЕН СЛУЧАЙ, ако в данните във VU липсва събитие „Опит за нарушаване на сигурността“ съгласно определението в приложение 1B, VU задава стойност 0x00FF.	Момент на последния опит за нарушаване на сигурността — Стойност по подразбиране =0x00FF	`tp15638LatestBreachAttempt INTEGER(0..4294967295),`
RTM15 **Последно калибриране**	VU генерира целочислена стойност (timeReal от допълнение 1) за елемента RTM15 на данните въз основа на наличните данни за последното калибриране (Last Calibration) съгласно определението в приложение 1B. VU присвоява като стойност момента на последните две калибрирания (RTM15 и RTM16), които са зададени във VuCalibrationData съгласно определението в допълнение 1. VU присвоява като стойност на RTM15 timeReal в записа за последното калибриране.	Данни за момента на последното калибриране	`tp15638LastCalibrationData INTEGER(0..4294967295),`

(1) Елемент на RTM Data	(2) Действие, извършено от VU		(3) ASN.1 определение на данните
RTM16 **Предишно калибриране**	VU генерира целочислена стойност (timeReal от допълнение 1) за елемента RTM16 на данните в записа за калибрирането, предхождащо последното калибриране. В ПРОТИВЕН СЛУЧАЙ, ако не е имало предишно калибриране, VU задава за RTM16 стойност 0.	Данни за момента на предишното калибриране	`tp15638PrevCalibrationData` `INTEGER(0..4294967295),`
RTM17 **Дата на свързване на тахографа**	За елемента RTM17 на данните VU генерира целочислена стойност (timeReal от допълнение 1). VU присвоява като стойност момента на първоначалното монтиране на VU. VU извлича тези данни от VuCalibrationData (допълнение 1) на vuCalibrationRecords, като CalibrationPurpose е равно на: ‘03’H	Дата на свързване на тахографа	`tp15638DateTachoConnected` `INTEGER(0..4294967295),`
RTM18 **Моментна скорост**	VU генерира цяло число като стойност на елемента RTM18 на данните. VU присвоява като стойност на RTM18 последната записана моментна скорост при последното актуализиране на RtmData.	Последна записана моментна скорост	`tp15638CurrentSpeed` `INTEGER (0..255),`
RTM19 **Времеви печат**	За елемента RTM17 на данните VU генерира целочислена стойност (timeReal от допълнение 1). VU присвоява като стойност на RTM19 момента на последното актуализиране на RtmData.	Времеви печат на текущия запис TachographPayload	`tp15638Timestamp` `INTEGER(0..4294967295),`

5.4.6 *Механизъм за прехвърляне на данни*

DSC_42 Полезните данни, определени преди, се заявяват от четеца (REDCR) след етапа на инициализиране и впоследствие се предават от *DSRC-VU* в разпределения прозорец. REDCR използва командата GET, за да извлече данните.

DSC_43 При всеки обмен на данни по DSRC те трябва да бъдат кодирани съгласно PER (Packed Encoding Rules).

5.4.7 *Подробно описание на транзакцията по DSRC*

DSC_44 Инициализирането се извършва съгласно DSC_44—DSC_48 и таблици 14.4—14.9. На етапа на инициализиране REDCR започва изпращането на фрейм, съдържащ BST (Beacon Service Table) съгласно EN 12834 и EN 13372, 6.2, 6.3, 6.4 и 7.1 с настройките, определени в таблица 14.4 по-долу.

Таблица 14.4.

Инициализиране — настройки за фрейма с BST

Поле	Настройки
Link Identifier („Идентификатор на връзката“)	Broadcast address
BeaconId	Съгласно EN 12834
Time	Съгласно EN 12834
Профил	Без разширение, да се използва 0 или 1
MandApplications	Без разширение, EID липсва, параметърът липсва, AID= 2 Freight&Fleet
NonMandApplications	Липсва
ProfileList	Без разширение, брой на профилите в списъка = 0
Fragmentation header	Без фрагментиране
Настройки за слой 2	PDU с команда, UI команда

Практически пример за настройките, определени в таблица 14.4, с указание за кодиранията на битовете, се дава в следващата таблица 14.5.

Таблица 14.5.

Инициализиране — пример за съдържанието на фрейма с BST

Октет #	Атрибут/поле	Битове в октета	Описание
1	FLAG	0111 1110	Флаг за начало
2	Broadcast ID	1111 1111	Broadcast address
3	MAC Control Field	1010 0000	PDU с команда
4	LLC Control field	0000 0011	UI команда
5	Fragmentation header	1xxx x001	Без фрагментиране

Октет #	Атрибут/поле	Битове в октета	Описание
6	BST	1000	Заявка за инициализиране
	SEQUENCE {		
	OPTION indicator BeaconID SEQUENCE { ManufacturerId INTEGER (0..65535)	0	Липсват незадължителни (NonMand) приложения
		xxx	Идентификатор на производителя
7		xxxx xxxx	
8		xxxx x	
	IndividualID INTEGER (0..134217727)	xxx	27 бита на разположение за идентификация на производителя
9		xxxx xxxx	
10		xxxx xxxx	
11	}	xxxx xxxx	
12	Time INTEGER (0..4294967295)	xxxx xxxx	32 bit UNIX в реално време
13		xxxx xxxx	
14		xxxx xxxx	
15		xxxx xxxx	
16	Profile INTEGER (0..127,...)	0000 0000	Без разширение. Пример за профил 0
17	MandApplications SEQUENCE (SIZE (0..127,...)) OF {	0000 0001	Без разширение, брой на mandApplications = 1
18	SEQUENCE {		
	OPTION indicator	0	EID липсва
	OPTION indicator	0	Липсващ параметър
	AID DSRCApplicationEntityID } }	00 0010	Без разширение. AID= 2 Freight&Fleet

Октет #	Атрибут/поле	Битове в октета	Описание
19	ProfileList SEQUENCE (0..127,...) OF Profile }	0000 0000	Без разширение, брой на профилите в списъка = 0
20	FCS	xxxx xxxx	Контролна поредица за фрейма
21		xxxx xxxx	
22	Flag	0111 1110	Флаг за край

DSC_45 Когато *DSRC-VU* получи BST, то заявява разпределянето на частен прозорец съгласно EN 12795 и EN 13372, 7.1.1, без специфични настройки за RTM. В таблица 14.6 се дава пример за кодирането на битовете.

Таблица 14.6.

Инициализиране — съдържание на фрейма със заявка за разпределяне на частен прозорец

Октет #	Атрибут/поле	Битове в октета	Описание
1	FLAG	0111 1110	Флаг за начало
2	Private LID	xxxx xxxx	Адрес на връзката за конкретно DSRC-VU
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control field	0110 0000	Заявка за частен прозорец
7	FCS	xxxx xxxx	Контролна поредица за фрейма
8		xxxx xxxx	
9	Flag	0111 1110	Флаг за край

DSC_46 В отговор REDCR разпределя частен прозорец съгласно EN 12795 и EN 13372, 7.1.1 без специфични настройки за RTM.

В таблица 14.7 се дава пример за кодирането на битовете.

Таблица 14.7.

Инициализиране — съдържание на фрейма за разпределяне на частен прозорец

Октет #	Атрибут/поле	Битове в октета	Описание
1	FLAG	0111 1110	Флаг за начало
2	Private LID	xxxx xxxx	Адрес на конкретното DSRC-VU за връзката
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control field	0010 s000	Разпределяне на частен прозорец
7	FCS	xxxx xxxx	Контролна поредица за фрейма
8		xxxx xxxx	
9	Flag	0111 1110	Флаг за край

DSC_47 Когато *DSRC-VU* получи разпределянето на частен прозорец, то изпраща своята VST (Vehicle Service Table) съгласно EN 12834 и EN 13372, 6.2, 6.3, 6.4 и 7.1 с настройки, определени в таблица 14.8, като използва разпределения частен прозорец.

Таблица 14.8.

Инициализиране — настройки за фрейма с VST

Поле	Настройки
Private LID	Съгласно EN 12834
Параметри на VST	Попълва се =0, после за всяко поддържано приложение: EID наличен, параметър наличен, AID=2, EID съгласно генерирания от бордовото устройство (OBU)
Параметър	Без разширение, съдържа RTM Context Mark
ObeConfiguration	Незадължителното поле ObeStatus може да е налично, но не се използва от REDCR
Fragmentation header	Без фрагментиране
Настройки за слой 2	PDU с команда, UI команда

DSC_48 *DSRC-VU* трябва да поддържа приложението „Freight and Fleet“, идентифицирана от Application Identifier ‘2’. Може да се поддържат и други Application Identifiers, но те не трябва да присъстват в тази VST, тъй като BST изисква само AID=2. Полето „Applications“ („Приложения“) съдържа списък на инстанции на поддържаните приложения в *DSRC-VU*. За инстанциирането на всяко поддържано приложение се дава препратка към съответния стандарт, състояща се от маркера RTM Context Mark, съставен от OBJECT IDENTIFIER, представляващ съответния стандарт, неговата част (9 за RTM) и евентуално неговата версия, плюс един EID, който е генериран от DSRC-VU и е свързан с инстанцията на това приложение.

Практически пример за настройките, определени в таблица 14.8, с указание за кодиранията на битовете, се дава в таблица 14.9.

Таблица 14.9.

Инициализиране — пример за съдържанието на фрейма с VST

Октет #	Атрибут/поле	Битове в октета	Описание
1	FLAG	0111 1110	Флаг за начало
2	Private LID	xxxx xxxx	Адрес на конкретното DSRC-VU за връзката
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control field	1100 0000	PDU с команда
7	LLC Control field	0000 0011	UI команда
8	Fragmentation header	1xxx x001	Без фрагментиране
9	VST SEQUENCE {	1001	Отговор на инициализиране
	Fill BIT STRING (SIZE(4))	0000	Не се използва и е зададен равен на 0
10	Profile INTEGER (0..127,…) Applications SEQUENCE OF {	0000 0000	Без разширение. Пример за профил 0
11		0000 0001	Без разширение, 1 приложение
12	SEQUENCE {		
	OPTION indicator	1	EID налице
	OPTION indicator	1	Параметърът липсва
	AID DSRCApplicationEntityID	00 0010	Без разширение. AID= 2 Freight&Fleet
13	EID Dsrc-EID	xxxx xxxx	Определен в рамките на OBU и идентифициращ инстанцията на приложението.

Октет #	Атрибут/поле	Битове в октета	Описание
14	Parameter Container {	0000 0010	Без разширение, Container Choice = 02, Октетен низ
15		0000 1000	Без разширение, дължина на Rtm Context Mark = 8
16	Rtm-ContextMark::= SEQUENCE {	0000 0110	Object Identifier на поддържания стандарт, част и версия. Пример: ISO (1) Standard (0) TARV (15638) part9(9) Version1 (1). Първият октет е 06H, който е Object Identifier,вторият октет е 06H, който дава неговата дължина. Следващите 6 октета кодират примерния Object Identifier. Забележете, че е налице само един елемент от поредицата (незадължителният елемент RtmCommProfile е изпуснат)
17	StandardIdentifier standardIdentifier	0000 0110	
18		0010 1000	
19		1000 0000	
20		1111 1010	
21		0001 0110	
22		0000 1001	
23		0000 0001	
24	ObeConfiguration Sequence { OPTION indicator	0	ObeStatus липсва
	EquipmentClass INTEGER (0..32767)	xxx xxxx	
25		xxxx xxxx	
26	ManufacturerId INTEGER (0..65535)	xxxx xxxx	Идентификатор на производителя на DSRC-VU, както е описано в ISO 14816 Register
27		xxxx xxxx	
28	FCS	xxxx xxxx	Контролна поредица за фрейма
29		xxxx xxxx	
30	Flag	0111 1110	Флаг за край

DCS_49 После REDCR извлича данните, като издава команда GET в съответствие с командата GET, определена в EN 13372, 6.2, 6.3, 6.4 и EN 12834, с настройки съгласно таблица 14.10.

Таблица 14.10.

Инициализиране — настройки за фрейма Get Request

Поле	Настройки
Invoker Identifier (IID)	Липсва
Link Identifier (LID)	Адрес на конкретното DSRC-VU за връзката
Chaining	Не

Поле	Настройки
Element Identifier (EID)	Както е указано във VST. Без разширение.
Access Credentials	Не
AttributeIdList	Без разширение, 1 атрибут, AttributeID = 1 (RtmData)
Fragmentation	Не
Layer2 settings	PDU с команда, Polled ACn команда

В таблица 14.11 се дава пример за извличането на данните за RTM.

Таблица 14.11.

Представяне — пример за фрейма Get Request

Октет #	Атрибут/поле	Битове в октета	Описание
1	FLAG	0111 1110	Флаг за начало
2	Private LID	xxxx xxxx	Адрес на конкретното DSRC-VU за връзката
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control field	1010 s000	PDU с команда
7	LLC Control field	n111 0111	Polled ACn команда, n бит
8	Fragmentation header	1xxx x001	Без фрагментиране
9	Get.request SEQUENCE {	0110	Заявка за получаване (Get)
	OPTION indicator	0	Access Credentials липсват
	OPTION indicator	0	IID липсва
	OPTION indicator	1	AttributeIdList налице
	Fill BIT STRING(SIZE(1))	0	Зададен на 0.
10	EID INTEGER(0..127,…)	xxxx xxxx	EID на инстанцията на приложението за RTM, както е указано във VST. Без разширение.
11	AttributeIdList SEQUENCE OF { AttributeId }}	0000 0001	Без разширение, брой на атрибутите = 1
12		0000 0001	AttributeId=1, RtmData. Без разширение.

Октет #	Атрибут/поле	Битове в октета	Описание
13	FCS	xxxx xxxx	Контролна поредица за фрейма
14		xxxx xxxx	
15	Flag	0111 1110	Флаг за край

DSC_50 Когато *DSRC-VU* получи заявката GET, то отговаря на GET със заявените данни в съответствие с отговора на GET, определен в EN 13372, 6.2, 6.3, 6.4 и EN 12834, с настройки съгласно таблица 14.12.

Таблица 14.12.

Представяне — настройки за фрейма с отговора на GET

Поле	Настройки
Invoker Identifier (IID)	Липсва
Link Identifier (LID)	Съгласно EN 12834
Chaining	Не
Element Identifier (EID)	Както е указано във VST.
Access Credentials	Не
Fragmentation	Не
Layer2 settings	PDU с отговора, отговорът е налице и командата е приета, ACn команда

В таблица 14.13 се дава пример за извличането на данните за RTM.

Таблица 14.13.

Представяне — пример за съдържанието на фрейма с отговора

Октет #	Атрибут/поле	Битове в октета	Описание
1	FLAG	0111 1110	Флаг за начало
2	Private LID	xxxx xxxx	Адрес на конкретното DSRC-VU за връзката
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	

Октет #	Атрибут/поле	Битове в октета	Описание
6	MAC Control field	1101 0000	PDU с отговора
7	LLC Control field	n111 0111	Отговорът е налице, ACn команда, n бит
8	LLC Status field	0000 0000	Отговорът е налице и командата е приета
9	Fragmentation header	1xxx x001	Без фрагментиране
10	Get.response SEQUENCE {	0111	Get Response (получаване на отговор)
	OPTION indicator	0	IID липсва
	OPTION indicator	1	Attribute List налице
	OPTION indicator	0	Return status липсва
	Fill BIT STRING(SIZE(1))	0	Не се използва
11	EID INTEGER(0..127,…)	xxxx xxxx	Отговор от инстанциирането на приложението за RTM. Без разширение
12	AttributeList SEQUENCE OF {	0000 0001	Без разширение, брой на атрибутите = 1
13	Attributes SEQUENCE { AttributeId	0000 0001	Без разширение, AttributeID = 1 (RtmData)
14	AttributeValue CONTAINER {	0000 1010	Без разширение, Container Choice = 10_{10}.
15		kkkk kkkk	RtmData
16		kkkk kkkk	
17		kkkk kkkk	
…		…	
n	}}}}	kkkk kkkk	
n+1	FCS	xxxx xxxx	Контролна поредица за фрейма
n+2		xxxx xxxx	
n+3	Flag	0111 1110	Флаг за край

DSC_51 След това REDCR приключва връзката, като издава команда EVENT_REPORT, RELEASE съгласно EN 13372, 6.2, 6.3, 6.4 и EN 12834,7.3.8, без специфични настройки за RTM. В таблица 14.14 се дава пример за кодирането на битовете за командата RELEASE.

Таблица 14.14.

Приключване. Съдържание на фрейма EVENT_REPORT Release

Октет #	Атрибут/поле	Битове в октета	Описание
1	FLAG	0111 1110	Флаг за начало
2	Private LID	xxxx xxxx	Адрес на конкретното DSRC-VU за връзката
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control field	1000 s000	Фреймът съдържа LPDU с команда
7	LLC Control field	0000 0011	UI команда
8	Fragmentation header	1xxx x001	Без фрагментиране
9	EVENT_REPORT.request SEQUENCE {	0010	EVENT_REPORT (Release)
	OPTION indicator	0	Access Credentials липсват
	OPTION indicator	0	Липсва параметър за събитието
	OPTION indicator	0	IID липсва
	Mode BOOLEAN	0	Не се очаква отговор
10	EID INTEGER (0..127,…)	0000 0000	Без разширение, EID = 0 (System)
11	EventType INTEGER (0..127,…) }	0000 0000	Event type 0 = Release
12	FCS	xxxx xxxx	Контролна поредица за фрейма
13		xxxx xxxx	
14	Flag	0111 1110	Флаг за край

DSC_52 Не се очаква *DSRC-VU* да отговори на командата Release. След това връзката приключва.

5.4.8 *Описание на изпитването за транзакция по DSRC*

DSC_53 Пълно изпитване, включващо защита на данните, трябва да се извършва съгласно допълнение 11 относно общите механизми за сигурност от оправомощени лица с достъп до процедури за сигурност, използвайки обичайната команда GET, както е определено по-горе.

DSC_54 Изпитването за въвеждане в експлоатация и при периодичен технически преглед, за което е необходимо дешифриране и разбиране на съдържанието на дешифрираните данни, се извършва съгласно допълнение 11 относно общите механизми за сигурност и съгласно списъка в допълнение 9 на минимално изискваните изпитания за одобрение на типа.

За базово изпитване на връзката по DSRC може да се използва обаче и командата ECHO. Такова изпитване може да се изисква за въвеждане в експлоатация, при периодичен технически преглед или другояче по искане на компетентния контролен орган или съгласно Регламент (ЕС) № 165/2014 (виж 6 по-долу).

DSC_55 За да се извърши това базово изпитване на връзката, REDCR издава командата ECHO по време на сесия, т.е. след като успешно завърши етапът на инициализиране. Поради това последователността на взаимодействията е сходна с тази при разпитване:

— Стъпка № 1: *REDCR* изпраща таблица за навигационните услуги (Beacon Service Table — BST), която включва идентификаторите на приложения (AID) в списъка на услугите, поддържани от него. В приложенията за RTM това ще бъде просто услугата със стойност на AID = 2.

DSRC-VU оценява получената BST и отговаря, когато установи, че BST заявява Freight&Fleet (AID = 2). Ако *REDCR* не предлага AID=2, *DSRC-VU* прекратява своята транзакция с *REDCR*.

— Стъпка № 2: *DSRC-VU* изпраща заявка за разпределяне на частен прозорец.

— Стъпка № 3: *REDCR* изпраща разпределение на частен прозорец.

— Стъпка № 4: *DSRC-VU* използва разпределения частен прозорец, за да изпрати своята таблица за услуги във връзка с превозното средство (Vehicle Service Table — VST). Тази VST включва списък на всички инстанциирания на различните услуги, поддържани от това *DSRC-VU* в рамките на AID=2. Различните инстанциирания се идентифицират посредством уникални идентификатори на елементи (Element Identifiers — EIDs), всеки от които е свързан със стойност на параметър, указваща инстанцията на приложението, което се поддържа.

— Стъпка № 5: след това четецът *REDCR* анализира предложената VST и или прекъсва връзката (RELEASE) поради липса на интерес към каквото и да било, предложено от VST (т.е. той получава VST от *DSRC-VU*, което не е за RTM), или започва инстанциирането на приложение, ако получи подходяща VST.

— Стъпка № 6: *REDCR* издава команда (ECHO) на конкретното *DSRC-VU* и разпределя частен прозорец.

— Стъпка № 7: *DSRC-VU* използва новоразпределения частен прозорец, за да изпрати фрейм с отговора на ECHO.

В следващите таблици се дава практически пример за сесия на обмен на данни чрез ECHO.

DSC_56 Инициализирането се извършва съгласно 5.4.7 (DSC_44—DSC_48) и таблици 14.4—14.9.

DSC_57 След това REDCR команда ACTION, ECHO съгласно ISO 14906, съдържаща 100 октета данни и без специфични настройки за RTM. Таблица 14.15 показва съдържанието на фрейма, изпратен от REDCR.

Таблица 14.15.

Пример за фрейм за заявка ACTION, ECHO

Октет #	Атрибут/поле	Битове в октета	Описание
1	FLAG	0111 1110	Флаг за начало
2	Private LID	xxxx xxxx	Адрес на конкретното DSRC-VU за връзката
3		xxxx xxxx	

Октет #	Атрибут/поле	Битове в октета	Описание
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control field	1010 s000	PDU с команда
7	LLC Control field	n111 0111	Polled ACn команда, n бит
8	Fragmentation header	1xxx x001	Без фрагментиране
9	ACTION.request SEQUENCE {	0000	Заявка за действие (ECHO)
	OPTION indicator	0	Access Credentials липсват
	OPTION indicator	1	Параметър за действие налице
	OPTION indicator	0	IID липсва
	Mode BOOLEAN	1	Очаква се отговор
10	EID INTEGER (0..127,…)	0000 0000	Без разширение, EID = 0 (System)
11	ActionType INTEGER (0..127,…)	0000 1111	Без разширение, вид на действието — заявка ECHO
12	ActionParameter CONTAINER {	0000 0010	Без разширение, Container Choice = 2
13		0110 0100	Без разширение. Дължина на низа = 100 октета
14		xxxx xxxx	Данни, които трябва да се върнат обратно
…		…	
113	}}	xxxx xxxx	
114	FCS	xxxx xxxx	Контролна поредица за фрейма
115		xxxx xxxx	
116	Flag	0111 1110	Флаг за край

DSC_58 Когато *DSRC-VU* получи заявката ECHO, то изпраща отговор от 100 октета на ECHO, като връща обратно получената команда, съгласно ISO 14906, без специфични настройки за RTM. В таблица 14.16 се дава пример за кодирането на равнище бит.

Таблица 14.16.

Пример за фрейм за отговор на ACTION, ECHO

Октет #	Атрибут/поле	Битове в октета	Описание
1	FLAG	0111 1110	Флаг за начало
2	Private LID	xxxx xxxx	Адрес на конкретното DSRC-VU за връзката
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control field	1101 0000	PDU с отговора
7	LLC Control field	n111 0111	ACn команда, n бит
8	LLC status field	0000 0000	Отговорът е налице
9	Fragmentation header	1xxx x001	Без фрагментиране
10	ACTION.response SEQUENCE {	0001	ACTION response (ECHO)
	OPTION indicator	0	IID липсва
	OPTION indicator	1	Параметър за отговор налице
	OPTION indicator	0	Return status липсва
	Fill BIT STRING (SIZE (1))	0	Не се използва
11	EID INTEGER (0..127,…)	0000 0000	Без разширение, EID = 0 (System)
12	ResponseParameter CONTAINER {	0000 0010	Без разширение, Container Choice = 2
13		0110 0100	Без разширение. Дължина на низа = 100 октета
14		xxxx xxxx	Данни, върнати обратно
…		…	
113	}}	xxxx xxxx	
114	FCS	xxxx xxxx	Контролна поредица за фрейма
115		xxxx xxxx	
116	Flag	0111 1110	Флаг за край

5.5 **Подкрепа за спазването на Директива 2015/71/ЕО**

5.5.1 *Преглед*

DSC_59 С цел подкрепа за спазването на Директива (ЕС) 2015/719 относно максимално допустимите размери и маси на тежкотоварни превозни средства, протоколът за транзакциите по изтегляне на данни от бордова система за претегляне (OWS) по интерфейсна връзка към DSRC на 5,8 GHz ще е същата, както използваната за данните за RTM (виж 5.4.1) с единствената разлика, че Object Identifier за отнасяне към стандарта TARV ще сочи стандарта ISO 15638 (TARV), част 20, отнасяща се за WOB/OWS.

5.5.2 *Команди*

DSC_60 Командите, които се използват за транзакция на данни от OWS ще бъдат същите, както използваните за транзакция на данни за RTM.

5.5.3 *Последователност на командите за разпитване*

DSC_61 Последователността на командите за разпитване за данни от OWS ще бъде същата, както за данни за RTM.

5.5.4 *Структура на данните*

DSC_62 Полезните данни (OWS data) се състоят от конкатенацията на:

1. данните EncryptedOwsPayload, които представляват криптираните данни OwsPayload, определени в ASN.1 в раздел 5.5.5. Методът на криптиране е същият, както приетият за RtmData, който е определен в допълнение 11.

2. DSRCSecurityData, изчислени по същия алгоритъм, както приетия за RtmData, който е определен в допълнение 11.

5.5.5 *Модул ASN.1 за транзакцията OWS DSRC*

DSC_63 Модулът ASN.1 за DSRC данните в рамките на приложението RTM е определен, както следва:

```
   TarvOws {iso(1) standard(0) 15638 part20(20)
   version1(1)} DEFINITIONS AUTOMATIC TAGS
   ::= BEGIN
   IMPORTS
   -- Imports data attributes and elements from EFC which are used for OWS
   LPN
   FROM EfcDsrcApplication {iso(1) standard(0) 14906 application(0) version5(5)}

   -- Imports function parameters from the EFC Application Interface Definition
   SetMMIRq
   FROM EfcDsrcApplication {iso(1) standard(0) 14906 application(0) version5(5)}

   -- Imports the L7 DSRCData module data from the EFC Application Interface Definition
   Action-Request, Action-Response, ActionType, ApplicationList, AttributeIdList, AttributeList,
   Attributes,
   BeaconID, BST, Dsrc-EID, DSRCApplicationEntityID, Event-Report-Request, Event-Report- Response,
   EventType, Get-Request, Get-Response, Initialisation-Request, Initialisation-Response,
   ObeConfiguration, Profile, ReturnStatus, Time, T-APDUs, VST
   FROM EfcDsrcGeneric {iso(1) standard(0) 14906 generic(1) version5(5)};

   -- Definitions of the OWS functions:
   OWS-InitialiseComm-Request ::= BST
   OWS-InitialiseComm-Response::= VST
   OWS-DataRetrieval-Request::= Get-Request (WITH COMPONENTS {fill (SIZE(1)), eid, accessCredentials
   ABSENT, iid ABSENT, attrIdList})
   OWS-DataRetrieval-Response::= Get-Response {OwsContainer} (WITH COMPONENTS {..., eid, iid ABSENT})
   OWS-TerminateComm::= Event-Report-Request {OwsContainer}(WITH COMPONENTS {mode (FALSE), eid (0),
   eventType (0)})
   OWS-TestComm-Request::= Action-Request {OwsContainer} (WITH COMPONENTS {..., eid (0), actionType
   (15), accessCredentials ABSENT, iid ABSENT})
   OWS-TestComm-Response::= Action-Response {OwsContainer} (WITH COMPONENTS {..., fill (SIZE(1)), eid
   (0), iid ABSENT})

   -- Definitions of the OWS attributes:
   OwsData :: = SEQUENCE {
        encryptedOwsPayload OCTET STRING (SIZE(51)) (CONSTRAINED BY { -- calculated encrypting
   OwsPayload as per Appendix 11 --}),
        DSRCSecurityData OCTET STRING
        }
   OwsPayload :: = SEQUENCE {
              tp15638VehicleRegistrationPlate LPN -- Vehicle Registration Plate as per EN 15509.
              recordedWeight INTEGER (0..65535),           -- 0= Total measured weight of the  heavy
   goods vehicle                                                          -- with 10 Kg
   resolution.
              axlesConfiguration OCTET STRING SIZE (3),     -- 0= 20 bits allowed for the number
                                                                  -- of axles for 10 axles.
              axlesRecordedWeight OCTET STRING SIZE (20),   -- 0= Recorded Weight for each axle
                                                                -- with 10 Kg resolution.
              tp15638Timestamp              INTEGER(0..4294967295)      -- Timestamp of current record
        }

Ows-ContextMark ::= SEQUENCE {
  standardIdentifier    StandardIdentifier, -- identifier of the TARV part and its version
        }

StandardIdentifier ::= OBJECT IDENTIFIER
  OwsContainer ::= CHOICE {
        integer                       [0]    INTEGER,
        bitstring                     [1]    BIT STRING,
        octetstring                   [2]    OCTET STRING (SIZE (0..127, ...)),
        universalString               [3]    UniversalString,
        beaconId                      [4]    BeaconID,
        t-apdu                        [5]    T-APDUs,
        dsrcApplicationEntityId       [6]    DSRCApplicationEntityID,
        dsrc-Ase-Id                   [7]    Dsrc-EID,
        attrIdList                    [8]    AttributeIdList,
        attrList                      [9]    AttributeList{RtmContainer},
        reserved10                    [10]   NULL,
        OwsContextmark                [11]   Ows-ContextMark,
        OwsData                       [12]   OwsData,
        reserved13                    [13]   NULL,
        reserved14                    [14]   NULL,
        time                          [15]   Time,
-- values from 16 to 255 reserved for ISO/CEN usage
        }}

END
```

5.5.6 *Елементи на OwsData, извършени действия и определения*

Елементите на OwsData са определени в подкрепа на спазването на Директива (ЕС) 2015/719 относно максимално допустимите размери и маси на тежкотоварни превозни средства. Те означават следното:

— recordedWeight представлява общата измерена маса на тежкотоварното превозно средство с разделителна способност от 10 кг, както е определено в стандарт EN ISO 14906. Например стойността 2500 представлява маса от 25 тона.

— axlesConfiguration представлява конфигурацията на тежкотоварното превозно средство по отношение на броя на осите. Конфигурацията се определя с маската от 20 бита (разширена спрямо EN ISO 14906).

Маска от 2 бита представлява конфигурацията на дадена ос в следния формат:

— Стойност 00B означава, че стойността всъщност „липсва“, тъй като превозното средство няма оборудване за измерване на теглото върху оста.

— Стойност 01B означава, че оста липсва.

— Стойност 10B означава, че оста е налична и масата се изчислява, съответните данни се събират и се предоставят в полето axlesRecordedWeight.

— Стойност 11B е резервирана за бъдеща употреба.

Последните 4 бита са резервирани за бъдеща употреба.

Брой на осите										
Брой на осите на влекача			Брой на осите на ремаркето							
00/01/-10/11	00/01/10/11	00/01/10/11	00/01/10/11	00/01/10/11	00/01/10/11	00/01/10/11	00/01/10/11	00/01/10/11	00/01/10/11	RFU (4 бита)

— axlesRecordedWeight представлява записаната конкретна маса за всяка ос с разделителна способност от 10 кг. За всяка ос се използват два октета. Например стойността 150 представлява маса от 1 500 кг.

Другите типове данни, са определени в 5.4.5.

5.5.7 *Механизми за прехвърляне на данни*

DSC_64 Механизмът за прехвърляне на данни от OWS между разпитващото устройство и средството за DSRC в превозното средство е същият, както за данните за RTM (виж 5.4.6).

DSC_65 Прехвърлянето на данни между платформата за събиране на данни за максималните маси и средството за DSRC в превозното средство се основава на физическата връзка и на определените в раздел 5.6 интерфейси и протокол.

5.6 **Прехвърляне на данни между DSRC-VU и VU**

5.6.1 *Физическа връзка и интерфейси*

DSC_66 Връзката между *VU* и *DSRC-VU* може да бъде физическа чрез кабел или безжична с малък обсег въз основа на Bluetooth v4.0 BLE.

DSC_67 Независимо от избора на физическата връзка и интерфейса трябва да бъдат изпълнени следните изисквания:

DSC_68 а) Връзката между VU и DSRC-VU трябва да бъде по отворен стандарт, за да е възможно договарянето с различни доставчици за получаването на VU и DSRC-VU, както и на DSRC-VU от различни партиди. VU се свързва с DSRC-VU по някой от следните начини:

i) по фиксиран кабел от най-малко 2 метра, използвайки от страната на DSRC-VU мъжки съединител от одобрен тип Straight DIN 41612 H11 с 11 щифта, а от страната на VU — съответен женски съединител, одобрен по DIN/ISO,

ii) чрез Bluetooth Low Energy (BLE),

iii) чрез стандартна връзка по ISO 11898 или SAE J1939.

DSC_69 б) Определението за интерфейсите и връзката между VU и DSRC-VU трябва да е в съответствие с командите на приложния протокол съгласно 5.6.2 и

DSC_70 в) VU и DSRC-VU трябва да поддържат операцията на прехвърляне на данни по връзката по отношение на характеристики и електрическо захранване.

5.6.2 *Приложен протокол*

DSC_71 Приложният протокол за комуникацията между устройството за връзка от разстояние на VU и DSRC-VU отговаря за периодичното прехвърляне на данни по връзката от разстояние от VU към DSRC.

DSC_72 Установяват се следните основни команди:

1. Initialisation of the communication link — Request („Инициализиране на съобщителната връзка — заявка“)
2. Initialisation of the communication link — Response („Инициализиране на съобщителната връзка — отговор“)
3. Send Data („Изпращане на данни“) с Identifier („идентификатор“) на приложението за RTM и Payload (полезни данни), определени от RTM Data
4. Acknowledgment („Потвърждаване на приемането“) на данните
5. Termination of the communication link — Request („Приключване на съобщителната връзка — заявка“)
6. Termination of the communication link — Response („Приключване на съобщителната връзка — отговор“)

DSC_73 В ASN1.0 горните команди могат да бъдат определени, както следва:

```
Remote Communication DT Protocol DEFINITIONS ::= BEGIN

     RCDT-Communication Link Initialization - Request ::= SEQUENCE {
          LinkIdentifier INTEGER
     }

     RCDT-Communication Link Initialization - Response::= SEQUENCE {
          LinkIdentifier INTEGER,
          answer          BOOLEAN
     }

          RCDT- Send Data ::=
          SEQUENCE { LinkIdentifier
          INTEGER, DataTransactionId
          INTEGER, RCDTData
          SignedTachographPayload
     }

          RCDT Data Acknowledgment ::
          SEQUENCE { LinkIdentifier
          INTEGER, DataTransactionId
          INTEGER,
          answer          BOOLEAN
     }

          RCDT-Communication Link Termination - Request ::= SEQUENCE {
          LinkIdentifier INTEGER
     }

          RCDT-Communication Link Termination - Response::= SEQUENCE {
          LinkIdentifier INTEGER,
          answer          BOOLEAN
     }

End
```

DSC_74 Следва описание на командите и параметрите:

— RCDT-Communication Link Initialization – Request се използва за инициализиране на съобщителната връзка. Командата се изпраща от VU на DSRC-VU. LinkIdentifier се задава от VU и се съобщава на DSRC-VU за проследяване на конкретна съобщителна връзка.

(Забележка: това е за поддържане на бъдещи връзки и други приложения/модули като бордово претегляне).

— RCDT-Communication Link Initialization – Response се използва от DSRC-VU за даване на отговор на заявката за инициализиране на съобщителната връзка. Командата се изпраща от DSRC-VU на VU. Командата предоставя резултата от инициализирането като отговор = 1 (Success, т.е. успешно) или 0 = (Failure, т.е. неуспешно).

DSC_75 Инициализирането на съобщителната връзка се извършва само след монтиране, калибриране и пускане на двигателя / VU е включено.

— RCDT-Send Data се използва от VU за изпращане на подписаните RCDTData (*данните от връзката от разстояние*) към DSRC-VU. Данните се изпращат на всеки 60 секунди. Параметърът DataTransactionId идентифицира конкретното предаване на данни. LinkIdentifier се използва и за да се гарантира, че съответната връзка е правилната.

— RCDT-Data Acknowledgment се изпраща от DSRC-VU за обратна връзка към VU относно приемането на данните вследствие на команда RCDT-Send Data , идентифицирана от параметъра DataTransactionId. Параметърът Answer е 1 (Success, т.е. успешно) или =0 (Failure, т.е. неуспешно). Ако VU получи повече от три отговора, равни на 0, или ако VU не получи RCDT Data Acknowledgment за изпратена преди това команда RCDT- Send Data с конкретен параметър DataTransactionId, VU генерира събитие, което регистрира.

— RCDT-Communication Link Termination request се изпраща от VU на DSRC-VUза приключване на връзката за конкретен LinkIdentifier.

DSC_76 При рестартирането на DSRC-VU или VU всички съществуващи съобщителни връзки се прекратяват, тъй като може да има „висящи“ връзки поради внезапното изключване на VU.

— RCDT-Communication Link Termination – Response се изпраща от DSRC-VU на VU, за да потвърди заявката за приключване на връзката от VU за конкретния LinkIdentifier.

5.7 **Третиране на грешки**

5.7.1 *Записване и съобщаване на данните в DSRC-VU*

DSC_77 *Данните* се предоставят, вече защитени, от функцията *VUSM* на *DSRC-VU*. *VUSM* проверява дали данните, регистрирани в *DSRC-VU*, са били записани правилно. Записването и протоколирането на всякакви грешки при прехвърлянето на данни от *VU* към паметта на *DSRC-VU* се извършва с типа EventFaultType и изброена стойност, зададена като '62'H Remote Communication Facility за неизправност във връзката, заедно с времевия печат.

DSC_78 *VU* трябва да поддържа файл, идентифициран от уникално име, което лесно да се разпознава от контрольори за целите на регистрирането на „вътрешни неизправности по връзката във VU“.

DSC_79 Ако VUPM се опита неуспешно да получи VU данни от модула за сигурност (за подаване на VU-DSRC), тя записва този неуспех с типа EventFaultType и изброена стойност, зададена като *'62'H Remote Communication Facility* за неизправност във връзката, заедно с времевия печат. Неуспешната връзка се открива, когато при повече от три последователни опита не се получи съобщение RCDT Data Acknowledgment за съответната команда RCDT Send Data (т.е. със същия DataTransactionId в съобщенията Send Data and Acknowledgment).

5.7.2 *Грешки при безжичната връзка*

DSC_80 Третирането на грешки при връзката трябва да бъде в съответствие със стандартите, отнасящи се за DSRC, а именно EN 300 674-1, EN 12253, EN 12795, EN 12834, и съответните параметри по EN 13372.

5.7.2.1 *Грешки по криптирането и подписа*

DSC_81 Грешките по криптирането и подписа се третират съгласно допълнение 11 относно общите механизми за сигурност и не присъстват в съобщения за грешки, свързани с прехвърлянето на данни по DSRC.

5.7.2.2 *Регистриране на грешки*

DSRC представлява динамична безжична връзка в среда на непостоянни атмосферни условия и смущения — особено в комбинациите от „преносим REDCR“ и „превозно средство в движение“ при това приложение. Поради това е необходимо да се установи разликата между „неуспешно извличане на данни“ (read failure) и „грешка“. При транзакция по безжичен интерфейс неуспешното извличане на данни е нещо обичайно, последицата от което обикновено е повторен опит за излъчване на BST и за изпълнение на поредицата от действия, водещо в повечето случаи до успешно свързване и прехвърляне на данни, ако целевото превозно средство не излезе извън обсега през времето, необходимо за повторно предаване. („Успешното“ извличане на данни може да включва няколко повторни опита).

Неуспешно извличане на данни може да се получи, понеже антените са „сдвоени“ неправилно (грешно „насочване“); понеже една от антените е екранирана — това може да е умишлено, но също така е възможно да е причинено от физическото присъствие на друго превозно средство; поради радиосмущения, по-специално от WIFI на около 5,8 GHz или други публично достъпни безжични връзки, или може да е причинено от радарни смущения или от неблагоприятни атмосферни условия (напр. по време на гръмотевична буря); или просто от излизането извън обсега на връзката по DSRC. Регистрирането на отделните случаи на неуспешно извличане на данни не е възможно поради неговото естество, просто защото не е била осъществена комуникация.

Ако обаче представителят на компетентния контролен орган се насочи към дадено превозно средство и се опита да разпита неговото *DSRC-VU*, но последващото прехвърляне на данни е неуспешно, това може да се дължи на умишлено манипулиране и следователно представителят на компетентния контролен орган се нуждае от средство, за да протоколира неуспеха и да предупреди своите колеги надолу по веригата за възможно наличие на нарушение. Колегите след това могат да спрат превозното средство и да извършат физическа проверка. DSRC-VU обаче не може да предостави данни относно неуспешната връзка, именно защото тя е била неуспешна. Следователно това протоколиране трябва да бъде функция на оборудването на REDCR, която да се предвиди при неговото проектиране.

Неуспешното извличане на данни (failure to read) технически се различава от „грешка“ (error). В настоящия контекст „грешка“ означава придобиване на погрешна стойност.

Данните, прехвърлени към *DSRC-VU*, се доставят вече защитени, така че трябва да бъдат проверени от доставчика на данните (виж 5.4).

Данните, предадени впоследствие по ефира, се проверяват чрез циклични контролни суми (CRC) на комуникационно равнище. Ако CRC бъде потвърдена, данните са правилни. Ако CRC не бъде потвърдена, данните се предават повторно. Вероятността неправилни данни да преминат успешно през проверка чрез CRC е толкова малка, че може да бъде пренебрегната.

Ако CRC не бъде потвърдена и няма време за повторно предаване и получаване на правилните данни, тогава резултатът ще бъде не грешка, а инстанциране на конкретния тип неуспешно извличане на данни.

Единствените значими данни за такъв „неуспех“, които могат да бъдат регистрирани, са за броя на осъществените успешни стартирания на транзакции, които не са довели до успешно прехвърляне на данни към REDCR.

DSC_82 Следователно *REDCR* трябва да регистрира, заедно с времеви печат, броя на случаите, в които етапът на инициализиране на разпитване по DSRC е бил успешен, но транзакцията е приключена преди успешното извличане на *данните* от REDCR. Тези данни трябва да са на разположение на представителя на компетентния контролен орган и да се съхраняват в паметта на REDCR. Начинът за постигане на това се определя при проектирането на съответния продукт или в спецификация от компетентния контролен орган.

Единствените значими данни за „грешка“, които могат да бъдат регистрирани, са за броя на случаите, в които REDCR не е успял да декриптира получените *данни*. Следва да се отбележи обаче, че това ще е показателно само за ефикасността на софтуера на REDCR. Възможно е данните технически да бъдат декриптирани, но да са безсмислени.

DSC_83 Следователно *REDCR* трябва да регистрира, заедно с времеви печат, броя на случаите, в които се е опитал, но не е успял да дешифрира данните, получени по интерфейса към DSRC.

6 ИЗПИТВАНИЯ ЗА ВЪВЕЖДАНЕ В ЕКСПЛОАТАЦИЯ И ПЕРИОДИЧЕН ТЕХНИЧЕСКИ ПРЕГЛЕД НА ФУНКЦИЯТА ЗА ВРЪЗКА ОТ РАЗСТОЯНИЕ

6.1 **Общи положения**

DSC_84 Предвидени са два вида изпитвания за функцията за връзка от разстояние:

1) Изпитване чрез ECHO за валидиране на *безжичния* съобщителен канал *DSRC-REDCR >>-:-<DSRC-VU*.

2) Изпитване за сигурност от край до край, за да се гарантира, че карта за монтаж и настройки може да получи достъп до съдържанието от криптирани и подписани данни, създадено от VU и предадено по безжичния съобщителен канал.

6.2 **ECHO**

Настоящият раздел съдържа специални разпоредби за изпитване само дали функционира каналът *DSRC-REDCR >>-:-<DSRC-VU*.

Целта на командата ECHO е да даде възможност на сервизи или изпитателни пунктове за одобрение на типа да проверят дали DSRC функционира, без да е нужен достъп до сертификати за сигурност. Поради това от изпитвателното оборудване се изисква само да е в състояние да инициализира връзка по DSRC (изпращайки BST с AID=2), след това да изпрати команда ECHO и, ако DSRC функционира, да приеме отговора на ECHO. Виж 5.4.8 за подробности. Ако то получи правилно този отговор, каналът за DSRC (*DSRC-REDCR >>-:-<DSRC-VU*) може да бъде валидиран като функциониращ правилно.

6.3 **Изпитване за валидиране на съдържанието от защитени данни**

DSC_85 Това изпитване се извършва за валидиране на защитения от край до край поток от данни. За такова изпитване е необходим тестов DSRC четец. Тестовият DSRC четец изпълнява същите функции и спецификации, както използваният от правоприлагащите органи, като разликата се състои в това, че за удостоверяване на автентичността на ползвателя на тестовия DSRC четец се използва карта за монтаж и настройки, а не контролна карта. Изпитването може да бъде извършено след първоначалното активиране на интелигентен тахограф или в края на процедурата на калибриране. След активирането превозното средство генерира и съобщава на DSRC-VU защитените данни за равно откриване.

DSC_86 Сервизният техник поставя тестовия DSRC четец на разстояние между 2 и 10 метра пред превозното средство.

DSC_87 После сервизният техник вкарва карта за монтаж и настройки в тестовия DSRC четец, за да заяви разпитването на бордовото устройство за данни за ранно откриване. След успешно разпитване сервизният техник осъществява достъп до получените данни, за да се убеди, че те са валидирани успешно за цялост и са декриптирани.

Допълнение 15

МИГРАЦИЯ: УПРАВЛЕНИЕ НА ЕДНОВРЕМЕННОТО СЪЩЕСТВУВАНЕ НА РАЗЛИЧНИ ПОКОЛЕНИЯ ОБОРУДВАНЕ

СЪДЪРЖАНИЕ

1. ОПРЕДЕЛЕНИЯ

За целите по настоящото допълнение се използват следните определения:

Интелигентна тахографска система: както е дефинирана в настоящото приложение (глава 1: определение ббб);

Първо поколение тахографска система: както е дефинирано в настоящия регламент (член 2: определение 1);

Второ поколение тахографска система: както е дефинирано в настоящия регламент (член 2: определение 7);

Дата на въвеждане: както е дефинирана в настоящото приложение (глава 1: определение ввв);

Специализирано интелигентно устройство (IDE): устройство, използвано за изтегляне на данни, както е дефинирано в допълнение 7 от настоящото приложение.

2. ОБЩИ РАЗПОРЕДБИ

2.1. **Преглед на прехода**

В преамбюла към настоящото приложение е направен преглед на прехода от първо към второ поколение тахографски системи.

В допълнение към разпоредбите на този преамбюл:

— първото поколение датчици за движение няма да бъдат оперативно съвместими с второто поколение бордови устройства;

— инсталирането на второто поколение датчици за движение в превозните средства ще започне по същото време като на второто поколение бордови устройства;

— устройствата за изтегляне на данни и за калибриране ще е необходимо да се развиват, за да могат да поддържат използването и на двете поколения уреди за регистриране на данни и тахографски карти.

2.2. **Оперативна съвместимост между бордовите устройства и картите**

Подразбира се, че първото поколение тахографски карти са оперативно съвместими с първото поколение бордови устройства (в съответствие с приложение 1B от настоящия регламент), както и че второто поколение тахографски карти са оперативно съвместими с второто поколение бордови устройства (в съответствие с приложение 1B от настоящия регламент). В допълнение към това са валидни следните изисквания:

MIG_001 С изключение на посоченото в изискване MIG_004 и изискване MIG_005, първото поколение тахографски карти могат да продължат да бъдат използвани във второто поколение бордови устройства до края на техния период на валидност. От друга страна, техните титуляри могат да поискат те да бъдат заменени с тахографски карти от второ поколение веднага щом се появят такива карти.

MIG_002 Второто поколение бордови устройства ще трябва да могат да използват всяка вкарана в тях карта от първо поколение от следните видове: карта на водач, контролна карта и фирмена карта на превозвач.

MIG_003 Тази способност на подобни бордови устройства може безвъзвратно да бъде премахвана в заводи/сервизи (workshops), така че да не могат повече да бъдат приемани тахографски карти от първо поколение. Това може да се прави само след като Европейската комисия инициира процедура, имаща за цел да се поиска от сервизите да извършват такава дейност, например при всяка периодичен технически преглед на тахограф.

MIG_004 По отношение на картите за монтаж и настройка, бордовите устройства от второ поколение трябва да могат да използват само второ поколение такива карти.

MIG_005 За целите по определяне на работния режим бордовите устройства от второ поколение трябва да вземат предвид само типовете на вкарваните валидни карти, без значение кое е тяхното поколение.

MIG_006 Всяка валидна тахографска карта от второ поколение трябва да може да се използва в бордови устройства от първо поколение точно по същия начин като тахографска карта от първо поколение от същия тип.

2.3. **Оперативна съвместимост между бордовите устройства и датчиците за движение**

Подразбира се, че първото поколение датчици за движение са оперативно съвместими с първото поколение бордови устройство, както и че второто поколение датчици за движение са оперативно съвместими с второто поколение бордови устройства. В допълнение към това са валидни следните изисквания:

MIG_007 Второто поколение бордови устройства няма да могат да се сдвояват и използват с първо поколение датчици за движение.

MIG_008 Възможно е датчици за движение от второ поколение да могат да бъдат сдвоявани или само с бордови устройства от второ поколение, или с бордови устройства и от двете поколения.

2.4. **Оперативна съвместимост между бордови устройства, тахографски карти и устройства за изтегляне на данни**

MIG_009 Възможно е устройства за изтегляне на данни да могат да бъдат използвани само с едно поколение бордови устройства и тахографски карти, или съответно и с двете поколения.

2.4.1 *Директно изтегляне на данни от карта със специализирано интелигентно устройство (IDE)*

MIG_010 IDE трябва да могат да изтеглят данни от тахографски карти от едно поколение, вкарани в съответните четящи устройства за карти, като използват механизмите за сигурност и протокола за изтегляне на данни за това поколение, и изтеглените данни трябва да са с формата, дефиниран за това поколение.

MIG_011 За да се даде възможност за контролиране на водачите от контролни органи на държави извън ЕС, трябва да е възможно изтегляне на данните от второ поколение карти на водачи (и карти за монтаж и настройки) точно по същия начин както от първо поколение карти на водачи (и карти за монтаж и настройки). Подобно изтегляне трябва да включва:

— неподписаните елементарни файлове `EF_IC` и `EF_ICC`,

— неподписаните елементарни файлове (от 1во поколение) `Card_Certificate` и `CA_Certificate`,

— останалите елементарни файлове с приложни данни (в рамките на TACHO DF), изисквани по протокола за изтегляне на данни от карти от първо поколение. Информацията трябва да бъде защитена с електронен подпис, в съответствие с механизмите за сигурност за първото поколение.

Подобно изтегляне не трябва да включва елементарни файлове от второ поколение, които присъстват само във второ поколение карти на водачи (и карти за монтаж и настройки) — елементарни файлове с приложни данни в рамките на TACHO_G2 DF.

2.4.2 *Изтегляне на данни от карта през бордово устройство*

MIG_012 Данните от второ поколение карта, вкарана в първо поколение бордово устройство, трябва да бъдат изтегляни с използване на първо поколение протокол за изтегляне на данни. Картата трябва да отговаря на командите на бордовото устройство точно по същия начин като карта от първо поколение и изтеглените данни трябва да бъдат със същия формат като данните, изтеглени от първо поколение карта.

MIG_013 Данните от първо поколение карта, вкарана във второ поколение бордово устройство, трябва да се изтеглят с използване на протокола за изтегляне на данни, дефиниран в допълнение 7 от настоящото приложение. Бордовото устройство трябва да изпраща команди на картата точно по същия начин като бордово устройство от първо поколение и изтеглените данни трябва да съответстват на формата, дефиниран за карти от първо поколение.

2.4.3 *Изтегляне на данни от бордово устройство*

MIG_014 Данните от второ поколение бордови устройства трябва да се изтеглят с използване на второ поколение механизми за сигурност и на протокола за изтегляне на данни, специфициран в допълнение 7 от настоящото приложение.

MIG_015 За да се даде възможност за контролиране на водачите от контролни органи на държави извън ЕС, както и за изтегляне на данни от бордовите устройства от заводи/сервизи в държави извън ЕС, възможно е като опция да може да се изтеглят данни от второ поколение бордови устройства с използване на първо поколение механизми за сигурност и на първо поколение протокол за изтегляне на данни. Изтеглените данни трябва да имат същия формат като данните, изтеглени от бордово устройство от първо поколение. Тази способност трябва да може да бъде избрана чрез команди в менюто.

2.5. **Оперативна съвместимост между бордово устройство и оборудване за калибриране**

MIG_016 Оборудването за калибриране трябва да може да извършва калибриране на всяко поколение тахографи, с използване на протокола за калибриране на това поколение. Възможно е калибриращото оборудване да може да се използва само с едно поколение тахографи, или и с двете поколения.

3. ОСНОВНИ СТЪПКИ ПРЕЗ ПЕРИОДА ПРЕДИ ДАТАТА НА ВЪВЕЖДАНЕ

MIG_017 Изпитвателните ключове и сертификати трябва да бъдат на разположение на производителите не по-късно от **30 месеца** преди датата на въвеждане.

MIG_018 Трябва да има готовност изпитванията за оперативна съвместимост да започнат при поискване от производителите не по-късно от **15 месеца** преди датата на въвеждане.

MIG_019 Официалните ключове и сертификати трябва да бъдат достъпни за производителите не по-късно от **12 месеца** преди датата на въвеждане.

MIG_020 Държавите членки трябва да могат да издават второ поколение карти за монтаж и настройки не по-късно **3 месеца** преди датата на въвеждане.

MIG_021 Държавите членки трябва да могат да издават всички видове тахографски карти от второ поколение не по-късно от **1 месец преди датата на въвеждане**.

4. РАЗПОРЕДБИ ЗА ПЕРИОДА СЛЕД ДАТАТА НА ВЪВЕЖДАНЕ

MIG_022 След датата на въвеждане държавите членки трябва да издават тахографски карти само от второ поколение.

MIG_023 На производителите на бордови устройства / датчици за движение се разрешава да произвеждат бордови устройства / датчици за движение от първо поколение докато те се използват в практиката, така че да могат да се заменят неизправни компоненти.

MIG_024 На производителите на бордови устройства / датчици за движение се разрешава да искат и да получават запазване на одобрението на типа на бордови устройства / датчици за движение, чийто тип вече е одобрен.

Допълнение 16

АДАПТОР ЗА ПРЕВОЗНИ СРЕДСТВА ОТ КАТЕГОРИИ M1 И N1

СЪДЪРЖАНИЕ

1. СЪКРАЩЕНИЯ И РЕФЕРЕНТНИ ДОКУМЕНТИ

1.1. **Съкращения**

Следва да се определи	Да се определи
VU	Бордово устройство

1.2. **Базови стандарти**

ISO16844-3 Пътни превозни средства. Тахографски системи. Част 3: Интерфейс на датчика за движение

2. ОБЩИ ХАРАКТЕРИСТИКИ И ФУНКЦИИ НА АДАПТОРА

2.1. **Общо описание на адаптора**

ADA_001 Адапторът осигурява на свързано с него бордово устройство защитени данни за движението, които постоянно са представителни за скоростта на превозното средство и за изминатото разстояние.

Адапторът е предназначен само за тези превозни средства, за които се изисква да са снабдени с уреди за регистриране на данните за движението в съответствие с настоящия регламент.

Той се монтира и използва само на типовете превозни средства, дефинирани в шш) „адаптор“, когато технически не е възможно монтирането на друг тип съществуващ датчик за движение, който иначе е в съответствие с разпоредбите в настоящото приложение и допълнения 1—16 към него.

Адапторът трябва да не е механично свързан с движеща се част от превозното средство, а да е свързан с импулсите за скорост/разстояние, генерирани от вградените датчици или от алтернативни интерфейси.

ADA_002 В корпуса на адаптора се монтира датчик за движение от одобрен тип (съгласно разпоредбите на настоящото приложение IB, раздел 8 — Типово одобрение на уредите за регистриране на данните за движението и на тахографските карти), като адапторът трябва да включва също преобразувател на импулси, индуктиращ входящите импулси във вградения датчик за движение. Вграденият датчик за движение трябва да е свързан с бордовото устройство, така че интерфейсът между бордовото устройство и адаптора да е в съответствие с изискванията, определени в ISO 16844-3.

2.2. **Функции**

ADA_003 Адапторът трябва да изпълнява следните функции:

— да служи като интерфейс и да адаптира входящите импулси за скоростта,

— да индуктира входящите импулси във вградения датчик за движение,

— всички функции на вградения датчик за движение, предоставящ защитени данни на бордовото устройство.

2.3. **Сигурност**

ADA_004 Не се изисква адапторът да има сертификат за сигурност в съответствие с общата цел за сигурност на датчика за движение, определена в допълнение 10 към настоящото приложение. Вместо това се прилагат свързаните със сигурността изисквания, определени в раздел 4.4 от настоящото допълнение.

3. ИЗИСКВАНИЯ КЪМ УРЕДИТЕ ЗА РЕГИСТРИРАНЕ НА ДАННИТЕ ЗА ДВИЖЕНИЕТО В СЛУЧАИТЕ, ПРИ КОИТО Е МОНТИРАН АДАПТОР

Изискванията в тази и следващите глави посочват как трябва да се тълкуват изискванията от настоящото приложение в случаите, при които се използва адаптор. Съответните номера на изискванията в приложение IB са посочени в скоби.

ADA_005 Уредите за регистриране на данните за движението на всяко превозно средство, снабдено с адаптор, трябва да съответстват на всички разпоредби от настоящото приложение, освен ако в настоящото допълнение е посочено друго.

ADA_006 Когато е монтиран адаптор, уредите за регистриране на данните за движението включват кабели, самия адаптор (заедно с датчик за движение) и бордово устройство [01].

ADA_007 Функцията за откриване на събития и/или на грешки на уредите за регистриране на данни за движението се променя както следва:

— събитието „прекъсване на захранването“ се поражда от бордовото устройство, ако то не е в режим на калибриране, в случай на прекъсване на захранването на вградения датчик за движение, продължаващо по-дълго от 200 милисекунди [79],

— събитието „грешка в данните за движение“ се поражда от бордовото устройство в случай на прекъсване на нормалния поток от данни между вградения датчик за движение и бордовото устройство и/или в случай на грешка, свързана с цялостността на данните или с удостоверяването им по време на техния обмен между вградения датчик за движение и бордовото устройство [83]

— събитието „опит за нарушаване на сигурността“ се поражда от бордовото устройство при всяко друго събитие от значение за сигурността на вградения датчик за движение, когато не е в режим на калибриране [85]

— грешката „уреди за регистриране на данните за движението“ се поражда от бордовото устройство, ако то не е в режим на калибриране при всяка грешка на вградения датчик за движение (88).

ADA_008 Грешките на адаптора, които се откриват от уредите за регистриране на данните за движението, са тези грешки, които са свързани с вградения датчик на движение [88].

ADA_009 Калибриращата функция на бордовото устройство трябва да дава възможност за автоматично сдвояване на вградения датчик за движение с бордовото устройство [202, 204].

4. КОНСТРУКТИВНИ И ФУНКЦИОНАЛНИ ИЗИСКВАНИЯ КЪМ АДАПТОРА

4.1. **Препредаване и адаптиране на входящите импулси за скорост**

ADA_011 Входният интерфейс на адаптора трябва да приема честотни импулси за скоростта на превозното средство и изминатото от него разстояние. Електрическите характеристики на входящите импулси: *подлежат на определяне от производителя*. В случай че е приложимо, за правилната интерфейсна връзка между входа на адаптора и превозното средство се допускат настройки, достъпни само за производителя на адаптора и за завода/сервиза (workshop), извършващ монтажа на адаптора.

ADA_012 Входният интерфейс на адаптора трябва да може, в случай че е приложимо, да умножава или да дели честотните импулси на входящите импулси за скоростта с постоянен коефициент, за да адаптира сигнала към интервала от стойностите на коефициента k, определен в настоящото приложение (4 000 до 25 000 импулса/km). Този постоянен коефициент може да бъде програмиран само от производителя на адаптора и от завода/сервиза, извършващ монтажа на адаптора.

4.2. **Индуктиране на входящите импулси във вградения датчик за движение**

ADA_013 Входящите импулси, които е възможно да са адаптирани, както е посочено по-горе, се индуктират във вградения датчик за движение, така че всеки входящ импулс да се регистрира от датчика за движение.

4.3. **Вграден датчик за движение**

ADA_014 Вграденият датчик за движение се стимулира от индуктираните импулси, като по този начин генерира данни за движението, представящи точно движението на превозното средство, както при механично свързване на датчика с движеща се част на превозното средство.

ADA_015 Идентификационните данни на вградения датчик за движение се използват от бордовото устройство за разпознаване на адаптора [95].

ADA_016 Монтажните данни, съхранявани във вградения датчик за движение, се считат, че представляват монтажните данни на адаптора [122].

4.4. **Изисквания за сигурност**

ADA_017 Корпусът на адаптора трябва да се проектира така, че да не може да се отваря. Той трябва да е пломбиран, така че опитите за отваряне да бъдат откривани лесно (напр. чрез визуална инспекция, вж. ADA_035). Пломбите трябва да съответстват на същите изисквания като изискванията за пломбите на датчика за движение [398 до 406].

ADA_018 Не трябва да е възможно сваляне на вградения датчик за движение от адаптора без да се счупи(ят) пломбата(ите) на корпуса на адаптора, или без да се счупи пломбата между датчика и корпуса на адаптора (вж. ADA_034).

ADA_019 Адапторът трябва да гарантира, че данни за движението могат да се обработват и получават само от постъпващите в адаптора данни.

4.5. **Експлоатационни характеристики**

ADA_020 Адаптерът трябва да е напълно работоспособен в температурния обхват, дефиниран от производителя.

ADA_021 Адаптерът трябва да е напълно работоспособен в интервала за стойности на влажността от 10 % до 90 % [214].

ADA_022 Адаптерът трябва да е защитен от пренапрежение, обръщане на поляритета на захранването и къси съединения [216].

ADA_023 Адаптерът трябва да е защитен по един от следните два начина:

— да реагира на магнитно поле, смущаващо събирането на данни за движението на превозното средство. При такива обстоятелства бордовото устройство регистрира и записва неизправност в датчика [88], или

— да има чувствителен елемент, който е защитен срещу магнитни полета или е устойчив на такива [217].

ADA_024 Адаптерът трябва да съответства на международното правило на ИКЕ на ООН UN ECE R10, отнасящо се за електромагнитната съвместимост, и трябва да бъде защитен срещу електростатични разряди и преходни процеси [218].

4.6. **Материали**

ADA_025 Адаптерът трябва да отговаря на степен на защита (определя се от производителя, в зависимост от мястото на монтаж) [220, 221].

ADA_026 Корпусът на адаптора трябва да е в жълт цвят.

4.7. **Маркировки**

ADA_027 Върху адаптора трябва да е закрепена указателна табелка, съдържаща следните данни:

— наименование и адрес на производителя на адаптора;

— фабричен номер от производителя, и година на производство на адаптора;

— знак за одобрение на типа на адаптора или типа на уредите за регистриране на данните за движението, включващи адаптора;

— датата, на която е монтиран адаптерът;

— идентификационния номер на превозното средство, на което е монтиран.

ADA_028 Указателната табелка трябва да съдържа също и следната информация (ако не може да се прочете отвън върху вградения датчик за движение):

— наименование на производителя на вградения датчик за движение;

— фабричен номер от производителя, и година на производство на вградения датчик за движение;

— знак за одобрение на вградения датчик за движение.

5. МОНТАЖ НА УРЕДИТЕ ЗА РЕГИСТРИРАНЕ НА ДАННИТЕ ЗА ДВИЖЕНИЕТО В СЛУЧАИТЕ, ПРИ КОИТО СЕ ИЗПОЛЗВА АДАПТОР

5.1. **Монтаж**

ADA_029 Адаптерите се монтират в превозни средства само от производители на превозни средства или от одобрени заводи/сервизи, оторизирани да монтират, задействат и калибрират цифрови и интелигентни тахографи.

ADA_030 Одобреният завод/сервиз, който монтира адаптора, трябва да настрои входния интерфейс и да избере отношението на делене на входния сигнал (в случаите, в които това е приложимо).

ADA_031 Одобреният завод/сервиз, който монтира адаптора, трябва да пломбира корпуса на адаптора.

ADA_032 Адапторът трябва да е монтиран възможно най-близо до тази част на превозното средство, от която идват входящите в него импулси.

ADA_033 Кабелите за захранване на адаптора трябва да са червен (положителен полюс) и черен (маса).

5.2. **Пломбиране**

ADA_034 Прилагат се следните изисквания за пломбиране:

— корпусът на адаптора трябва да е пломбиран (вж. ADA_017),

— корпусът на вградения датчик трябва да е пломбиран за корпуса на адаптора, освен ако изваждането на вградения датчик от корпуса на адаптора е невъзможно без да се счупи(ят) пломбата(ите) на корпуса на адаптора (вж. ADA_018),

— корпусът на адаптора трябва да е пломбиран за превозното средство,

— връзката между адаптора и оборудването, което подава входящите в него импулси, трябва да е пломбирана в двата края (доколкото това е разумно осъществимо).

6. ПРОВЕРКИ, ТЕХНИЧЕСКИ ПРЕГЛЕДИ И ПОПРАВКИ

6.1. **Периодични технически прегледи**

ADA_035 Когато се използва адаптор, всеки периодичен технически преглед (периодичният технически преглед означава инспекция в съответствие с изискванията с номера от [409] до [413] от приложение 1B) на уредите за регистриране на данните за движението трябва да включва следните проверки:

— че върху адаптора е поставен съответният знак за одобрение на типа,

— че пломбите на адаптора и връзките му са невредими,

— че адапторът е монтиран, както е показано на монтажната табелка,

— че адапторът е монтиран, както е посочено от производителя на адаптора и/или на превозното средство,

— че монтирането на адаптор е разрешено за преглежданото превозно средство.

ADA_036 Тези технически прегледи трябва да включват калибриране и замяна на всички пломби, каквото и да е тяхното състояние.

7. ОДОБРЕНИЕ НА ТИПА НА УРЕДИТЕ ЗА РЕГИСТРИРАНЕ НА ДАННИТЕ ЗА ДВИЖЕНИЕТО В СЛУЧАИТЕ, ПРИ КОИТО СЕ ИЗПОЛЗВА АДАПТОР

7.1. **Общи положения**

ADA_037 Уредите за регистриране на данните за движението се представят за одобрение на типа, окомплектовани с адаптор [425].

ADA_038 Даден адаптор може да бъде представен за одобрение на собствения му тип, или за одобрение на типа като елемент от уредите за регистриране на данните за движението.

ADA_039 Такова одобрение на типа трябва да включва функционални изпитвания с участието на адаптора. Положителните резултати при всяко от тези изпитвания се удостоверяват чрез съответен сертификат [426].

7.2. **Функционален сертификат**

ADA_040 Функционален сертификат на адаптор или на уреди за регистриране на данните за движението, включващи адаптор, се издава на производителя на адаптора само след като са били преминати успешно следните функционални изпитвания.

№	Изпитване	Описание	Съответни изисквания
1.	**Административен преглед**		
1.1	Документация	Коректност на документацията на адаптора	
2.	**Визуално инспектиране**		
2.1	Съответствие на адаптора с документацията		
2.2	Идентификация/маркировка на адаптора		ADA_027, ADA_028
2.3	Материали, от които е направен адапторът		[219] до [223] ADA_026
2.4	Пломбиране		ADA_017, ADA_018, ADA_034
3.	**Функционални изпитвания**		
3.1	Индуктиране на импулсите за скорост във вградения датчик за движение		ADA_013
3.2	Препредаване и адаптиране на входящите импулси за скорост		ADA_011, ADA_012
3.3	Точност на измерване на движението		[30] до [35], [217]
4.	**Изпитания за въздействията на околната среда**		
4.1	Резултати от изпитване, проведено от производителя	Резултати от изпитванията на производителя за въздействието на околната среда	ADA_020, ADA_021, ADA_022, ADA_024
5.	**Изпитание за електромагнитна съвместимост**		
5.1	Излъчени емисии и чувствителност към тях	Проверява се съответствието с Директива 2006/28/ЕО	ADA_024
5.2	Резултати от изпитване, проведено от производителя	Резултати от изпитванията на производителя за въздействието на околната среда	ADA_024