

# Официален вестник

## на Европейския съюз

L 85



Издание  
на български език

Законодателство

Година 61  
28 март 2018 г.

Съдържание

II *Незаконодателни актове*

РЕГЛАМЕНТИ

- ★ Регламент за изпълнение (ЕС) 2018/502 на Комисията от 28 февруари 2018 година за изменение на Регламент за изпълнение (ЕС) 2016/799 по отношение на определянето на изискванията за конструкцията, изпитването, монтирането, експлоатацията и ремонта на тахографите и техните компоненти <sup>(1)</sup> ..... 1

<sup>(1)</sup> Текст от значение за ЕИП.

BG

Актовете, чиито заглавия се отпечатват със светъл шрифт, са актове по текущо управление на селскостопанската политика и имат кратък срок на действие.

Заглавията на всички останали актове се отпечатват с получер шрифт и се предшества от звездичка.



## II

(Незаконодателни актове)

## РЕГЛАМЕНТИ

## РЕГЛАМЕНТ ЗА ИЗПЪЛНЕНИЕ (ЕС) 2018/502 НА КОМИСИЯТА

от 28 февруари 2018 година

за изменение на Регламент за изпълнение (ЕС) 2016/799 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 <sup>(1)</sup>, и по-специално член 11 и член 12, параграф 7 от него,

като има предвид, че:

- (1) С Регламент (ЕС) № 165/2014 бяха въведени интелигентните тахографи — цифрови тахографи от второ поколение, които включват свързване към глобалната навигационна спътникова система (GNSS), устройство за връзка с цел ранно откриване от разстояние и по избор — интерфейс с интелигентни транспортни системи.
- (2) Техническите изисквания за конструкцията, изпитването, монтирането, експлоатацията и ремонта на тахографите и техните компоненти са определени с Регламент за изпълнение (ЕС) 2016/799 <sup>(2)</sup>.
- (3) Съгласно членове 8, 9 и 10 от Регламент (ЕС) № 165/2014 в превозни средства, които са регистрирани за първи път на 15 юни 2019 г. или след тази дата, следва да бъдат монтирани интелигентни тахографи. С оглед на това Регламент за изпълнение (ЕС) 2016/799 следва да бъде изменен, така че установените с него технически разпоредби да се прилагат от тази дата.
- (4) С цел да се изпълни изискването съгласно член 8 от Регламент (ЕС) № 165/2014 местоположението на превозното средство да се регистрира на всеки три часа от общото време на управление, Регламент за изпълнение (ЕС) 2016/799 следва да бъде изменен, така че информацията за местоположението на превозното средство да може да се съхранява през три часа с измерим показател, който не може да бъде върнат към първоначално зададената стойност, както и за да се избегне объркване с измеримия показател „време на непрекъснато управление“, който има различна функция.
- (5) Бордовото устройство може да се състои само от един блок или от няколко блока, които са разположени на различни места в превозното средство. Така устройствата за връзка към GNSS и към специализирани съобщителни системи с малък обсяг на действие (DSRC) могат да бъдат в основния корпус на бордовото устройство или извън него. Когато се използват външни устройства, следва да бъде възможно и двете да могат да получат одобрение на типа като компоненти заедно с основния корпус на бордовото устройство, така че процесът за одобрение на типа за интелигентните тахографи да бъде съобразен с нуждите на пазара.
- (6) Правилата за съхранение на информация за събитие на времеви конфликт и за сверяване на часовника трябва да бъдат изменени, за да може да се направи разлика между автоматичните сверявания на часовника, които се задействат след евентуален опит за намесителство или при неизправност на тахографа, и сверявания на часовника, настъпили по други причини, например при поддръжка.
- (7) Идентификаторите на данни следва да могат да правят разлика между данните, извлечени от интелигентен тахограф и от тахограф от предишно поколение.

<sup>(1)</sup> ОВ L 60, 28.2.2014 г., стр. 1.

<sup>(2)</sup> Регламент за изпълнение (ЕС) 2016/799 на Комисията от 18 март 2016 г. 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 (ОВ L 139, 26.5.2016 г., стр. 1).

- (8) Срокът на валидност на картата на превозвач следва да бъде удължен от две на пет години, за да се уеднакви със срока на валидност на картата на водача.
- (9) Следва по-добре да се уточнят описанието на някои неизправности и събития, потвърждаването на въведеното местоположение в началото и/или в края на дневен период на работа, използването на съгласието на водача при интерфейс с интелигентни транспортни системи във връзка с данните, предадени от бордовото устройство чрез мрежата на превозното средство, както и други технически въпроси.
- (10) С цел да се гарантира актуалната им сертификация пломбите на тахографите трябва да бъдат приведени в съответствие с новия стандарт относно сигурността на механичните пломби, използвани за тахографи.
- (11) Настоящият регламент се отнася за конструкцията, изпитването, монтирането и експлоатацията на системи, съдържащи и радиосъоръжения, като съответните разпоредби са уредени с Директива 2014/53/ЕС на Европейския парламент и на Съвета<sup>(1)</sup>. С директивата се регламентират пускането на пазара и пускането в употреба на електронно и електрическо оборудване, което използва радиовълни за комуникация и/или за хоризонтално радиоопределяне, по-специално във връзка с електронните компоненти за безопасност, съвместимостта с други системи, достъпа до радиочестотния спектър, достъпа до услуги за спешна помощ и/или други делегирани разпоредби. С цел да се гарантира ефикасното използване на радиочестотния спектър, да се предотвратят вредни радиосмущения, да се обезпечат безопасността и електромагнитната съвместимост на радиосъоръженията, както и за да се осигури възможност за въвеждането на други специфични изисквания посредством делегирани актове, настоящият регламент следва да се прилага, без да се засягат разпоредбите на посочената директива.
- (12) Поради това Регламент за изпълнение (ЕС) 2016/799 следва да бъде изменен.
- (13) 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

Регламент за изпълнение (ЕС) 2016/799 се изменя, както следва:

1) Член 1 се изменя, както следва:

а) втори и трети параграф се заменят със следното:

„2. Конструкцията, изпитването, монтирането, проверката, експлоатацията и ремонтът на интелигентните тахографи и техните компоненти трябва да отговарят на техническите изисквания, формулирани в приложение IV 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 в приложение I към Регламент (ЕС) № 165/2014 или приложение B към Регламент (ЕИО) № 3821/85 на Съвета (\*), според случая.

(\*) 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).“;

б) добавя се следният параграф 5:

„5. Настоящият регламент не засяга разпоредбите на Директива 2014/53/ЕС на Европейския парламент и на Съвета (\*).

(\*) Директива 2014/53/ЕС на Европейския парламент и на Съвета от 16 април 2014 г. за хармонизирането на законодателствата на държавите членки във връзка с предоставянето на пазара на радиосъоръжения и за отмяна на Директива 1999/5/ЕО (ОВ L 153, 22.5.2014 г., стр. 62).“

2) Член 2 се изменя, както следва:

а) определение 3 се заменя със следното:

„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, и за извършването на изпитванията, определени в приложение IV към настоящия регламент, както и чертежи, снимки и други съответни документи;“

<sup>(1)</sup> Директива 2014/53/ЕС на Европейския парламент и на Съвета от 16 април 2014 г. за хармонизирането на законодателствата на държавите членки във връзка с предоставянето на пазара на радиосъоръжения и за отмяна на Директива 1999/5/ЕО (ОВ L 153, 22.5.2014 г., стр. 62).

б) определение 7 се заменя със следното:

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

в) определение 8 се заменя със следното:

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

г) добавя се следното определение 10:

„10) „бордово устройство“ е тахографът, с изключение на датчика за движение и кабелите за връзка с него.

Бордовото устройство може да се състои само от един блок или от няколко блока, разположени на различни места в превозното средство, и включва блок за обработване на данните, памет за данни, функция за измерване на времето, две устройства за интерфейс с карти с памет за водач и помощник-водач, печатащо устройство, екран, електрически съединители и устройства, позволяващи въвеждането на данни от потребителя, приемник на сигнали от GNSS и устройство за връзка от разстояние.

Бордовото устройство може да се състои от следните компоненти, за които се изисква одобрение на типа:

- бордово устройство като единичен компонент (с приемник на сигнали от GNSS и устройство за връзка от разстояние),
- основен корпус на бордовото устройство (с устройство за връзка от разстояние) и външно устройство за GNSS;
- основен корпус на бордовото устройство (с приемник на сигнали от GNSS) и външно устройство за връзка от разстояние,
- основен корпус на бордовото устройство, външен приемник на сигнали от GNSS и външно устройство за връзка от разстояние.

Ако бордовото устройство се състои от няколко блока, разположени на различни места в превозното средство, основен корпус на бордовото устройство е блокът, в който са блокът за обработване на данните, паметта за данните и функцията за измерване на времето.

„Бордово устройство (VU)“ се използва за бордовото устройство или за основния корпус на бордовото устройство.“

3) В член 6 трета алинея се заменя със следното:

„Приложение IV обаче се прилага от 15 юни 2019 г., с изключение на допълнение 16, което се прилага от 2 март 2016 г.“

4) Приложение IV се изменя в съответствие с приложение I към настоящия регламент.

5) Приложение II се изменя в съответствие с приложение II към настоящия регламент.

## Член 2

### Влизане в сила

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

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

Съставено в Брюксел на 28 февруари 2018 година.

За Комисията  
Председател  
Jean-Claude JUNCKER

## ПРИЛОЖЕНИЕ I

Приложение IV към Регламент (ЕС) 2016/799 се изменя, както следва:

1) Съдържанието се изменя, както следва:

а) точка 3.12.5 се заменя със следното:

„3.12.5. Места и местоположения, където започват и завършват дневните периоди на работа и/или където общото време на управление на МПС достига 3 часа“;

б) точка 4.5.3.2.16 се заменя със следното:

„4.5.3.2.16 Данни за местата за три часа общо управление на МПС“;

в) точка 4.5.4.2.14 се заменя със следното:

„4.5.4.2.14 Данни за местата за три часа общо управление на МПС“;

г) точка 6.2 се заменя със следното:

„6.2 Проверка на новите или поправените компоненти“.

2) Точка 1 се изменя, както следва:

а) определение ии) се заменя със следното:

„и) „устройство за връзка от разстояние“ или „устройство за ранно откриване от разстояние“ означава:

оборудването в бордовото устройство, използвано за извършването на целенасочени пътни проверки;“

б) определение рр) се заменя със следното:

„рр) „сверяване на часовника“ означава:

сверяване на текущото време, което може да се извършва автоматично през равни интервали, като за еталонна стойност се използва времето, получено от приемника на сигнали от GNSS, или при калибриране;“

в) в определение хх) първото тире се заменя със следното:

„— монтирано и се използва само в превозни средства от типове M1 и N1 (както са определени в последното изменение на приложение II към Директива 2007/46/ЕО на Европейския парламент и на Съвета (\*),“;

г) добавя се ново определение яя):

„яя) „общо време на управление“ означава:

стойност, представляваща общо натрупания брой минути управление на дадено превозно средство.

Стойността на общото време на управление е непрекъснато отброяваната стойност на всички минути, които функцията за следене на дейностите, извършвани от водача, в уредите за регистриране на данните за движението отчита като „УПРАВЛЕНИЕ“, и се използва само за да се задейства регистриране на местоположението на превозното средство всеки път, когато общото време на управление достигне кратно число на три часа. Отброяването с натрупване започва с активирането на уреда за регистриране на данните за движението. То не се влияе от други условия, като местоположение извън обсега или пътуване с ферибот/влак.

Не се предвижда показване, разпечатване или извличане на стойността на общото време на управление;“.

3) В точка 2.3, подточка 13 последното тире се заменя със следното:

„— бордовите устройства обикновено са със срок на валидност на действията от 15 години, считано от датата, на която влизат в сила сертификатите на бордовото устройство, но устройствата могат да се използват още 3 месеца само за изтегляне на данни.“

4) В точка 2.4 първият абзац се заменя със следното:

„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 бордовото устройство и външното устройство за GNSS, ако има такова, както и да защитава поверителността, целостта и автентичността на данните, обменяни чрез връзката за ранно откриване от разстояние с контролна цел, и да проверява целостта и автентичността на изтеглените данни.“

5) В точка 3.2, подточка 27 второто тире се заменя със следното:

„— места, където времето на общо управление на МПС достигакратно число на три часа;“

6) В точка 3.4 подточка 49 се заменя със следното:

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

7) В точка 3.6.1 подточка 59 се заменя със следното:

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

Временно въвеждане, направено при последното изваждане на картата, се потвърждава (т.е. впоследствие не се замества) при следните условия:

— въвеждане на място, където започва текущият дневен период на работа, при ръчно въвеждане съгласно изискването в подточка 61;

— следващо въвеждане на място, където започва текущият дневен период на работа, ако титулярят на картата не въведе място, където започва или където е свършил периодът на работа, по време на ръчното въвеждане съгласно изискването в подточка 61.

Временно въвеждане, направено при последното изваждане на картата, се изтрива и новата стойност се потвърждава при следните условия:

— следващо въвеждане на място, където завършва текущият дневен период на работа, ако титулярят на картата не въведе място, където започва или където е свършил периодът на работа, по време на ръчното въвеждане съгласно изискването в подточка 61.“

8) В точка 3.6.2 шестото и седмото тире се заменят със следното:

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

— място, където започва текущият дневен период на работа, заедно със съответното време (като по този начин се потвърждава временно въведеното при последното изваждане на картата).“

9) Точка 3.9.15 се заменя със следното:

„3.9.15 Събитие „времеви конфликт“

86) Това събитие се задейства, **извън режима на калибриране**, когато бордовото устройство установи несъответствие, по-дълго от 1 минута, между показанията на функцията за измерване на времето на бордовото устройство и данните за времето, постъпващи 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, ако в продължение на 30 или повече дни от приемника на сигнали от GNSS не е можел да бъде открит валиден сигнал от GNSS.“

10) В точка 3.9.17 се добавя следното тире:

„— неизправност на интерфейса с ITS (ако е приложимо)“.

11) Точка 3.10 се изменя, както следва:

i) текстът преди таблицата в подточка 89 се заменя със следното:

„Уредът за регистриране на данните за движението трябва да открива неизправности чрез функции за изпробване и самоизпробване в съответствие с таблицата по-долу:“;

ii) в таблицата се добавя следният ред:

„интерфейс с ITS (незадължителен)	Правилно функциониране“	
-----------------------------------	-------------------------	--

12) В точка 3.12 второто тире се заменя със следното:

„— средният брой на местоположенията на ден се определя като най-малко 6 местоположения, в които започва дневният период на работа, 6 местоположения, в които общото време на управление на МПС достига кратно число на три часа, и 6 местоположения, в които завършва дневният период на работа, така че „365 дни“ включват най-малко 6570 местоположения.“.

13) Точка 3.12.5 се изменя, както следва:

a) заглавието и подточка 108 се заменят със следното:

„3.12.5. Места и местоположения, където започват и завършват дневните периоди на работа и/или където общото време на управление на МПС достига 3 часа

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

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

— местоположения, където общото време на управление на МПС достига кратно число на три часа;

— места и местоположения, където водачът и/или вторият водач приключва своя дневен период на работа.“;

б) в подточка 110 четвъртото тире се заменя със следното:

„— вид на въвеждането (начало, край или 3 часа общо време на управление на МПС);“;



в) подточка 111 се заменя със следното:

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

14) В точка 3.12.7 подточка 116 се заменя със следното:

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

15) Таблицата в точка 3.12.8 се изменя, както следва:

а) между позициите „Липса на информация за местоположението от приемник на сигнали от GNSS“ и „Грешка в данните за движението“ се вмъква следната позиция:

„Грешка в комуникацията с външното устройство за GNSS	<ul style="list-style-type: none"> <li>— най-продължителното събитие за всеки от последните 10 дни на възникване,</li> <li>— 5-те най-продължителни събития през последните 365 дни.</li> </ul>	<ul style="list-style-type: none"> <li>— дата и час на началото на събитие,</li> <li>— дата и час на края на събитие,</li> <li>— 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,</li> <li>— брой сходни събития, възникнали същия ден.“</li> </ul>
---	---	--

б) позицията „Времеви конфликт“ се заменя със следното:

„Времеви конфликт	<ul style="list-style-type: none"> <li>— най-сериозното събитие за всеки от десетте последни дена на възникване (т.е. с най-голяма разлика между датата и часа на уреда за регистриране на данните за движението и датата и часа по GNSS).</li> <li>— 5-те най-сериозни събития през последните 365 дни.</li> </ul>	<ul style="list-style-type: none"> <li>— дата и час на уреда за регистриране на данните за движението,</li> <li>— дата и час по GNSS,</li> <li>— 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,</li> <li>— брой сходни събития, възникнали същия ден.“</li> </ul>
-------------------	---	--

16) В точка 3.20 подточка 200 се заменя със следното:

„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 или в режим на калибриране от външно устройство.

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

Изискването за съгласието на водача не се прилага за данните, които уредите за регистриране на данните за движението предават към мрежата на превозното средство. Ако постъпилите в мрежата на превозното средство лични данни се обработват допълнително извън нея, производителят на превозното средство носи отговорност за това обработването им да се извършва в съответствие с разпоредбите на Регламент (ЕС) 2016/679 (Общ регламент относно защитата на данните).

Изискването за съгласието на водача не се прилага също така за данните от тахографа, извлечени от превозвач от разстояние (съгласно изискването в подточка 193), тъй като този сценарий се следи чрез правото за достъп на картата на превозвача.

За ITS данните, предоставяни чрез този интерфейс, се прилагат следните изисквания:

- тези данни представляват набор от избрани съществуващи данни от речника на данните на тахографа (допълнение 1),
- поднабор на тези избрани данни е отбелязан 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,
- съгласието на водача може да бъде активирано или деактивирано във всеки един момент чрез команди от менюто, при условие че е вкарана картата на водач,
- наборът и поднаборът от данни се излъчват чрез безжичния протокол Bluetooth с обхват кабината на превозното средство при честота на обновяване 1 минута,
- съдвояването на външното устройство с интерфейса с ITS е защитено чрез специален за целта случаен PIN от най-малко 4 числа, записани във и достъпни чрез дисплея на всяко бордово устройство,
- наличието на интерфейс с ITS при никакви обстоятелства 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.

Уредът за регистриране на данните за движението трябва да може да съобщава информация за съгласието на водача на други платформи в мрежата на превозното средство.

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

17) В точка 3.23 подточка 211 се заменя със следното:

„211) Настройката на часа на вътрешния часовник на бордовото устройство трябва да се коригира автоматично на всеки 12 часа. Когато това не е възможно, тъй като няма сигнал от GNSS, настройката на часа трябва да се извършва 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.“

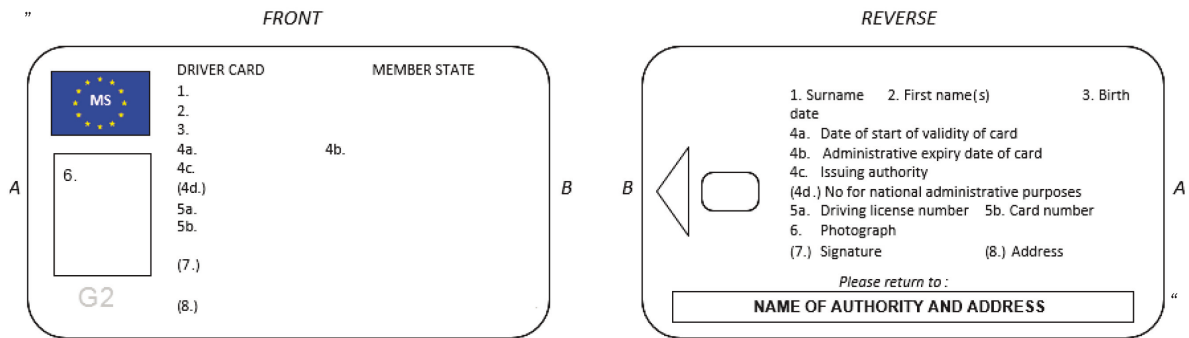
18) В точка 3.26 подточки 225 и 226 се заменят със следното:

„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,
- серийен номер,
- знак за одобрение на типа.

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

19) В точка 4.1 изображението, на което са показани лицевата и обратната страна на картата на водача, се заменя със следното:



20) В точка 4.5.3.1.8, подточка 263 първото тире се заменя със следното:

„— Неизправност на картата (когато неизправна е самата карта),“.

21) В точка 4.5.3.2.8, подточка 288 първото тире се заменя със следното:

„— Неизправност на картата (когато неизправна е самата карта),“.

22) Точка 4.5.3.2.16 се заменя със следното:

„4.5.3.2.16 Данни за местата за три часа общо управление на МПС

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

- дата и час, когато общото време на управление на МПС достигне кратно число на три часа,
- местоположението на превозното средство,
- точността на GNSS, датата и часа, когато е било определено местоположението,
- стойността от километражния брояч на превозното средство.

306) Картата на водач трябва да може да съхранява най-малко 252 такива записа.“

23) Точка 4.5.4.2.14 се заменя със следното:

„4.5.4.2.14 Данни за местата за три часа общо управление на МПС

353) Картата за монтаж и настройки трябва да позволява съхраняването на следните данни, свързани с местоположението на превозното средство, когато общото време на управление на МПС достигне кратно число на три часа:

- дата и час, когато общото време на управление на МПС достигне кратно число на три часа,

- местоположението на превозното средство,
- точността на GNSS, датата и часа, когато е било определено местоположението,
- стойността от километражния брояч на превозното средство.

354) Картата за монтаж и настройки трябва да позволява съхраняването на най-малко 18 такива записа.“

24) В точка 5.2 подточка 396 се заменя със следното:

„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 „ $w = \dots$  импулса/km“,
- константа на уредите за регистриране на данните за движението, във вида „ $k = \dots$  импулса/km“,
- действителна обиколка на колелата с гумите, във вида „ $l = \dots$  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, ако има такова,
- серийния номер на устройството за връзка от разстояние, ако има такова,
- 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 частта на превозното средство, която изработва входящите за адаптера импулси,
- серийния номер на вградения в адаптера датчик за движение.“

25) Точка 5.3 се изменя, както следва:

а) след подточка 398 се вмъква нова подточка 398а:

„398а) Посочените по-горе пломби трябва да бъдат сертифицирани по стандарт EN 16882:2016.“;

б) в подточка 401 вторият абзац се заменя със следното:

„Този уникален идентификационен номер се определя като: MMNNNNNNNN чрез неизтриваема маркировка, като MM е уникална идентификация на производителя (регистрирането в базата данни се управлява от ЕК), а NNNNNNNN е буквено-цифров номер на пломбата, който е уникален в областта на производителя.“;

в) подточка 403 се заменя със следното:

„403) След като сертифицират даден модел пломба по стандарт EN 16882:2016, производителите на пломби трябва да се регистрират в специална база данни и публично да оповестят своите идентификационни номера на пломби чрез процедура, която ще се определи от Европейската комисия.“;

г) подточка 404 се заменя със следното:

„404) За целите на Регламент (ЕС) № 165/2014 одобрените сервизи и производители на превозни средства използват само пломби, сертифицирани по стандарт EN 16882:2016, от производители на пломби, включени в гореспоменатата база данни.“

26) Точка 6.2 се заменя със следното:

„6.2. Проверка на новите или поправените компоненти

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 глави 3.2.1, 3.2.2, 3.2.3 и 3.3.“

27) В точка 6.3 подточка 408 се заменя със следното:

„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 3.2.1, 3.2.2, 3.2.3 и 3.3. Всички монтирани компоненти трябва да бъдат пломбирани в съответствие с глава 5.3, като монтажът трябва да включва и калибриране.“

28) Точка 8.1 се изменя, както следва:

а) в точка 8.1 уводният текст преди подточка 425 се заменя със следното:

„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 или кабелите, свързващи датчика за движение с бордовото устройство, външното устройство за GNSS с бордовото устройство или външното устройство 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 един или повече компоненти на уредите за регистриране на данните за движението с всеки друг компонент или компоненти на такива уреди, 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.

Както се посочва в член 2, определение 10 от настоящия регламент, бордовите устройства могат да включват различни компоненти. С каквито и компоненти да е слобено бордовото устройство, външната антена и (ако е приложимо) високочестотният разклонител за антената, свързан с приемника на сигнали от GNSS или с устройството за връзка от разстояние, не са част от одобрението на типа на бордовото устройство.

При все това производителите, получили одобрение на типа за бордово устройство, трябва да поддържат публично достъпен списък на съвместимите антени и високочестотни разклонители за всяко получило одобрение на типа бордово устройство, външно устройство за GNSS и външно устройство за връзка от разстояние.“;

б) подточка 427 се заменя със следното:

„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 (ако съгласно настоящото приложение се изисква такъв),
- сертификат за функциониране,
- сертификат за оперативна съвместимост (ако съгласно настоящото приложение се изисква такъв),

за уредите за регистриране на данните за движението или за тахографската карта, за които се иска одобряване на типа.“

29) Допълнение 1 се изменя, както следва:

а) съдържанието се изменя, както следва:

i) точка 2.63 се заменя със следното:

„2.63 Reserved for future use“;

ii) точка 2.78 се заменя със следното:

„2.78 GNSSAccumulatedDriving“;

iii) точка 2.79 се заменя със следното:

„2.79 GNSSAccumulatedDrivingRecord“;

iv) точка 2.111 се заменя със следното:

„2.111 NoOfGNSSADRecords“;

v) точка 2.160 се заменя със следното:

„2.160 Reserved for future use“;

vi) точка 2.203 се заменя със следното:

„2.203 VuGNSSADRecord“;

vii) точка 2.204 се заменя със следното:

„2.204 VuGNSSADRecordArray“;

viii) точка 2.230 се заменя със следното:

„2.230 Reserved for future use“;

ix) точка 2.231 се заменя със следното:

„2.231 Reserved for future use“;

б) в точка 2 преди точка 2.1 се добавя следният текст:

„Посоченият в настоящото допълнение размер за типовете карти за данни, които се използват за приложенията от поколение 1 и 2, е размерът за приложение от поколение 2. Предполага се, че четецът вече познава размера за приложение от поколение 1. Номерата на изискванията в приложение IB, свързани с тези типове данни, се отнасят за приложенията от поколение 1 и 2.“;

в) точка 2.19 се заменя със следното:

„2.19. **CardEventData**

Поколение 1:

Информация, съхранена на карта на водач или карта за монтаж и настройки и отнасяща се до събитията, свързани с титуляря на картата (изисквания в подточки 260 и 318 от приложение IB).

```
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).

Поколение 2:

Информация, съхранена на карта на водач или карта за монтаж и настройки и отнасяща се до събитията, свързани с титуляря на картата (изисквания в подточки 285 и 341 от приложение IB).

```
CardEventData ::= SEQUENCE SIZE(11) 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).“;

г) точка 2.30 се заменя със следното:

„2.30. **CardRenewalIndex**

Индекс за подновяване на валидността на картата (определение и).

```
CardRenewalIndex ::= IA5String(SIZE(1))
```

**Присвояване на стойност:** (вж. глава 7 от настоящото приложение).

„0“ Първо издаване.

Възходящ ред: „0, ..., 9, A, ..., Z“;

д) в точка 2.61 текстът след заглавието „Поколение 2“ се заменя със следното:

```
„DriverCardApplicationIdentification ::= SEQUENCE {
  typeOfTachographCardId      EquipmentType,
  cardStructureVersion        CardStructureVersion,
  noOfEventsPerType           NoOfEventsPerType,
  noOfFaultsPerType           NoOfFaultsPerType,
  activityStructureLength      CardActivityLengthRange,
  noOfCardVehicleRecords      NoOfCardVehicleRecords,
  noOfCardPlaceRecords        NoOfCardPlaceRecords,
  noOfGNSSADRecords           NoOfGNSSADRecords,
  noOfSpecificConditionRecords NoOfSpecificConditionRecords,
  noOfCardVehicleUnitRecords  NoOfCardVehicleUnitRecords
}
```

В допълнение към поколение 1 се използват следните елементи от данни:

**noOfGNSSADRecords** е броят на записите за общо управление по GNSS, които картата може да съхранява.

**noOfSpecificConditionRecords** е броят на записите за специфични условия, които картата може да съхранява.

**noOfCardVehicleUnitRecords** е броят на записите за използваните бордови устройства, които картата може да съхранява.“;

е) точка 2.63 се заменя със следното:

„2.63. **Reserved for future use**“;

ж) в точка 2.67 текстът под заглавието „Поколение 2“ се заменя със следното:

„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
--Driver Card (Sign) (17), --only to be used in the CHA
field of a signing certificate
--Workshop Card (Sign) (18), --only to be used in the CHA
field of a signing certificate
--Vehicle Unit (Sign) (19), --only to be used in the CHA
field of a signing certificate
--RFU (20..255)
```

*Забележка 1:* стойностите от поколение 2 за пластината, адаптера и външното устройство за 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.

*Забележка 2:* Приема се, че в полето CardHolderAuthorisation (CHA) в сертификат от поколение 2 стойностите (1), (2), и (6) означават сертификат за взаимно удостоверяване на автентичността за съответния вид оборудване. За обозначаване на съответния сертификат за създаване на цифров подпис трябва да се използват стойностите (17), (18) или (19).“;



з) в точка 2.70 текстът под заглавието „Поколение 2“ се заменя със следното:

„Поколение 2:

'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	Превिшаване на скоростта,
'08' H	Прекъсване на електрическото захранване,
'09' H	Грешка в данните за движението,
'0A' H	Конфликт относно движението на превозното средство,
'0B' H	Времеви конфликт (GNSS/вътрешния часовник на бордовото устройство),
'0C' H	Грешка в комуникацията с устройството за връзка от разстояние,
'0D' H	Липса на информация за местоположението от приемник на сигнали от GNSS,
'0E' H	Грешка в комуникацията с външното устройство за GNSS,
'0F' H	RFU,
'1x' H	Опити за нарушаване на сигурността, свързани с бордовото устройство,
'10' H	Няма допълнителна информация,
'11' H	Неуспешна процедура по удостоверяване на датчика за движение,
'12' H	Неуспешна процедура по удостоверяване на тахографската карта,
'13' H	Неразрешена смяна на датчика за движение,
'14' H	Грешка във връзка с целостта на входящите данни на картата
'15' H	Грешка във връзка с целостта на съхранените данни на потребител,
'16' H	Грешка при вътрешно прехвърляне на данни,
'17' H	Неразрешено отваряне на корпус,
'18' H	Възпрепятстване на работата на хардуера,
'19' H	Установяване на вмешателство във връзка с GNSS,
'1A' H	Неуспешна процедура по удостоверяване на външно устройство за GNSS,
'1B' H	Изтекъл сертификат на външно устройство за GNSS,
'1C' H to '1F' H	RFU,
'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 вътрешно прехвърляне на 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	Вътрешен приемник на сигнали от GNSS,
'37' H	Външно устройство за GNSS,
'38' H	Устройство за връзка от разстояние,
'39' H	Интерфейс с ITS,
'3A' 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.“;

и) точка 2.71 се заменя със следното:

#### „2.71. **ExtendedSealIdentifier**

Поколение 2:

Разширеният идентификатор на пломбата идентифицира еднозначно пломбата (съгласно изискването в подточка 401 от приложение IB).

```
ExtendedSealIdentifier ::= SEQUENCE {
    manufacturerCode      OCTET STRING (SIZE(2)),
    sealIdentifier        OCTET STRING (SIZE(8))
}
```

**manufacturerCode** е кодът на производителя на пломбата.

**sealIdentifier** е идентификатор за пломбата, който е уникален за производителя.“;

й) точки 2.78 и 2.79 се заменят със следното:

#### „2.78 **GNSSAccumulatedDriving**

Поколение 2:

Информация, съхранена на карта на водач или карта за монтаж и настройки и отнасяща се до местоположението на превозното средство по GNSS, ако общото време на управление на МПС достигне кратно число на три часа (съгласно изискванията в подточки 306 и 354 от приложение IB).

```
GNSSAccumulatedDriving := SEQUENCE {
    gnssADPointerNewestRecord    INTEGER(0..NoOfGNSSADRecords -1),
    gnssAccumulatedDrivingRecords SET SIZE(NoOfGNSSADRecords) OF
    GNSSAccumulatedDrivingRecord
}
```

**gnssADPointerNewestRecord** е индексът на последния актуализиран запис за общо управление по GNSS.

**Присвояване на стойност** е число, съответстващо на номератора на записа за общо управление по GNSS, като се започва с 0 за първия случай на запис за общо управление по GNSS в структурата.

**gnssAccumulatedDrivingRecords** е набор от записи, съдържащ датата и часа, когато общото управление на МПС достигне кратно число на три часа, и информация за местоположението на превозното средство.

#### 2.79. **GNSSAccumulatedDrivingRecord**

Поколение 2:

Информация, съхранена на карта на водач или карта за монтаж и настройки и отнасяща се до местоположението на превозното средство по GNSS, ако общото време на управление на МПС достигне кратно число на три часа (съгласно изискванията в подточки 305 и 353 от приложение IB).

```
GNSSAccumulatedDrivingRecord ::= SEQUENCE {
    timeStamp              TimeReal,
    gnssPlaceRecord       GNSSPlaceRecord,
    vehicleOdometerValue   OdometerShort
}
```

**timeStamp** е датата и часът, когато общото време на управление на МПС достигне кратно число на три часа.

**gnssPlaceRecord** съдържа информация за местоположението на превозното средство.

**vehicleOdometerValue** е стойността от километражния брояч, когато общото време на управление на МПС достигне кратно число на три часа.“;

к) точка 2.86 се заменя със следното:

**„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, тахографска карта или външно устройство за GNSS.

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.“;

л) точка 2.92 се заменя със следното:

**„2.92. MAC**

Поколение 2:

Сума за криптографски контрол с дължина от 8, 12 или 16 байта, съответстваща на криптографските повепиши, посочени в попълнение 11.

```
MAC ::= CHOICE {
    Mac8           OCTET STRING (SIZE(8)),
    Mac12          OCTET STRING (SIZE(12)),
    Mac16          OCTET STRING (SIZE(16)),
}“;
```

м) точка 2.111 се заменя със следното:

**„2.111. NoOfGNSSADRecords**

Поколение 2:

Брой на записите за общо управление по GNSS, които картата може да съхранява.

```
NoOfGNSSADRecords ::= INTEGER (0..216-1)
```

**Присвояване на стойност:** вж. допълнение 2.“;

н) в точка 2.120 присвояването на стойност „16H“ се заменя със следното:

„'16'H VuGNSSADRecord“;

о) точка 2.160 се заменя със следното:

**„2.160. Reserved for future use“;**

п) точка 2.162 се заменя със следното:

„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.“;

р) точка 2.179 се заменя със следното:

„2.179 **VuCardRecord**

Поколение 2:

Информация, съхранена в бордово устройство, относно използвана тахографска карта (съгласно изискването в подточка 132 от приложение IB).

```
VuCardRecord ::= SEQUENCE {
    cardNumberAndGenerationInformation      FullCardNumberAndGeneration,
    cardExtendedSerialNumber               ExtendedSerialNumber,
    cardStructureVersion                   CardStructureVersion,
    cardNumber                              CardNumber
}
```

**cardNumberAndGenerationInformation** е пълният номер и поколението на използваната карта (тип данни 2.74).

**cardExtendedSerialNumber** е от файла EF\_ICC под MF на картата.

**cardStructureVersion** е от файла EF\_Application\_Identification под DF\_Tachograph\_G2.

**cardNumber** е от файла EF\_Identification под DF\_Tachograph\_G2.“;

с) точки 2.203 и 2.204 се заменят със следното:

„2.203 **VuGNSSADRecord**

Поколение 2:

Информация, съхранена в бордово устройство и отнасяща се за местоположението на превозното средство по GNSS, ако общото време на управление на МПС достигне кратно число на три часа (съгласно изискванията в подточки 108 и 110 от приложение IB).

```
VuGNSSADRecord ::= SEQUENCE {
    timeStamp                               TimeReal,
    cardNumberAndGenDriverSlot              FullCardNumberAndGeneration,
    cardNumberAndGenCodriverSlot           FullCardNumberAndGeneration,
    gnssPlaceRecord                         GNSSPlaceRecord,
    vehicleOdometerValue                    OdometerShort
}
```

**timeStamp** е датата и часът, когато общото време на управление на МПС достигне кратно число на три часа.

**cardNumberAndGenDriverSlot** идентифицира картата, вкарана в процепата за водача, в т.ч. поколението ѝ.

**cardNumberAndGenCodriverSlot** идентифицира картата, вкарана в пропеца за втория водач, в т.ч. поколението ѝ.

**gnssPlaceRecord** съдържа информация за местоположението на превозното средство.

**vehicleOdometerValue** е стойността от километражния брояч, когато общото време на управление на МПС достигнекратно число на три часа.

#### 2.204. VuGNSSADRecordArray

Поколение 2:

Информация, съхранена в бордово устройство и отнасяща се за местоположението на превозното средство по GNSS, ако общото време на управление на МПС достигнекратно число на три часа (съгласно изискванията в подточки 108 и 110 от приложение IV).

```
VuGNSSADRecordArray ::= SEQUENCE {
    recordType                RecordType,
    recordSize                INTEGER(1..65535),
    noOfRecords               INTEGER(0..65535),
    records                   SET SIZE(noOfRecords) OF VuGNSSADRecord
}
```

**recordType** указва типа запис (VuGNSSADRecord).

**Присвояване на стойност:** вж. RecordType.

**recordSize** е размерът на VuGNSSADRecord в байтове.

**noOfRecords** е броят на записите в набора от записи.

**Records** е набор от записи за общо управление по GNSS.;

т) точки 2.230 и 2.231 се заменят със следното:

„2.230. Reserved for future use

2.231. Reserved for future use“;

у) в точка 2.234 текстът под заглавието „Поколение 2“ се заменя със следното:

```
„WorkshopCardApplicationIdentification ::= SEQUENCE {
    typeOfTachographCardId    EquipmentType,
    cardStructureVersion       CardStructureVersion,
    noOfEventsPerType          NoOfEventsPerType,
    noOfFaultsPerType          NoOfFaultsPerType,
    activityStructureLength     CardActivityLengthRange,
    noOfCardVehicleRecords     NoOfCardVehicleRecords,
    noOfCardPlaceRecords       NoOfCardPlaceRecords,
    noOfCalibrationRecords     NoOfCalibrationRecords,
    noOfGNSSADRecords          NoOfGNSSADRecords,
    noOfSpecificConditionRecords NoOfSpecificConditionRecords,
    noOfCardVehicleUnitRecords NoOfCardVehicleUnitRecords
}
```

В допълнение към поколение 1 се използват следните елементи от данни:

**noOfGNSSADRecords** е броят на записите за общо управление по GNSS, които картата може да съхранява.

**noOfSpecificConditionRecords** е броят на записите за специфични условия, които картата може да съхранява.

**noOfCardVehicleUnitRecords** е броят на записите за използваните бордови устройства, които картата може да съхранява.“

30) Допълнение 2 се изменя, както следва:

а) в точка 1.1 се добавят следните съкращения:

„CHA Certificate Holder Authorisation (разрешение за титуляря на сертификата)

DO Data Object (обект от данни)“;

б) точка 3.3 се изменя, както следва:

i) раздел TCS\_24 се заменя със следното:

„TCS\_24 Тези условия за сигурност 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. Изразът „не се прилага“ се използва, ако няма изискване да се поддържа изпълнението на командата. В този случай командата може да се поддържа или може да не се поддържа, но условието за достъп е извън обхват.“;

ii) таблицата в раздел TCS\_25 се заменя със следното:

„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

Команда	Карта на водач	Карта за монтаж и настройки	Контролна карта	Карта на превозвач
PERFORM 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“

iii) таблицата в раздел TCS\_26 се заменя със следното:

„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	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
PERFORM 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“

iv) таблицата в раздел TCS\_27 се заменя със следното:

„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
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
PERFORM HASH of FILE	Не се прилага	Не се прилага	Не се прилага	Не се прилага
PSO: Verify Certificate	ALW	ALW	ALW	ALW
PSO: Verify Digital Signature	Не се прилага	Не се прилага	Не се прилага	Не се прилага
Verify	Не се прилага	ALW	Не се прилага	Не се прилага“

v) в точка 3.4 раздел TCS\_29 се заменя със следното:

„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 оставшите опити, осигуряван от ‘X’



SW1	SW2	Значение
64	00	Грешка при изпълнението — непроменено състояние на енергонезависимата памет. Грешка в целостта 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	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)
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 (поправка 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

Може да бъдат върнати други байтове за състояние, определени в стандарт ISO/IEC 7816-4, ако поведението им не е изрично упоменато в настоящото допълнение.

Например по избор може да бъдат върнати следните байтове за състояние:

6881: Несъвместим логически канал

6882: Не се поддържа защитен обмен на съобщения“;

г) в точка 3.5.1.1, в раздел TCS\_38 последното тире се заменя със следното:

„— Ако избраното приложение се смята за повредено (открита е грешка в целостта на атрибутите на файла), за състоянието на обработката се връща **'6400'** или **'6500'**“;

д) в точка 3.5.1.2, в раздел TCS\_41 последното тире се заменя със следното:

„— Ако избраният файл се смята за повреден (открита е грешка в целостта на атрибутите на файла), за състоянието на обработката се връща **„6400“** или **„6500“**“;

е) в точка 3.5.2.1, в раздел TCS\_43 шестото тире се заменя със следното:

„— Ако е открита грешка в целостта на атрибутите на файла, картата счита файла за повреден и невъзстановим, а за състоянието на обработката се връща **„6400“** или **„6500“**“;

ж) точка 3.5.2.1.1 се изменя, както следва:

и) таблицата в раздел TCS\_45 се заменя със следното:

„Байт	Дължина	Стойност	Описание
#1	1	'81h'	T <sub>pv</sub> : таг за простата стойност на данните
#2	L	'NNh' или '81 NNh'	L <sub>pv</sub> : дължина на върнатите данни (= първоначална Le). L е 2 байта, ако L <sub>pv</sub> >127 байта
#(2+L) - #(1+L+NN)	NN	'XX...XXh'	Проста стойност на данните
#(2+L+NN)	1	'99h'	Таг за състоянието на обработката (SW1-SW2) — по избор за защитен обмен на съобщения от поколение 1
#(3+L+NN)	1	'02h'	Дължина на стойността за състоянието на обработката — по избор за защитен обмен на съобщения от поколение 1
#(4+L+NN) - #(5+L+NN)	2	'XX XXh'	Състояние на обработката на незащитената ответна APDU, т.е. с отговора — незадължително при защитен обмен на съобщения от поколение 1
#(6+L+NN)	1	'8Eh'	TCC: таг за криптографската контролна сума
#(7+L+NN)	1	'XXh'	LCC: дължина на следната криптографска контролна сума '04h' за защитения обмен на съобщения от поколение 1 (вж. допълнение 11, част А) '08h', '0Ch' или '10h' в зависимост от дължината на ключа по AES за защитен обмен на съобщения от поколение 2 (вж. допълнение 11, част Б)

„Байт	Дължина	Стойност	Описание
#(8+L+NN)-#(7+M+L+NN)	M	'XX..XXh'	Криптографска контролна сума
SW	2	'XXXXh'	Байтове за състоянието (SW1, SW2)“

ii) таблицата в раздел TCS\_46 се заменя със следното:

„Байт	Дължина	Стойност	Описание
#1	1	'87h'	TPI CG: таг за криптираните данни (криптограма)
#2	L	'MMh' или '81 MMh'	LPI CG: дължина на върнатите криптирани данни (различна от първоначалната Le на командата поради запълване). L е 2 байта, ако LPI 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 — по избор за защитен обмен на съобщения от поколение 1
#(4+L+MM) - #(5+L+MM)	2	'XX XXh'	Състояние на обработката на незащитената ответна APDU, т.е. с отговора — незадължително при защитен обмен на съобщения от поколение 1
#(6+L+MM)	1	'8Eh'	TCC: таг за криптографската контролна сума
#(7+L+MM)	1	'XXh'	LCC: дължина на следната криптографска контролна сума '04h' за защитения обмен на съобщения от поколение 1 (вж. допълнение 11, част А) '08h', '0Ch' или '10h' в зависимост от дължината на ключа по AES за защитен обмен на съобщения от поколение 2 (вж. 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)“

з) в точка 3.5.2.2, в раздел TCS\_50 шестото тире се заменя със следното:

„— Ако е открита грешка в целостта на атрибутите на файла, картата счита файла за повреден и невъзстановим, а за състоянието на обработката се връща „6400“ или „6500“.“;

и) в точка 3.5.2.3 раздел TCS\_52 се изменя, както следва:

i) последният ред в таблицата се заменя със следното:

„Le	1	'XXh'	Съгласно стандарта ISO/IEC 7816-4“
-----	---	-------	------------------------------------

ii) добавя се следното изречение:

„Ако  $T=0$ , картата приема за стойност на  $Le = '00h'$ , ако не се прилага защитен обмен на съобщения.

Ако  $T = 1$ , за състоянието на обработката се връща „6700“, ако  $Le='01h'$ .“;

й) в точка 3.5.2.3, в раздел TCS\_53 шестото тире се заменя със следното:

„— Ако е открита грешка в целостта на атрибутите на файла, картата счита файла за повреден и невъзстановим, а за състоянието на обработката се връща „6400“ или „6500“.“;

к) в точка 3.5.3.2, в раздел TCS\_63 шестото тире се заменя със следното:

„— Ако е открита грешка в целостта на атрибутите на файла, картата счита файла за повреден и невъзстановим, а за състоянието на обработката се връща „6400“ или „6500“.“;

л) в точка 3.5.5 раздел TCS\_72 се заменя със следното:

„TCS\_72 Въведеният от потребителя PIN трябва да е по стандарта ASCII за кодиране на символи и да е запълнен от IFD отлясно с байтове 'FFh' до дължина от 8 байта — вж. също в допълнение 1 за типа на данните WorkshopCardPIN.“;

м) в точка 3.5.8 раздел TCS\_95 се заменя със следното:

„TCS\_95 Ако командата INTERNAL\_AUTHENTICATE бъде изпълнена успешно, активният ключ на сесията от поколение 1, ако има такъв, се изтрива и повече не е наличен. За да има на разположение нов ключ на сесия от поколение 1, е необходимо да се изпълни успешно командата EXTERNAL AUTHENTICATE за механизма от поколение 1 за удостоверяване на автентичността.

*Забележка* За ключове за сесия от поколение 2 вж. допълнение 11, раздели CSM\_193 и CSM\_195. Ако бъдат установени ключове за сесия от поколение 2 и тахографската карта получи обикновена APDU за командата INTERNAL AUTHENTICATE, тя прекратява създаването на сесия за защитен обмен на съобщения от поколение 2 и унищожава ключовете за сесия от поколение 2.“;

н) в точка 3.5.9 раздел TCS\_97 се заменя със следното:

„TCS\_97 Вариантът на командата за механизма от второ поколение за взаимно удостоверяване на бордовото устройство и картата може да се изпълнява в MF, DF Tachograph и DF Tachograph\_G2, вж. също TCS\_34. Ако командата EXTERNAL AUTHENTICATE от поколение 2 бъде изпълнена успешно, активният ключ на сесията от поколение 1, ако има такъв, се изтрива и повече не е наличен.

*Забележка:* За ключове за сесия от поколение 2 вж. допълнение 11, раздели CSM\_193 и CSM\_195. Ако бъдат установени ключове за сесия от поколение 2 и тахографската карта получи обикновена APDU за командата EXTERNAL AUTHENTICATE, тя прекратява създаването на сесия за защитен обмен на съобщения от поколение 2 и унищожава ключовете за сесия от поколение 2.“;

о) в точка 3.5.10, в таблицата в раздел TCS\_101 се добавя следният ред:

„5 + L + 1	1	'00h'	Съгласно стандарта ISO/IEC 7816-4“
------------	---	-------	------------------------------------

п) в точка 3.5.11.2.3, в раздел TCS\_114 се добавят следните абзаци:

„— Ако currentAuthenticatedTime на картата е по-късно от датата, на която изтича срокът на валидност на избрания публичен ключ, за състоянието на обработката се връща „6A88“.

*Забележка:* Ако за командата за удостоверяване на автентичността на бордовото устройство (VU Authentication) се използва MSE: SET AT, указаният ключ е публичен ключ VU\_MA. Картата задава за използване публичния ключ VU\_MA, ако е наличен в паметта ѝ, като той съвпада с указанието за титуляря на сертификата (Certificate Holder Reference — CHR), посочено в полето за данни на командата (картата може да идентифицира публичните ключове VU\_MA чрез полето за CHA в сертификата). Ако е наличен само публичен ключ VU\_Sign или ако за бордовото устройство няма наличен публичен ключ, в отговор на тази команда картата връща „6A 88“. Вж. определението за полето CHA в допълнение 11 и за типа данни equipmentType в допълнение 1.

По същия начин, ако към контролната карта бъде изпратена команда MSE: SET DST с указание за оборудването EQT (т.е. бордово устройство или карта), в съответствие с раздел CSM\_234 указаният ключ винаги е ключ EQT\_Sign, който трябва да се използва за удостоверяване на цифровия подпис. В съответствие с фигура 13 в допълнение 11 контролната карта винаги съхранява съответния публичен ключ EQT\_Sign. В някои случаи контролната карта може да е съхранила съответния публичен ключ EQT\_MA. Винаги, когато получи командата MSE: SET DST, контролната карта задава за използване публичния ключ EQT\_Sign.“;

р) точка 3.5.13 се изменя, както следва:

i) раздел TCS\_121 се заменя със следното:

„TCS\_121 Временно съхраняваната хеш-стойност на файла се заличава, ако бъде изчислена нова хеш-стойност на файла посредством командата PERFORM HASH of FILE, ако бъде избран DF и ако тахографската карта бъде инициализирана.“;

ii) раздел TCS\_123 се заменя със следното:

„TCS\_123 Тахографското приложение от поколение 2 трябва да поддържа алгоритъма SHA-2 (SHA-256, SHA-384 или SHA-512), посочен в криптографската поредица в допълнение 11, част Б, за ключа за подпис на картата Card\_Sign.“;

iii) таблицата в раздел TCS\_124 се заменя със следното:

„Байт	Дължина	Стойност	Описание
CLA	1	'80h'	CLA
INS	1	'2Ah'	Извършване на операция, свързана със защитата от неразрешен достъп
P1	1	'90h'	Tag: Hash
P2	1	'00h'	Алгоритъм, известен по подразбиране За тахографското приложение от поколение 1: SHA-1 За тахографското приложение от поколение 2: алгоритъм SHA-2 (SHA-256, SHA-384 или SHA-512), определен в криптографската поредица в допълнение 11, част Б, за ключа за подпис на картата Card_Sign“

с) точка 3.5.14 се изменя, както следва:

текстът под заглавието и до раздел TCS\_126 се заменя със следното:

„Тази команда служи за изчисляване на цифровия подпис на изчислен преди това хеш-код (вж. PERFORM HASH of FILE, точка 3.5.13).

Само за картата на водач и за картата за монтаж и настройки 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. При тахографското приложение от поколение 2 само картата на водач и картата за монтаж и настройки имат ключ за подпис от поколение 2; другите карти не могат успешно да изпълнят командата и прекратяват изпълнението с подходящ код за грешка.

Тази команда може да е или да не е достъпна в MF. Ако командата не е достъпна в MF, нейното изпълнение се прекратява с подходящ код за грешка.

Тази команда е в съответствие със стандарт ISO/IEC 7816-8. Нейното използване е по-ограничено, отколкото съгласно посочения стандарт.“;

т) точка 3.5.15 се изменя, както следва:

i) таблицата в раздел TCS\_133 се заменя със следното:

„Байт	Дължина	Стойност	Описание
CLA	1	‘00h’	CLA
INS	1	‘2Ah’	Извършване на операция, свързана със защитата от неразрешен достъп
P1	1	‘00h’	
P2	1	‘A8h’	Таг: поле за данни, съдържащо съответните обекти от данни (DO) за проверката
Lc	1	‘XXh’	Дължина Lc на последващото поле за данни
#6	1	‘9Eh’	Таг за цифров подпис
#7 или #7-#8	L	‘NNh’ или ‘81 NNh’	Дължина на цифровия подпис (L е 2 байта, ако цифровият подпис е по-дълъг от 127 байта): 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 (вж. допълнение 11, част Б).
#(7+L)-#(6+L+NN)	NN	‘XX..XXh’	Съдържание на цифровия подпис“

ii) в раздел TCS\_134 се добавя следното тире:

„— Ако избраният публичен ключ (използван за проверка на въведения цифров подпис) има CHA.LSB (CertificateHolderAuthorisation.equipmentType), който не е подходящ за проверка на цифровия подпис съгласно допълнение 11, за състоянието на обработката се връща „6985“.“;

у) точка 3.5.16 се изменя, както следва:

i) в таблицата в раздел TCS\_138 се добавя следният ред:

„5 + L + 1	1	'00h'	Съгласно стандарта ISO/IEC 7816-4“
------------	---	-------	------------------------------------

ii) в раздел TCS\_139 се добавя следният абзац:

„— „6985“ указва, че времевият печат от 4 байта, посочен в полето за данни на командата, е по-ранен от cardValidityBegin или по-късен от cardExpiryDate.“;

ф) точка 4.2.2 се изменя, както следва:

i) в структурата на данните в раздел TCS\_154 редовете от DF Tachograph G2 до EF CardMA\_Certificate и редовете от EF GNSS\_Places до края на раздела се заменят със следното:

Файл / елемент на данни	Брой записи	Размер (байтове)		Стойности по подразбиране
		Мин.	Макс.	
└ DF Tachograph G2		20268	40316	
└└ EF Application_Identification		17	17	
└└└ DriverCardApplicationIdentification		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 00}
└└└└ noOfGNSSADRecords		2	2	{00 00}
└└└└ noOfSpecificConditionRecords		2	2	{00 00}
└└└└ noOfCardVehicleUnitRecords		2	2	{00 00}
└└ EF CardMA_Certificate		204	341	
...				
EF GNSS_Places	4538	6050		
└ GNSSContinuousDriving	4538	6050		
└└ gnssADPointerNewestRecord	2	2	{00 00}	
└└ gnssAccumulatedDrivingRecords	4536	6048		
└└└ GNSSContinuousDrivingRecord	n <sub>g</sub>	18	18	
└└└└ timeStamp		4	4	{00..00}
└└└└ gnssPlaceRecord		14	14	
└└└└└ timeStamp		4	4	{00..00}
└└└└└ gnssAccuracy		1	1	{00}
└└└└└ geoCoordinates		6	6	{00..00}
└└└└└ vehicleOdometerValue		3	3	{00..00}

ii) в таблицата в раздел TCS\_155 позицията NoOfGNSSCDRecords се заменя със следното:

„n <sub>8</sub> ”	NoOfGNSSADRecords	252	336“
-------------------	-------------------	-----	------

x) в точка 4.3.1 текстът за съкращение SC4 в раздел TCS\_156 се заменя със следното:

„**SC4** За командата READ BINARY с четен байт INS:

(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“;

ц) точка 4.3.2 се изменя, както следва:

i) в структурата на данните в раздел TCS\_162 редовете от DF Tachograph G2 до EF CardMA\_Certificate, редовете от EF Calibration до extendedSealIdentifier и редовете от EF GNSS\_Places до vehicleOdometerValue се заменят със следното:



”

Файл / елемент на данни	Брой записи	Размер (байтове)		Стойности по подразбиране
		Мин.	Макс.	
DF Tachograph_G2	1878		49787	
EF Application_Identification	19		19	
↳ WorkshopCardApplicationIdentificatio	19		19	
↳ 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 00}
↳ noOfCalibrationRecords	2		2	{00 00}
↳ noOfGNSSADRecords	2		2	{00 00}
↳ noOfSpecificConditionRecords	2		2	{00 00}
↳ noOfCardVehicleUnitRecords	2		2	{00 00}
EF CardMA_Certificate	204		341	
...				
EF Calibration		15668	45394	
↳ WorkshopCardCalibrationData		15668	45394	
↳ calibrationTotalNumber		2	2	{00 00}
↳ calibrationPointerNewestRecord		2	2	{00}
↳ calibrationRecords		15664	45390	
↳ WorkshopCardCalibrationRecord	n <sub>5</sub>	178	178	
↳ 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		56	56	
↳ noOfSealRecords		1	1	{00}
↳ SealRecords		55	55	
↳ SealRecord	5	11	11	
↳ equipmentType		1	1	{00}
↳ extendedSealIdentifier		10	10	{00..00}

...

EF	GNSS_Places		326	434	
	└ GNSSContinuousDriving		326	434	
	└ gnssADPointerNewestRecord		2	2	{00 00}
	└ gnssAccumulatedDrivingRecords		324	432	
	└┬ GNSSContinuousDrivingRecord	n <sub>8</sub>	18	18	
	└┬ timeStamp		4	4	{00..00}
	└┬ gnssPlaceRecord		14	14	
	└┬ timeStamp		4	4	{00..00}
	└┬ gnssAccuracy		1	1	{00}
	└┬ geoCoordinates		6	6	{00..00}
	└┬ vehicleOdometerValue		3	3	{00..00}

ii) в таблицата в раздел TCS\_163 позицията NoOfGNSSCDRecords се заменя със следното:

„n <sub>8</sub> “	NoOfGNSSADRecords	18	24“
-------------------	-------------------	----	-----

31) В допълнение 3 точка 2 се изменя, както следва:

a) след реда с пиктограмите „Местоположение в началото на дневния период на работа“ и „Местоположение в края на дневния период на работа“ се вмъква следният ред:

☞ ☒ местоположение след 3 часа общо време на управление на МПС“;

б) комбинацията от пиктограми „Сверяване на часовника (в сервиз)“ се заменя със следното:

⌚ ☒ Времеви конфликт или сверяване на часовника (в сервиз)“;

в) към списъка „Събития“ се добавят следните комбинации от пиктограми:

⌚ ☒ Липса на информация за местоположението от приемник на сигнали от GNSS или Грешка в комуникацията с външното устройство за GNSS;

! ⚡ Грешка в комуникацията с устройството за връзка от разстояние“.

32) Допълнение 4 се изменя, както следва:

a) точка 2 се изменя, както следва:

i) блок 11.4 се заменя със следното:

„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)  
 дължина на регистрираното местоположение  
 ширина на регистрираното местоположение  
 времеви печат в момента, когато е било определено местоположението  
 показание на километражния брояч

pihh:mm Cou Reg lon ±DDD°MM.M' lat ± DD°MM.M' hh:mm x xxx xxx km“
---

ii) блок 11.5 се заменя със следното:

„11.5 Местоположения след 3 часа общо време на управление на МПС  
ri=местоположение след 3 часа общо време на управление на МПС

час

дължина на регистрираното местоположение

ширина на регистрираното местоположение

времеви печат в момента, когато е било определено местоположението

показание на километражния брояч

```
pihh:mm
lon ± DDD°MM.M'
lat ± DD°MM.M '
hh:mm
x xxx xxx km"
```

б) в точка 3.1 позиция 11.5 във формата за ежедневната разпечатка на данните се заменя със следното:

„11.5	Местоположения след 3 часа общо време на управление на МПС в хронологичен ред“;
-------	---

в) в точка 3.2 форматът за ежедневната разпечатка на данните се заменя със следното:

„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 бордовото устройство (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 обсер“ 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 обсер“ 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 процеп на четящото устройство на водача
11.4	Въведени местоположения в хронологичен ред
11.5	Местоположения след 3 часа общо време на управление на МПС в хронологичен ред
11.7	Общо времетраене на всяка дейност
11.2	Справка за периодите без вкарана карта в процеп на четящото устройство на втория водач
11.4	Въведени местоположения в хронологичен ред
11.5	Местоположения след 3 часа общо време на управление на МПС в хронологичен ред

11.8	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	Местоположения след 3 часа общо време на управление на МПС в хронологичен ред
11.9	Общо времетраене на всяка дейност на този водач
13.1	Разграничител на данни за събития и неизправности
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
22.3	От час (празно място, където водач без карта посочва
22.4	До час периодите, валидни за него)
22.5	Подпис на водача“;

г) в точка 3.7 раздел PRT\_014 се заменя със следното:

„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	Последна карта, вкарана в бордовото устройство
23.1	Вкарани карти (до 88 записа)
12.3	Разграничител на данни за неизправности“.

33) Допълнение 7 се изменя, както следва:

а) точка 1.1 се заменя със следното:

#### „1.1. Обхват

Някои данни могат да бъдат изтеглени върху външно запамяващо устройство:

- от бордовото устройство чрез свързано към него специализирано интелигентно устройство (IDE),
- от тахографска карта чрез IDE, оборудвано с интерфейсно устройство за карта (IFD),
- през бордовото устройство от тахографска карта чрез IDE, свързано към бордовото устройство.

С цел да се даде възможност за проверка на автентичността и целостта на изтеглените данни, съхранени върху външно запамяващо устройство, те се придружават от подпис съгласно общите механизми за сигурност от допълнение 11. Изтеглят се също данните за идентификацията на изходното оборудване (бордово устройство или карта) и неговите сертификати за сигурност (държава членка и оборудване). Проверителят на данните трябва да притежава свой собствен защитен европейски публичен ключ.

Данните, изтеглени от бордовото устройство, се подписват съгласно общите механизми за сигурност от допълнение 11, част Б (тахографска система от второ поколение), освен когато проверката на водача се извършва от контролен орган на държава извън ЕС с контролна карта от първо поколение; в тези случаи данните се подписват съгласно общите механизми за сигурност от допълнение 11, част А (тахографска система от първо поколение) в съответствие с изискванията в раздел MIG\_015 от допълнение 15 — „Миграция“.

За тази цел в посоченото допълнение се предвиждат два типа изтегляния на данни от бордовото устройство:

- изтегляне на данни от бордово устройство от поколение 2 със структура на данните от поколение 2, като данните се подписват съгласно общите механизми за сигурност от допълнение 11, част Б,
- изтегляне на данни от бордово устройство от поколение 1 със структура на данните от поколение 1, като данните се подписват съгласно общите механизми за сигурност от допълнение 11, част А.

По същия начин съществуват и два типа данни, изтеглени от карта на водач от второ поколение, вкарана в бордовото устройство, както се посочва в параграфи 3 и 4 от настоящото допълнение.“;

б) точка 2.2.2 се изменя, както следва:

i) таблицата се заменя със следното:

„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
Transfer Data Request									
Overview		80	EE	F0	02	36	01 or 21		97
Activities		80	EE	F0	06	36	02 or 22	Date	CS
Events & Faults		80	EE	F0	02	36	03 or 23		99
Detailed Speed		80	EE	F0	02	36	04 or 24		9A
Technical Data		80	EE	F0	02	36	05 or 25		9B
Card download		80	EE	F0	02	36	06	Slot	CS

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
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"

ii) към забележките след таблицата се добавят следните тирета:

„— TRTP 21 — 25 се използват за заявки за изтегляне на данни от бордово устройство от поколение 2; TRTP 01 — 05 се използват за заявки за изтегляне на данни от бордово устройство от поколение 1, които бордовото устройство може да приеме само при проверка на водача, която се извършва от контролен орган на държава извън ЕС с контролна карта от първо поколение,

— TRTP 11 — 19 и 31 — 39 са запазени за заявки за специфични изтегляния на данни от производителя.“;

в) точка 2.2.2.9 се изменя, както следва:

i) раздел DDP\_011 се заменя със следното:

„DDP\_011 IDE изпраща Transfer Data Request, за да уточни за бордовото устройство вида на данните, които трябва да се изтеглят. Transfer Request Parameter (TRTP) на определен байт показва типа трансфер.

Съществуват шест типа трансфер на данни. За изтегляне на данни от бордовото устройство за всеки тип трансфер могат да се използват две различни стойности на TRTP:

Тип трансфер на данни	Стойност на TRTP при изтегляне на данни от бордово устройство от поколение 1	Стойност на TRTP при изтегляне на данни от бордово устройство от поколение 2
Overview	01	21
Activities of a specified date	02	22
Events and faults	03	23
Detailed speed	04	24
Technical data	05	25

Тип трансфер на данни	Стойност на TRTP
Card download	06“

ii) раздел DDP\_054 се заменя със следното:

„DDP\_054 За IDE е задължително да заяви overview data transfer (TRTP 01 или 21) по време на сесия за изтегляне на данни, защото единствено това гарантира, че сертификатите на бордовото устройство се регистрират в изтегления файл (и това позволява проверката на цифровия подпис).

Във втория случай (TRTP 02 или 22) съобщението Transfer Data Request съдържа указание за календарния ден (формат TimeReal), чиито данни трябва да се изтеглят.“;

г) в точка 2.2.2.10 раздел DDP\_055 се заменя със следното:

„DDP\_055 В първия случай (TREP 01 или 21) бордовото устройство ще изпрати данни, предназначени да помогнат на потребителя на IDE при избора на данните, които иска да изтегли. Съобщението съдържа следната информация:

- сертификати за сигурност,
- идентификация на превозното средство,
- актуалната дата и час на бордовото устройство,
- най-ранната и най-късната дата за изтегляне на данните (данни от бордовото устройство),
- указване за наличието на карти в бордовото устройство,
- предишни изтеглени данни към превозвач,
- блокировки от страна на превозвача,
- предишни проверки.“;

д) в точка 2.2.2.16, в раздел DDP\_018 последното тире се заменя със следното:

„— Данни FA, които не са на разположение

Обектът от данни на заявка за трансфер на данни не е достъпен в бордовото устройство (например не е поставена карта; получената заявка за изтегляне на данни от бордовото устройство от поколение 1 не е при проверка на водача от контролен орган на държава извън ЕС...)“;

е) точка 2.2.6.1 се изменя, както следва:

i) в раздел DDP\_029 първият абзац се заменя със следното:

„Полего за данни на съобщението „Positive Response Transfer Data Overview“ трябва да дава данните по-долу по следния ред по SID 76 Hex, TREP 01 или 21 Hex и съответните критерии за разделяне и преброяване на подсъобщенията.“;

ii) заглавието „Структура на данните от поколение 1“ се заменя със следното:

„Структура на данните от поколение 1 (TREP 01 Hex)“;

iii) заглавието „Структура на данните от поколение 2“ се заменя със следното:

„Структура на данните от поколение 2 (TREP 21 Hex)“;

ж) точка 2.2.6.2 се изменя, както следва:

i) в раздел DDP\_030 първият абзац се заменя със следното:

„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 или 22 Hex и съответните критерии за разделяне и преброяване на подсъобщенията:“;

ii) заглавието „Структура на данните от поколение 1“ се заменя със следното:

„Структура на данните от поколение 1 (TREP 02 Hex)“;

iii) заглавието „Структура на данните от поколение 2“ се заменя със следното:

„Структура на данните от поколение 2 (TREP 22 Hex)“;

iv) позицията VuGNSSCDRecordArray под заглавието „Структура на данните от поколение 2 (TREP 22 Hex)“ се заменя със следното:

„VuGNSSADRecordArray

Местоположения на превозното средство по GNSS, когато общото време на управление на МПС достигнекратно число на три часа. Ако тази част е празна, се изпраща заглавна част на масив с noOfRecords = 0.“

з) точка 2.2.6.3 се изменя, както следва:

i) в раздел DDP\_031 първият абзац се заменя със следното:

„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 или 23 Hex и съответните критерии за разделяне и преброяване на подсъобщенията:“;

ii) заглавието „Структура на данните от поколение 1“ се заменя със следното:

„Структура на данните от поколение 1 (TREP 03 Hex)“;

iii) заглавието „Структура на данните от поколение 2“ се заменя със следното:

„Структура на данните от поколение 2 (TREP 23 Hex)“;

iv) позицията VuTimeAdjustmentGNSSRecordArray под заглавието „Структура на данните от поколение 2 (TREP 23 Hex)“ се заличава;

и) точка 2.2.6.4 се изменя, както следва:

i) в раздел DDP\_032 първият абзац се заменя със следното:

„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 или 24 Hex и съответните критерии за разделяне и преброяване на подсъобщенията:“;



ii) заглавието „Структура на данните от поколение 1“ се заменя със следното:

„Структура на данните от поколение 1 (TREP 04)“;

iii) заглавието „Структура на данните от поколение 2“ се заменя със следното:

„Структура на данните от поколение 2 (TREP 24)“;

й) точка 2.2.6.5 се изменя, както следва:

i) в раздел DDP\_033 първият абзац се заменя със следното:

„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 или 25 Hex и съответните критерии за разделяне и преброяване на подсъобщенията:“;

ii) заглавието „Структура на данните от поколение 1“ се заменя със следното:

„Структура на данните от поколение 1 (TREP 05)“;

iii) заглавието „Структура на данните от поколение 2“ се заменя със следното:

„Структура на данните от поколение 2 (TREP 25)“;

к) в точка 3.3 раздел DDP\_035 се заменя със следното:

„DDP\_035 Изтеглянето на данни от тахографска карта съдържа следните операции:

- изтегляне на общата информация на картата в EF ICC и IC. Тази информация е незащитена и не е защитена с цифров подпис;
- (за тахографски карти от първо и второ поколение) изтегляне на EF в рамките на Tachograph DF:

- изтегляне на EF Card\_Certificate и CA\_Certificate. Тази информация не е защитена с цифров подпис.

Тези файлове трябва задължително да се изтеглят за всяка сесия за изтегляне на данни;

- изтегляне на останалите елементарни файлове с приложни данни (в рамките на Tachograph DF) освен EF Card\_Download. Тази информация е защитена с цифров подпис съгласно общите механизми за сигурност от допълнение 11, част А;

- задължително е да се изтеглят поне Application\_Identification и Identification за всяка сесия за изтегляне на данни;

- когато се извършва изтегляне на данни от карта на водач, е задължително също да се изтеглят следните EF:

- Events\_Data,

- Faults\_Data,

- Driver\_Activity\_Data,
  - Vehicles\_Used,
  - Places,
  - Control\_Activity\_Data,
  - Specific\_Conditions,
- (само за тахографски карти от второ поколение) с изключение на случаите, когато изтеглянето на данни от карта на водач, вкарана в бордовото устройство, се извършва при проверка на водача от контролен орган на държава извън ЕС с контролна карта от първо поколение, изтегляне на EF в рамките на Tachograph\_G2 DF:

- изтегляне на EF CardSignCertificate, CA\_Certificate и Link\_Certificate (ако е наличен). Тази информация не е защитена с цифров подпис.

Тези файлове трябва задължително да се изтеглят за всяка сесия за изтегляне на данни;

- изтегляне на останалите елементарни файлове с приложни данни (в рамките на Tachograph\_G2 DF) освен EF Card\_Download. Тази информация е защитена с цифров подпис съгласно общите механизми за сигурност от допълнение 11, част Б.
- задължително е да се изтеглят поне EF Application\_Identification и Identification за всяка сесия за изтегляне на данни;
- когато се извършва изтегляне на данни от карта на водач, е задължително също да се изтеглят следните EF:

- Events\_Data,
- Faults\_Data,
- Driver\_Activity\_Data,
- Vehicles\_Used,
- Places,
- Control\_Activity\_Data,
- Specific\_Conditions,
- VehicleUnits\_Used,
- GNSS Places.

- когато се извършва изтегляне на данни от карта на водач, трябва да се актуализира датата на LastCardDownload в EF Card\_Download, както и в Tachograph и ако е уместно — в DF Tachograph\_G2 .
- когато се извършва изтегляне на данни от карта за монтаж и настройки, трябва да се инициализира броячът за калибриране в EF Card\_Download, както и в Tachograph и ако е уместно — в DF Tachograph\_G2 .

— когато се изтеглят данни от карта за монтаж и настройки, не трябва да се изтеглят данните от `Sensor_Installation_Data` в `Tachograph` и ако е уместно — в `DF Tachograph_G2` .“;

л) в точка 3.3.2, в раздел `DDP_037` първият абзац се заменя със следното:

„Последователността за изтегляне на данни от `EF ICC`, `IC`, `Card_Certificate` (или `CardSignCertificate` за `DF Tachograph_G2`), `CA_Certificate` и `Link_Certificate` (само за `DF Tachograph_G2`) е, както следва:“;

м) таблицата в точка 3.3.3 се заменя със следното:

„Карта	Посока	IDE/IFD	Значение/Забележки
	←	<b>Select File</b>	
<b>ОК</b>	⇒		
	←	<b>Perform Hash of File</b>	— Позволява да се изчисли хеш-стойността по отношение на съдържанието на избрания файл, като се използва хеш-алгоритъмът, посочен в допълнение 11, част А или Б. Това не е команда ISO.
Изчислява се Hash of File и временно се съхранява хеш-стойността			
<b>ОК</b>	⇒		
	←	<b>Read Binary</b>	Ако файлът съдържа повече данни от капацитета на буферната памет на четящото устройство или картата, командата трябва да се повтори, докато се прочете целият файл.
<b>Данни от файла ОК</b>	⇒	Получените данни се съхраняват върху ESM	Съгласно 3.4. Формат за съхранение на данните
	←	<b>PSO: Compute Digital Signature</b>	
Изпълнение на операция за сигурност „Compute Digital Signature“, като се използва временно съхранената хеш-стойност			
<b>Подпис ОК</b>	⇒	Добавяне на данни към тези, които са съхранени преди това върху ESM	съгласно 3.4. Формат за съхранение на данните“

н) в точка 3.4.2 раздел DDP\_046 се заменя със следното:

„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) в Tachograph или за общата информация на картата	3 байта
FID (2 байта)    „01“	Таг за подпис на EF (FID) в DF Tachograph	3 байта
FID (2 байта)    „02“	Таг за EF (FID) в DF Tachograph_G2	3 байта
FID (2 байта)    „03“	Таг за подпис на EF (FID) в DF Tachograph_G2	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 (в DF Tachograph)
05 05 01	00 80	Подпис на EF Vehicles_Used (в DF Tachograph)
05 05 02	0A 2E	Данни от EF Vehicles_Used в DF Tachograph_G2
05 05 03	xx xx	Подпис на EF Vehicles_Used в DF Tachograph_G2 “

о) в точка 4 раздел DDP\_049 се заменя със следното:

„DDP\_049 Карти на водач от първо поколение: Данните трябва да се изтеглят, като се използва протоколът за изтегляне на данни от първо поколение, и изтеглените данни трябва да са със същия формат като данните, изтеглени от бордово устройство от първо поколение.

Карти на водач от второ поколение: Тогава бордовото устройство 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“.

34) В допълнение 8, точка 2 текстът под заглавието „Справочни материали“ се заменя със следното:

„ISO 14230-2: Пътни превозни средства. Системи за диагностика. Протокол „Keyword 2000“. Част 2: канален слой.

Първо издание: 1999 г.“

35) Допълнение 9 се изменя, както следва:

а) точка 6 в съдържанието се заменя със следното:

„6. ИЗПИТВАНИЯ НА ВЪНШНОТО УСТРОЙСТВО ЗА ВРЪЗКА ОТ РАЗСТОЯНИЕ“;

б) в точка 1.1 първото тире се заменя със следното:

„— **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“;

в) таблицата за функционални изпитвания на бордовото устройство в точка 2 се заменя със следното:

„№	Изпитване	Описание	Съответни изисквания
<b>1</b>	<b>Административен преглед</b>		
1.1	Документиране	Правилност на документацията	
1.2	Резултати от изпитване, проведено от производителя	Резултати от изпитване при интегриране, проведено от производителя Писмени демонстрации.	88, 89, 91
<b>2</b>	<b>Визуално инспектиране</b>		
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		
<b>3</b>	<b>Функционални изпитвания</b>		
3.1	Осигурявани функции		02, 03, 04, 05, 07, 382
3.2	Режими на работа		09 до 11*, 134, 135
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*, 134
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, 134
3.8	Следене на състоянието при управление на МПС		54, 55, 134
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, 134

„№	Изпитване	Описание	Съответни изисквания
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		136, 137, 138*, 139*, 141*, 142, 143 144, 145, 146*, 147*, 148*, 149, 150
3.28	Показване върху дисплея		90, 134, 151 до 168, PIC_001, DIS_001
3.29	Разпечатване		90, 134, 169 до 181, PIC_001, PRT_001 до PRT_014
3.30	Предупреждаване		134, 182 до 191, PIC_001
3.31	Изтегляне на данни към външни носители		90, 134, 192 до 196
3.32	Връзка от разстояние за извършване на целенасочени пътни проверки		197 до 199
3.33	Данни, прехвърляни към допълнителни външни устройства		200, 201
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

„№	Изпитване	Описание	Съответни изисквания
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 събитие(ята) 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 (cipher suite) и стандартизирани домейн параметри		CSM_48, CSM_50
<b>4</b>	<b>Изпитвания за въздействията на околната среда</b>		
4.1	Температура	<p>Проверяват се функционалните възможности чрез следните изпитвания:</p> <p>Изпитване съгласно ISO 16750-4, глава 5.1.1.2: Изпитване за работа при ниска температура (72 часа при <math>-20\text{ }^{\circ}\text{C}</math>)</p> <p>Това изпитване е с позоваване на IEC 60068-2-1: Изпитване на въздействия на околната среда — Част 2-1: Изпитвания — Изпитване А: Студ</p> <p>Изпитване съгласно ISO 16750-4: глава 5.1.2.2: Изпитване за работа при висока температура (72 часа при <math>70\text{ }^{\circ}\text{C}</math>)</p> <p>Това изпитване е с позоваване на IEC 60068-2-2: Основни процедури за изпитване на въздействия на околната среда; Част 2: Изпитвания; Изпитвания В: Суха топлина</p> <p>Изпитване съгласно ISO 16750-4: Глава 5.3.2: Бърза промяна на температурата при зададена продължителност на прехода (<math>-20\text{ }^{\circ}\text{C}/70\text{ }^{\circ}\text{C}</math>, 20 цикъла, време на задържане при всяка от температурите 2 часа)</p> <p>Възможно е да се проведат намален набор изпитвания (измежду посочените в раздел 3 от настоящата таблица) съответно при ниските температури, високите температури и температурните цикли</p>	213
4.2	Влажност	<p>Проверява се, че бордовото устройство може да понесе циклично изпитване на топлина във влажна среда съгласно IEC 60068-2-30, изпитване Db, с шест цикъла по 24 часа, като във всеки от тях температурата се изменя от <math>+25\text{ }^{\circ}\text{C}</math> до <math>+55\text{ }^{\circ}\text{C}</math> и относителната влажност е съответно 97 % при <math>+25\text{ }^{\circ}\text{C}</math> и 93 % при <math>+55\text{ }^{\circ}\text{C}</math></p>	214
4.3	Механични въздействия	<p>1. Синусоидални вибрации.</p> <p>Проверява се, че бордовото устройство може да понесе синусоидални вибрации със следните характеристики:</p> <p>постоянно изместване, при честота между 5 и 11 Hz: максимум 10 mm</p> <p>постоянно ускорение, при честота между 11 и 300 Hz: 5 g</p> <p>Съответствието с това изискване се проверява чрез изпитване Fc по IEC 60068-2-6, с минимално времетраене на изпитването <math>3 \times 12</math> часа (по 12 часа на координатна ос)</p> <p>Стандартът ISO 16750-3 не изисква да се провежда изпитване със синусоидални вибрации за устройства, намиращи се в отделна кабина на превозното средство.</p>	219

„№	Изпитване	Описание	Съответни изисквания
		<p>2. Случайни вибрации:</p> <p>Изпитване съгласно ISO 16750-3: глава 4.1.2.8: Изпитване VIII: Търговски превозни средства с отделна кабина</p> <p>Изпитване за случайни вибрации, 10...2000 Hz, вертикално средноквадратично отклонение <math>21,3 \text{ m/s}^2</math>, надлъжно средноквадратично отклонение <math>11,8 \text{ m/s}^2</math>, напречно средноквадратично отклонение <math>13,1 \text{ m/s}^2</math>, 3 оси, по 32 часа за ос, включително температурен цикъл – 20...70 °C.</p> <p>Това изпитване е с позоваване на IEC 60068-2-64: Изпитване на въздействия на околната среда — Част 2-64: Изпитвания — Изпитване Gh: Вибрации, широколентови случайни, и указания</p> <p>3. Удари:</p> <p>механичен удар с ускорение 3 g, полусинусоидален, съгласно ISO 16750.</p> <p>Гореописаните изпитвания се извършват върху различни мостри на изпитваните съоръжения.</p>	
4.4	Защита срещу проникване на вода и чужди тела	Изпитване съгласно ISO 20653: Пътни превозни средства. Степен на защита (IP код). Защита на електрическото оборудване срещу проникване на чужди тела, 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 напрежение 24 V: 34 V при + 40 °C в продължение на 1 час при варианти за напрежение 12 V: 17 V при + 40 °C в продължение на 1 час: при варианти за напрежение 12 V: 17 V при + 40 °C в продължение на 1 час (ISO 16750-2)	216
4.6	Защита срещу включване с обратна полярност	Проверява се, че бордовото устройство може да издържи на размяна на полюсите на електрическото му захранване (ISO 16750-2)	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)	216
<b>5</b>	<b>Изпитване за електромагнитна съвместимост (EMC)</b>		
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



„№	Изпитване	Описание	Съответни изисквания
5.3	Чувствителност към преходни процеси по проводниците на захранването	<p>При варианти за напрежение 24 V: съответствие със стандарт ISO 7637-2 + Правило № 10 на ИКЕ на ООН, Преработка 3:</p> <p>импулс 1a: <math>V_s = -450\text{ V}</math>, <math>R_i = 50\ \Omega</math></p> <p>импулс 2a: <math>V_s = +37\text{ V}</math>, <math>R_i = 2\ \Omega</math></p> <p>импулс 2b: <math>V_s = +20\text{ V}</math>, <math>R_i = 0,05\ \Omega</math></p> <p>импулс 3a: <math>V_s = -150\text{ V}</math>, <math>R_i = 50\ \Omega</math></p> <p>импулс 3b: <math>V_s = +150\text{ V}</math>, <math>R_i = 50\ \Omega</math></p> <p>импулс 4: <math>V_s = -16\text{ V}</math>, <math>V_a = -12\text{ V}</math>, <math>t_6 = 100\text{ ms}</math></p> <p>импулс 5: <math>V_s = +120\text{ V}</math>, <math>R_i = 2,2\ \Omega</math>, <math>t_d = 250\text{ ms}</math></p> <p>При варианти за напрежение 12 V: съответствие със стандарт ISO 7637-1 + Правило № 10 на ИКЕ на ООН, Преработка 3:</p> <p>импулс 1: <math>V_s = -75\text{ V}</math>, <math>R_i = 10\ \Omega</math></p> <p>импулс 2a: <math>V_s = +37\text{ V}</math>, <math>R_i = 2\ \Omega</math></p> <p>импулс 2b: <math>V_s = +10\text{ V}</math>, <math>R_i = 0,05\ \Omega</math></p> <p>импулс 3a: <math>V_s = -112\text{ V}</math>, <math>R_i = 50\ \Omega</math></p> <p>импулс 3b: <math>V_s = +75\text{ V}</math>, <math>R_i = 50\ \Omega</math></p> <p>импулс 4: <math>V_s = -6\text{ V}</math>, <math>V_a = -5\text{ V}</math>, <math>t_6 = 15\text{ ms}</math></p> <p>импулс 5: <math>V_s = +65\text{ V}</math>, <math>R_i = 3\ \Omega</math>, <math>t_d = 100\text{ ms}</math></p> <p>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</p> <p>За примерни стойности на повишено напрежение вследствие разкачане на акумулаторната батерия при зареждащ я алтернатор, вж. стандарт ISO 16750-2, 4-то издание, глава 4.6.4.</p>	218“

г) точка 6 се заменя със следното:

„6. ИЗПИТВАНИЯ НА ВЪНШНОТО УСТРОЙСТВО ЗА ВРЪЗКА ОТ РАЗСТОЯНИЕ

№	Изпитване	Описание	Съответни изисквания
1.	<b>Административен преглед</b>		
1.1	Документиране	Правилност на документацията	
2.	<b>Визуално инспектиране</b>		
2.1.	Съответствие с документацията		
2.2.	Идентификация/маркировки		225, 226
2.3	Материали		219 до 223
3.	<b>Функционални изпитвания</b>		
3.1	Връзка от разстояние за извършване на целенасочени пътни проверки		4, 197 до 199

№	Изпитване	Описание	Съответни изисквания
3.2	Записване и съхраняване на данните в паметта		91
3.3	Връзка с бордовото устройство		Допълнение 14, раздели DSC_66 до DSC_70 и DSC_71 до DSC_76
4.	<b>Изпитвания за въздействията на околната среда</b>		
4.1	Температура	<p>Проверяват се функционалните възможности чрез следните изпитвания:</p> <p>Изпитване съгласно ISO 16750-4, глава 5.1.1.2: Изпитване за работа при ниска температура (72 часа при <math>-20\text{ }^{\circ}\text{C}</math>)</p> <p>Това изпитване е с позоваване на IEC 60068-2-1: Изпитване на въздействия на околната среда — Част 2-1: Изпитвания — Изпитване А: Студ</p> <p>Изпитване съгласно ISO 16750-4: глава 5.1.2.2: Изпитване за работа при висока температура (72 часа при <math>70\text{ }^{\circ}\text{C}</math>)</p> <p>Това изпитване е с позоваване на IEC 60068-2-2: Основни процедури за изпитване на въздействия на околната среда; Част 2: Изпитвания; Изпитвания В: Суха топлина</p> <p>Изпитване съгласно ISO 16750-4: Глава 5.3.2: Бърза промяна на температурата при зададена продължителност на прехода (<math>-20\text{ }^{\circ}\text{C}/70\text{ }^{\circ}\text{C}</math>, 20 цикъла, време на задържане при всяка от температурите 1 час)</p> <p>Възможно е да се проведат намален набор изпитвания (измежду посочените в раздел 3 от настоящата таблица) съответно при ниските температури, високите температури и температурните цикли</p>	213
4.2	Защита срещу проникване на вода и чужди тела	Изпитване съгласно ISO 20653: Пътни превозни средства. Степен на защита (IP код). Защита на електрическото оборудване срещу проникване на чужди тела, вода и достъп (целева стойност IP40)	220, 221
5	<b>Изпитание за електромагнитна съвместимост (EMC)</b>		
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: $\pm 4\text{ kV}$ за контактен разряд и $\pm 8\text{ kV}$ за разряд през въздух	218

№	Изпитване	Описание	Съответни изисквания
5.3	Чувствителност към преходни процеси по проводниците на захранването	<p>При варианти за напрежение 24 V: съответствие със стандарт ISO 7637-2 + Правило № 10 на ИКЕ на ООН, Преработка 3:</p> <p>импулс 1a: <math>V_s = -450\text{ V}</math>, <math>R_i = 50\ \Omega</math></p> <p>импулс 2a: <math>V_s = +37\text{ V}</math>, <math>R_i = 2\ \Omega</math></p> <p>импулс 2b: <math>V_s = +20\text{ V}</math>, <math>R_i = 0,05\ \Omega</math></p> <p>импулс 3a: <math>V_s = -150\text{ V}</math>, <math>R_i = 50\ \Omega</math></p> <p>импулс 3b: <math>V_s = +150\text{ V}</math>, <math>R_i = 50\ \Omega</math></p> <p>импулс 4: <math>V_s = -16\text{ V}</math>, <math>V_a = -12\text{ V}</math>, <math>t_6 = 100\text{ ms}</math></p> <p>импулс 5: <math>V_s = +120\text{ V}</math>, <math>R_i = 2,2\ \Omega</math>, <math>t_d = 250\text{ ms}</math></p> <p>При варианти за напрежение 12 V: съответствие със стандарт ISO 7637-1 + Правило № 10 на ИКЕ на ООН, Преработка 3:</p> <p>импулс 1: <math>V_s = -75\text{ V}</math>, <math>R_i = 10\ \Omega</math></p> <p>импулс 2a: <math>V_s = +37\text{ V}</math>, <math>R_i = 2\ \Omega</math></p> <p>импулс 2b: <math>V_s = +10\text{ V}</math>, <math>R_i = 0,05\ \Omega</math></p> <p>импулс 3a: <math>V_s = -112\text{ V}</math>, <math>R_i = 50\ \Omega</math></p> <p>импулс 3b: <math>V_s = +75\text{ V}</math>, <math>R_i = 50\ \Omega</math></p> <p>импулс 4: <math>V_s = -6\text{ V}</math>, <math>V_a = -5\text{ V}</math>, <math>t_6 = 15\text{ ms}</math></p> <p>импулс 5: <math>V_s = +65\text{ V}</math>, <math>R_i = 3\ \Omega</math>, <math>t_d = 100\text{ ms}</math></p> <p>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</p> <p>За примерни стойности на повишено напрежение вследствие разкачане на акумулаторната батерия при зареждащ я алтернатор, вж. стандарт ISO 16750-2, 4-то издание, глава 4.6.4.</p>	218“

д) таблицата за оперативна съвместимост в точка 8 се заменя със следното:

„№	Изпитване	Описание
8.1 Изпитвания за оперативна съвместимост между бордови устройства и тахографски карти		
1	Взаимно удостоверяване на автентичност	Проверява се дали взаимното удостоверяване на автентичност между бордовото устройство и тахографската карта протича нормално
2	Изпитвания за четене /записване	<p>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</p> <p>Чрез изтегляне на данните от бордовото устройство се проверява дали всички съответни записи са направени правилно.</p> <p>Чрез изтегляне на данните от картата се проверява дали всички съответни записи са направени правилно.</p> <p>Чрез дневни разпечатки се проверява дали всички съответни записи могат да бъдат прочетени правилно.</p>

„№	Изпитване	Описание
8.2 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	<p>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.</p> <p>Чрез изтегляне на данните от бордовото устройство се проверява дали всички съответни записи са направени правилно.</p> <p>Чрез изтегляне на данните от картата се проверява дали всички съответни записи са направени правилно.</p> <p>Чрез дневна разпечатка се проверява дали всички съответни записи могат да бъдат прочетени правилно.</p>

8.3 Изпитвания за оперативна съвместимост между бордови устройства и външни устройства за GNSS (когато има такива)

1	Взаимно удостоверяване на автентичност	Проверява се дали взаимното удостоверяване на автентичност (свързване) между бордовото устройство и външното устройство за GNSS протича нормално.
2	Изпитвания на действието	<p>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.</p> <p>Чрез изтегляне на данните от бордовото устройство се проверява дали всички съответни записи са направени правилно.</p> <p>Чрез изтегляне на данните от картата се проверява дали всички съответни записи са направени правилно.</p> <p>Чрез дневна разпечатка се проверява дали всички съответни записи могат да бъдат прочетени правилно.“</p>

36) Допълнение 11 се изменя, както следва:

а) в точка 8.2.3 раздел CSM\_49 се заменя със следното

„CSM\_49 Бордовите устройства, тахографските карти и външните устройства за GNSS трябва да поддържат алгоритмите SHA-256, SHA-384 и SHA-512, специфицирани в [SHS].“;

б) в точка 9.1.2, в раздел CSM\_58 първият абзац се заменя със следното:

„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. Срокът на валидност на свързващия сертификат е 17 години и 3 месеца. Това е показано също на фигура 1 в раздел 9.1.7.“;

в) в точка 9.1.4 раздел CSM\_72 се заменя със следното

„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, генериралата ключовете страна трябва да изпрати публичния ключ на своя MSCA, за да получи съответен сертификат за бордовото устройство, подписан от MSCA. Частният ключ трябва да се използва само от бордовото устройство.“;

г) точка 9.1.5 се изменя, както следва

i) раздел CSM\_83 се заменя със следното:

„CSM\_83 За всяка тахографска карта трябва да бъде генерирана една уникална двойка ключове ECC, обозначена като Card\_MA. Допълнително трябва да бъде генерирана втора уникална двойка ключове ECC, 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, генериралата ключовете страна трябва да изпрати публичния ключ на своя MSCA, за да получи съответен сертификат за картата, подписан от MSCA. Частният ключ трябва да се използва само от тахографската карта.“;

ii) раздел CSM\_88 се заменя със следното:

„CSM\_88 Срокът на валидност на сертификат Card\_MA е, както следва:

- за карти на водач: 5 години
- за карти на превозвач: 5 години
- за контролни карти: 2 години
- за карти за монтаж и настройки: 1 година“;

iii) в раздел CSM\_91 се добавя следният текст:

„— В допълнение — само за контролните карти, картите на превозвач и картите за монтаж и настройки, и то само ако се издават през първите три месеца от срока на валидност на нов сертификат EUR — ако съществува — сертификата EUR, който е по-стар с две поколения.

*Забележка към последното тире:* Например през първите три месеца от срока на действие на сертификат на ERCA(3) (вж. фигура 1) посочените карти трябва да съдържат сертификата на ERCA(1). Това е необходимо, за да се гарантира, че картите могат да се използват за изтегляне на данни от бордови устройства със сертификат на ERCA(1), чийто обичаен 15-годишен срок на експлоатация и допълнителният 3-месечен срок за изтегляне на данни изтичат през тези месеци; вж. изискването в приложение IV, подточка 13, последното тире.“;

д) точка 9.1.6 се изменя, както следва

i) раздел CSM\_93 се заменя със следното:

„CSM\_93 За всяко външно устройство за GNSS трябва да бъде генерирана една уникална двойка ключове ECC, обозначена като EGF\_MA. Тази задача се изпълнява от производителите на външни устройства за GNSS. Когато бъде генерирана двойка ключове EGF\_MA, генериралата ключовете страна трябва да изпрати публичния ключ на своя MSCA, за да получи съответен сертификат за EGF\_MA, подписан от MSCA. Частният ключ се използва само от външното устройство за GNSS.“;

ii) раздел CSM\_95 се заменя със следното:

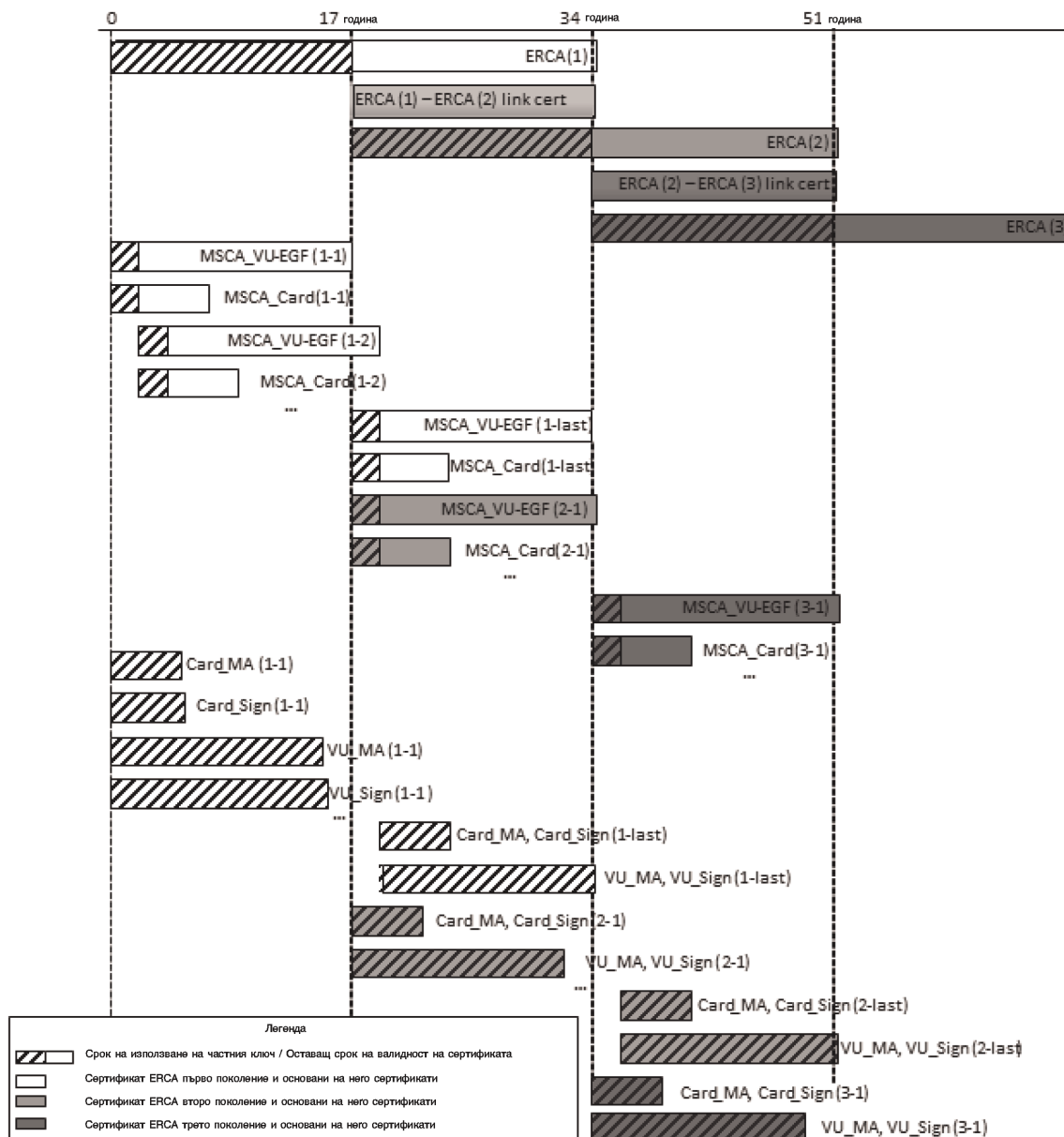
„CSM\_95 Всяко външно устройство за GNSS трябва да използва своята двойка ключове EGF\_MA, състояща се от частен ключ EGF\_MA.SK и публичен ключ EGF\_MA.PK, изключително и само за взаимно удостоверяване на автентичността и договаряне на сесийни ключове с бордови устройства, както е посочено в раздел 11.4 от настоящото допълнение.“;

е) точка 9.1.7 се изменя, както следва

и) фигура 1 се заменя със следното:

„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)



ii) забележка 6 към фигура 1 се заменя със следното:

„6. За да се пести място, разликата между сроковете на валидност на сертификатите Card\_MA и Card\_Sign е показана само за първото поколение.“;

ж) точка 9.2.1.1 се изменя, както следва:

i) в раздел CSM\_106 първото тире се заменя със следното:

„— За 128-битови главни ключове на датчици за движение: CV = 'B6 44 2C 45 0E F8 D3 62 0B 7A 8A 97 91 E4 5D 83'“;

ii) в раздел CSM\_107 първият абзац се заменя със следното:

„Всеки производител на датчици за движение генерира за всеки датчик за движение случаен и уникален ключ за сдвояване  $K_p$  и изпраща всеки ключ за сдвояване до своя сертифициращ орган на държавата членка (MSCA). MSCA криптира всеки ключ за сдвояване поотделно с главния ключ на датчика за движение  $K_M$  и връща криптирания ключ на производителя на датчика за движение. За всеки криптиран ключ MSCA уведомява производителя на датчика за движение за номера на версията на съответния  $K_M$ “;

iii) раздел CSM\_108 се заменя със следното:

„CSM\_108 Всеки производител на датчици за движение генерира уникален сериен номер за всеки датчик за движение и изпраща всички серийни номера до своя сертифициращ орган на държавата членка (MSCA). MSCA криптира всеки сериен номер поотделно с идентификационния ключ  $K_{ID}$  и връща криптирания сериен номер на производителя на датчика за движение. За всеки криптиран сериен номер MSCA уведомява производителя на датчика за движение за номера на версията на съответния  $K_{ID}$ “;

з) точка 9.2.2.1 се изменя, както следва:

i) раздел CSM\_123 се заменя със следното:

„CSM\_123 За всяко бордово устройство производителят на бордови устройства създава уникален сериен номер VU и изпраща този номер на своя сертифициращ орган на държавата членка с искане да получи набор от два специфични за бордово устройство ключа за DSRC. Сериеният номер на бордовото устройство трябва да съдържа типа данни VuSerialNumber.“

*Забележка:*

— Сериеният номер на бордовото устройство трябва да е същият като елемента vuSerialNumber от VuIdentification, вж. допълнение 1, и указанието за титуляря на сертификата (Certificate Holder Reference) в сертификатите на бордовото устройство.

— Сериеният номер на бордовото устройство може още да не е известен към момента, когато производителят на бордовото устройство подава искане за специфичните за бордово устройство ключове за DSRC. В този случай вместо него производителят на бордовото устройство трябва да изпрати уникалния идентификатор на подаденото от него искане за сертификатите на бордовото устройство; вж. CSM\_153. Съответно идентификаторът на искането за сертификат трябва да е същият като указанието за титуляря на сертификата (Certificate Holder Reference) в сертификатите на бордовото устройство.“;

ii) в раздел CSM\_124 изискването за информация в стъпка 2 се заменя със следното:

„info = сериен номер на бордовото устройство или идентификатор на искането за сертификат, както е специфициран в CSM\_123“;

iii) раздел CSM\_128 се заменя със следното:

„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 серийния номер на бордовото устройство или идентификатора на искането за сертификат, който е използвал за тяхното създаване.“;

и) в точка 9.3.1, в раздел CSM\_135 първият абзац се заменя със следното:

„За кодиране на обекти от данни в сертификатите трябва да бъдат използвани разграничените правила за кодиране (DER) съгласно [ISO 8825-1]. Пълното кодиране на сертификата, в т.ч. всички байтове за таг и дължина, е показано в таблица 4.“;

й) в точка 9.3.2.3 раздел CSM\_141 се заменя със следното:

„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, следвани от типа уред, указващ за какъв тип уреди е предназначен сертификатът. При сертификат за бордово устройство, сертификат за карта на водач или сертификат за карта за монтаж и настройки типът уред се използва също така, за да се направи разлика между сертификат за взаимно удостоверяване на автентичността и сертификат за създаване на цифрови подписи (вж. раздел 9.1 и допълнение 1, тип данни EquipmentType).“;

к) в точка 9.3.2.5, в раздел CSM\_146 се добавя следният абзац:

„Забележка: При сертификат на карта стойността на CHR трябва да бъде равна на стойността на cardExtended-SerialNumber в EF\_ICC; вж. допълнение 2. При сертификат на EGF стойността на CHR трябва да бъде равна на стойността на sensorGNSSSerialNumber в EF\_ICC; вж. допълнение 14. При сертификат на бордово устройство стойността на CHR трябва да бъде равна на елемента vuSerialNumber от VuIdentification, вж. допълнение 1, освен ако към момента, когато подава искане за сертификат, производителят не знае специфичния за него сериен номер.“;

л) в точка 9.3.2.6 раздел CSM\_148 се заменя със следното:

„CSM\_148 Датата на влизане в сила на сертификата показва началната дата и час на срока на валидност на сертификата.“;

м) точка 9.3.3 се изменя, както следва:

i) в раздел CSM\_151 първият абзац се заменя със следното:

„При поискване на сертификат MSCA трябва да изпрати на ERCA следните данни:“;

ii) раздел CSM\_153 се заменя със следното:

„CSM\_153 Производител на оборудване изпраща следните данни в искане за сертификат до MSCA, които да дадат възможност на MSCA да създаде указанието на титуляря на новия сертификат на 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.

Производителът гарантира, че тези данни са правилни и че полученият от MSCA сертификат е вложен в оборудването, за което е предназначен.“;

н) точка 10.2.1 се изменя, както следва:

i) в раздел CSM\_157 текстът преди забележките към фигура 4 се заменя със следното:

„За проверяване на веригата на сертифициране на тахографска карта бордовите устройства трябва да използват протокола, описан във фигура 4. За всеки сертификат, който чете от картата, бордовото устройство трябва да провери дали полето за оторизация на титуляря на картата (Certificate Holder Authorisation — CHA) е правилно:

— Полето CHA в сертификата на картата трябва да указва сертификат на карта за взаимно удостоверяване на автентичността (вж. допълнение 1, тип данни EquipmentType);



— CHA в сертификат Card.CA трябва да указва MSCA;

— CHA в сертификат Card.Link трябва да указва ERCA.“;

ii) в раздел CSM\_159 се добавя следното изречение:

„Въпреки че съхранението на всички други видове сертификати не е задължително, бордовото устройство задължително съхранява нов свързващ сертификат, представен от картата.“;

o) точка 10.2.2 се изменя, както следва:

i) в раздел CSM\_161 текстът преди фигура 5 се заменя със следното:

„За проверяване на веригата на сертифициране на бордово устройство тахографските карти трябва да използват протокола, описан във фигура 5. За всеки сертификат, представен от бордовото устройство, картата трябва да провери дали полето за оторизация на титуляра на картата (Card Holder Authorisation — CHA) е правилно:

— CHA в сертификат VU.Link трябва да указва ERCA.

— CHA в сертификат VU.CA трябва да указва MSCA.

— Полето CHA в сертификата на бордовото устройство трябва да указва сертификат на бордово устройство за взаимно удостоверяване на автентичността (вж. допълнение 1, тип данни EquipmentType).“;

ii) раздел CSM\_165 се заменя със следното:

„CSM\_165 Ако командата MSE: Set AT бъде изпълнена успешно, картата трябва да зададе посочения VU.PK за последваща употреба при удостоверяване на автентичността на бордовото устройство и временно да съхрани Comp(VU.PKerh). Ако бъдат изпратени две или повече успешни команди MSE: Set AT, преди да е направено договаряне на сесиен ключ, картата трябва да съхрани само последното получено Comp(VU.PKerh). След успешна команда GENERAL AUTHENTICATE картата трябва да инициализира Comp(VU.PKerh).“;

p) точка 10.3 се изменя, както следва:

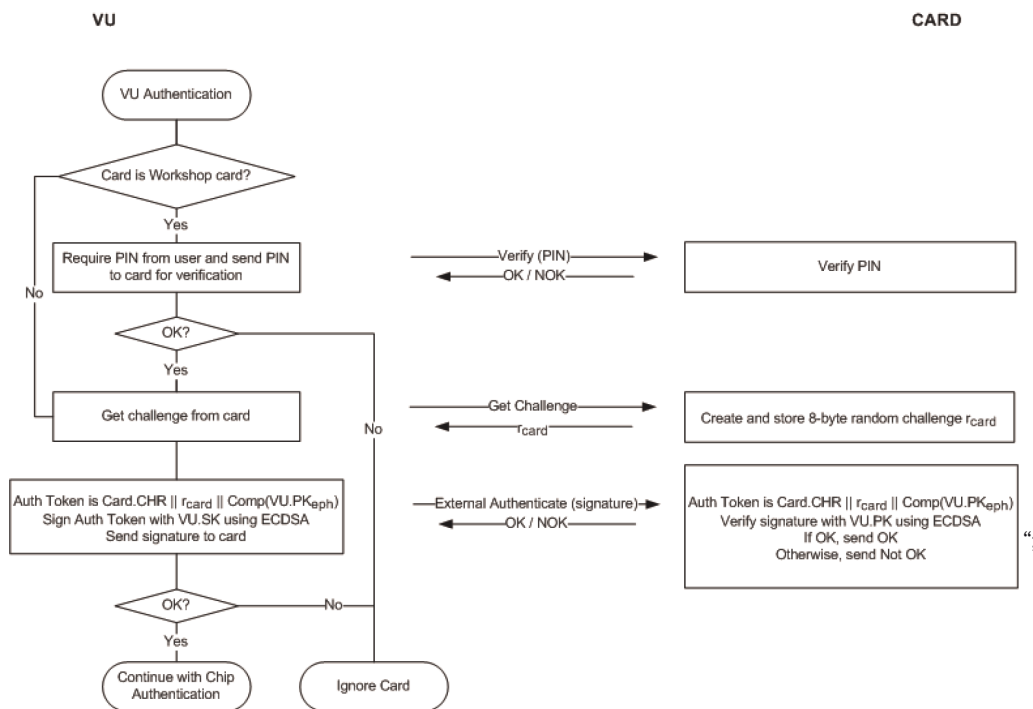
i) в раздел CSM\_170 първият абзац се заменя със следното:

„Непосредствено след изпратеното от картата случайно число бордовото устройство включва в подписа указанието за титуляра на сертификата, взето от сертификата на картата.“;

ii) в раздел CSM\_171 фигура 6 се заменя със следното:

„Фигура 6

**Протокол за удостоверяване на автентичността на бордово устройство**



iii) раздел CSM\_174 се заменя със следното:

„CSM\_174 При получаване на подписа на бордовото устройство в команда EXTERNAL AUTHENTICATE картата трябва да изпълни следните операции:

- Да изчисли удостоверяващия автентичността маркер (authentication token) чрез конкатенация на Card.CHR, случайно число от картата r<sub>card</sub> и идентификатора на краткотрайния публичен ключ на бордовото устройство Comp(VU.PK<sub>eph</sub>),
- Да провери подписа на бордовото устройство, като използва алгоритъма ECDSA и алгоритъма за хеширане, съответстващ на размера на ключовете в двойката ключове VU\_MA на бордовото устройство, както е специфицирано в CSM\_50, в комбинация с VU.PK и изчисления удостоверяващ автентичността маркер.“;

p) в точка 10.4 раздел CSM\_176 се изменя, както следва:

i) подточка 2 се заменя със следното:

„2. Бордовото устройство изпраща на картата публичната точка VU.PK<sub>eph</sub> от своята двойка краткотрайни ключове. Публичната точка трябва да се преобразува в октетен низ, както е специфицирано в [TR-03111]. Трябва да се използва некомпесирият формат за кодиране. 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 идентификатора на краткотрайния публичен ключ Comp(VU.PK<sub>eph</sub>) и картата го е съхранила.“;

ii) подточка 6 се заменя със следното:

„6. Използвайки K<sub>MAC</sub>, картата изчислява удостоверяващ автентичността маркер върху кратковременния публичен ключ на бордовото устройство: T<sub>PICC</sub> = CMAC(K<sub>MAC</sub>, VU.PK<sub>eph</sub>). Публичната точка трябва да бъде в използвания от бордовото устройство формат (вж. подточка 2 по-горе). Картата изпраща на бордовото устройство N<sub>PICC</sub> и T<sub>PICC</sub>.“;

с) в точка 10.5.2 раздел CSM\_191 се заменя със следното:

„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 също трябва да бъде запълнен 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) без криптиране: DO '81' || DO '99' || DO '8E' || SW1SW2

Случай 2 или 4 (четен INS байт) с криптиране: DO '87' || DO '99' || DO '8E' || SW1SW2

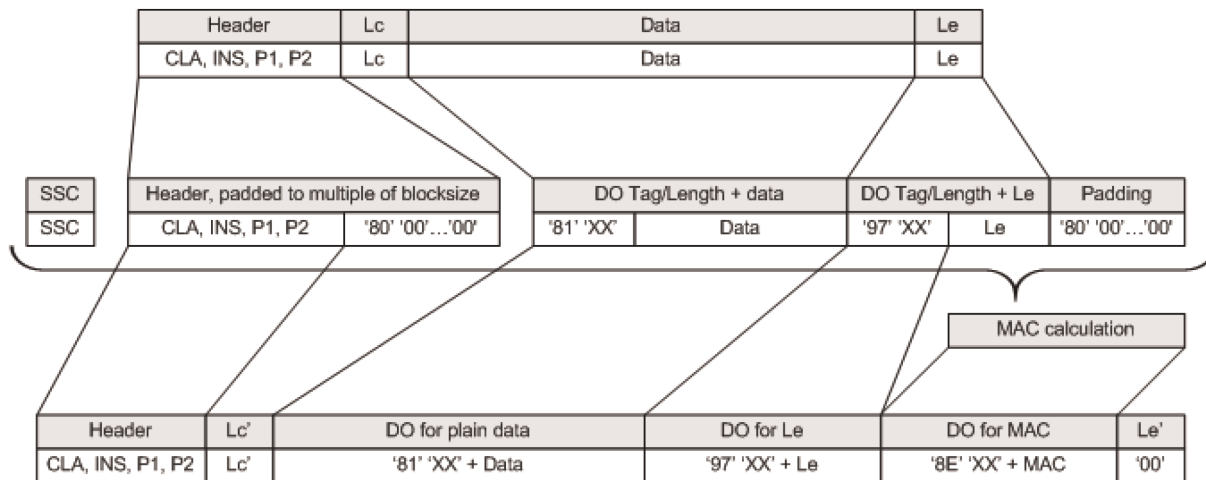
Случай 2 или 4 (нечетен INS byte) без криптиране: DO 'B3' || DO '99' || DO '8E' || SW1SW2

*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 APDU за команди с четен INS код. На фигура 8 е показана командна APDU с удостоверена автентичност — случай 4, на фигура 9 е показана ответна APDU с удостоверена автентичност — случай 1/случай 3, а на фигура 10 е показана криптирана ответна APDU с удостоверена автентичност — случай 2/случай 4.

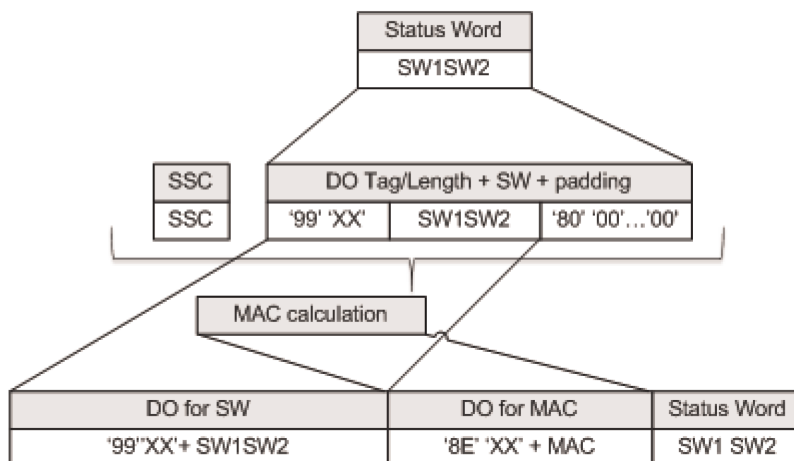
Фигура 8

Преобразуване на командна APDU с удостоверена автентичност, случай 4



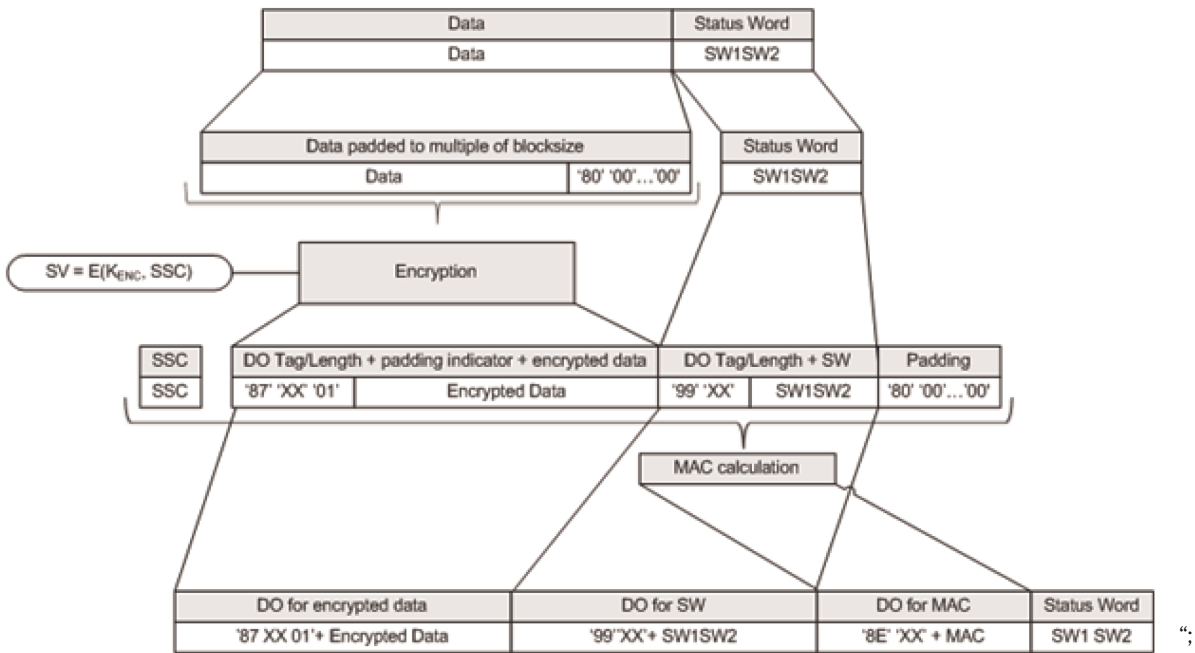
Фигура 9

Преобразуване на ответна APDU с удостоверена автентичност, случай 1/случай 3



Фигура 10

Преобразуване на криптирана ответна APDU с удостоверена автентичност, случай 2/случай 4



т) в точка 10.5.3 раздел CSM\_193 се заменя със следното:

„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 командна APDU в открит текст,
- тахографската карта открие в командната 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 или е инициализирана,
- 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. Лимитът за дадена карта се определя 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.“;

у) точка 11.3.2 се изменя, както следва:

i) в раздел CSM\_208 първият абзац се заменя със следното:

„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.“;

ii) раздел CSM\_210 се заменя със следното:

„CSM\_210 След като веднъж е проверило сертификата VU\_MA, външното устройство за GNSS трябва да го съхрани за използване при нормална работа; вж. раздел 11.3.3.“;

ф) в точка 11.3.3, в раздел CSM\_211 първият абзац се заменя със следното:

„При нормална работа дадено бордово устройство и EGF трябва да използват протокола, описан във фигура 11, за проверка на валидността във времето на съхранения сертификат EGF\_MA и за задаване на публичния ключ VU\_MA за последващо удостоверяване на автентичността на бордовото устройство. При нормална работа не трябва да се прави по-нататъшна взаимна проверка на веригите за сертифициране.“;

х) таблица 6 в точка 12.3 се заменя със следното:

„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 удостоверяване на автентичността + номер на файла	8	8	16	16	16
11	Отговор	Данни за удостоверяване на автентичността + съдържание на файла	16 или 32, зависи от файла	16 или 32, зависи от файла	32 / 48	32 / 48	32 / 48
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 удостоверяване на автентичността	8	8	16	16	16
80	Отговор	Стойност на брояча на MoS + данни за удост. на автент.	8	8	16	16	16“

ц) в точка 13.1, раздел CSM\_224, изискването за серийния номер на бордовото устройство се заменя със следното:

„Сериен номер на бордовото устройство (серийният номер на бордовото устройство или идентификаторът на искането за сертификат (тип данни VuSerialNumber или CertificateRequestID) — вж. CSM\_123“;

ч) в точка 13.3, в раздел CSM\_228 втората подточка се заменя със следното:

„2. Контролната карта трябва да използва посочения главен ключ DSRC в комбинация със серийния номер на бордовото устройство или с идентификатора на искането за сертификат 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.“;

щ) точка 14.3 се изменя, както следва:

i) в раздел CSM\_234 текстът преди забележките към фигура 13 се заменя със следното:

„Дадено IDE може само 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 се извършва, както е показано във фигура 13. За да провери валидността във времето на представен от IDE сертификат, контролната карта трябва да използва вътрешно генерираното от нея текущо време съгласно посоченото в раздел CSM\_167. Ако датата на влизане в сила на автентичен сертификат, представляващ „валиден източник на данни за времето“, е по-скорошна от текущото време на картата, картата трябва да актуализира своето текущо време. 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 VU\_Sign или Card\_Sign от второ поколение, издадени от същата държава като издалата собствения сертификат на контролната карта.

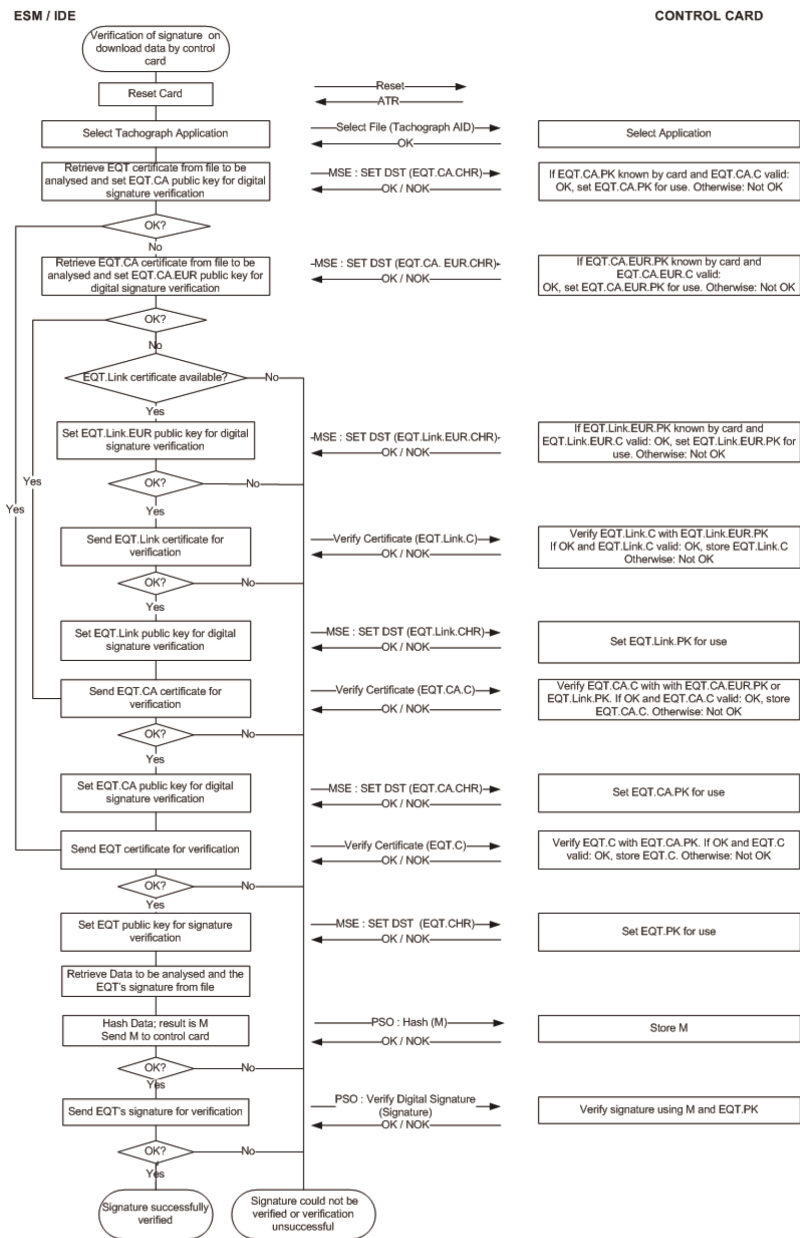
В случай че самото IDE проверява подписа, то трябва да провери автентичността и валидността на всички сертификати в сертификационната верига във файла с данни, както и подписа върху данните, в съответствие със схемата за подписване, дефинирана в [DSS]. И в двата случая за всеки сертификат, който се чете от файла с данни, трябва да се провери дали полето за оторизация на титуляря на сертификата (Certificate Holder Authorisation — CHA) е правилно:

- Полето CHA в сертификата EQT трябва да указва сертификат за подпис на бордово устройство или карта според случая (вж. допълнение 1, тип данни EquipmentType).
- CHA в сертификат EQT.CA трябва да указва MSCA.
- CHA в сертификат EQT.Link трябва да указва ERCA.“;

ii) фигура 13 се заменя със следното:

„Фигура 13

Протокол за проверка на подписа върху изтеглен файл с данни





37) Допълнение 12 се изменя, както следва:

а) точка 3 се изменя, както следва:

i) в раздел GNS\_4 вторият абзац след фигура 2 се заменя със следното:

„Разделителната способност за местоположението се базира на формата на гореописаното изречение RMC. Първата част от полета 3) и 5) 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 една минута е 1/60 от градуса).“;

ii) раздел GNS\_5 се заменя със следното:

„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 съответния идентификатор на NMEA за всяка група спътници на GNSS и за спътниковата система за диференциална корекция (Satellite- Based Augmentation System, SBAS).

### Фигура 3

#### Структура на изречение GSA

1234                      1415 16 1718  
 ↓ ↓ ↓ ↓                      ↓ ↓ ↓ ↓ ↓

\$<GNSS Id.>GSA,a,a,x,x,x,x,x,x,x,x,x,x,x,x,x,x,x,x\*hh

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 12-ия спътник, използван за фиксиране)

15) PDOP

16) HDOP

17) VDOP

18) Checksum (контролна сума) „

iii) раздел GNS\_6 се заменя със следното:

„GNS\_6 Изречението GSA трябва да бъде съхранявано с номер на записа „02“ — „06“.“;

б) точка 4.2.1 се изменя, както следва:

i) раздел GNS\_16 се заменя със следното:

„GNS\_16 В протокола за връзка не трябва да се поддържат полета с увеличена дължина.“;

ii) раздел GNS\_18 се заменя със следното:

„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 управление, защитеният приемопредавател за GNSS трябва да симулира карта с чип с архитектура на файловата система, състояща се от главен файл (Master File, MF), специализиран файл (Dedicated 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 таблица 1.“;

iii) раздел GNS\_20 се заменя със следното:

„GNS\_20 Паметта, използвана от защитения приемопредавател за GNSS за съхраняване на данните, трябва да може да изпълни поне 20 милиона цикъла запис/четене. С изключение на този аспект, вътрешната конструкция и изпълнението на защитения приемопредавател за GNSS е по усмотрение на производителите.

Разпределянето на номерата на записите и данните в паметта е дадено в таблица 1. Отбележете, че съществуват пет изречения GSA за GNSS и за спътниковата система за диференциална корекция (SBAS).“;

v) в точка 4.2.2, в раздел GNS\_23 подточка 5 се заменя със следното:

„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 и стойностите на HDOP и изчислява средната стойност по наличните спътникови системи (т.е. когато има налично фиксиране).“;

г) в точка 4.4.1 раздел GNS\_28 се заменя със следното:

„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 'OE'H — Грешка в комуникацията с външното устройство за GNSS, и с времеви печат, 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 е в движение. В този случай регистрирането на грешка във връзката се задейства, когато защитеният приемопредавател на бордовото устройство не получи съобщение, съдържащо отговор, след изпращането на съобщение със заявка, както е описано в раздел 4.2.“;

д) в точка 4.4.2 раздел GNS\_29 се заменя със следното:

„GNS\_29 Ако целостта на външното устройство за GNSS бъде нарушена, защитеният приемопредавател за GNSS трябва да изтрие цялата си памет, включително криптографския материал. Както е описано в раздели GNS\_25 и GNS\_26, бордовото устройство трябва да констатира наличие на вмешателство, ако отговорът е със статус '6690'. В такъв случай бордовото устройство трябва да генерира събитие от типа EventFaultType с изброена (enum) стойност '19'H — Установяване на вмешателство в GNSS. Като алтернатива, външното устройство за GNSS може повече да не отговаря на други външни заявки.“;

е) в точка 4.4.3 раздел GNS\_30 се заменя със следното:

„GNS\_30“ Ако защитеният приемопредавател за GNSS не получава данни от приемника на сигнали от GNSS в течение на повече от 3 последователни часа, защитеният приемопредавател за GNSS трябва да генерира съобщение, съдържащо 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 съдържащо отговор съобщение с тази стойност в полето за данни, бордовото устройство трябва да генерира и регистрира събитие от типа EventFaultType с изброена (enum) стойност 'OD'H — Липса на информация за местоположението от приемник на сигнали от GNSS, 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 е в движение.“;

ж) в точка 4.4.4 текстът в раздел GNS\_31 до фигура 4 се заменя със следното:

„Ако установи, че използваният за взаимно удостоверяване на автентичността сертификат EGF вече не е валиден, бордовото устройство трябва да генерира и регистрира събитие, свързано с уредите за регистриране на данни за движението, от типа EventFaultType с изброена (enum) стойност '1B'H — Изтекъл сертификат на външно устройство за GNSS, с времеви печат, съответстващ на текущото време. При това бордовото устройство трябва да продължи да използва получаваните от GNSS данни за местоположението.“;

з) в точка 5.2.1 раздел GNS\_34 се заменя със следното:

„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 '0D'H — Липса на информация за местоположението от приемник на сигнали от GNSS, 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 е в движение.“;

и) точка 6 се заменя със следното:

#### „6. ВРЕМЕВИ КОНФЛИКТ В ДАННИТЕ ОТ GNSS

Ако установи несъответствие, по-дълго от 1 минута, между показанията на функцията за измерване на времето на бордовото устройство и данните за времето, постъпващи от приемника на сигнали от GNSS, бордовото устройство трябва да регистрира събитие от типа EventFaultType с изброена (enum) стойност '0B'H — *Времеви конфликт (GNSS/вътрешния часовник на бордовото устройство)*. След задействане на събитие на времеви конфликт през следващите 12 часа бордовото устройство не проверява за времеви конфликт. Това събитие не трябва да се преизвиква, ако през последните 30 дни от приемника на сигнали от GNSS не е можел да бъде открит валиден сигнал от GNSS.“

38) Допълнение 13 се изменя, както следва:

а) в точка 2 четвъртият абзац се заменя със следното:

„Трябва да се поясни, че в настоящото допълнение не са определени:

- събирането и управлението на *данните* в рамките на бордовото устройство (които са определени на друго място в *регламента* или — ако не е така — зависят 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 са определени на друго място в *регламента* [общите механизми за сигурност от допълнение 11]),
- протоколите за Bluetooth®, използвани от интерфейса с ITS.“;

б) в точка 4.2 третият абзац се заменя със следното:

„Процесът на сдвояване за връзка Bluetooth® може да започне, когато външно устройство попадне в обсега на бордовото устройство за първи път (вж. 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 общите механизми за сигурност от допълнение 11.“;

в) точка 4.3 се изменя, както следва:

и) първият абзац се заменя със следното:

„От съображения за сигурност бордовото устройство изисква система за разрешаване на достъпа чрез PIN код, която е отделена от сдвояването по Bluetooth. Всяко бордово устройство 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 бордовото устройство, то трябва да подаде правилния PIN код, преди да получи каквито и да било данни.“;

ii) третият абзац след таблица 1 се заменя със следното:

„Производителят може да предлага възможност за промяна на PIN кода пряко чрез бордовото устройство, 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 в бордовото устройство.“;

г) в точка 4.4, вторият абзац след заглавието „Поле за данни“ се заменя със следното:

„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 една и съща заглавна част и SID, но съдържа брояч от 2 байта — Counter Current (CC) и Counter Max (CM), който посочва номера на подсъобщението. С цел да се осигури контрол за грешки и евентуално да се прекрати обменът 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.“;

д) приложение 1 се изменя, както следва:

i) заглавието се заменя със следното:

„1) СПИСЪК НА ДАННИТЕ, ПРЕДОСТАВЯНИ ЧРЕЗ ИНТЕРФЕЙСА С ITS“;

ii) в таблицата в точка 3 — след позицията „Липса на информация за местоположението от приемник на сигнали от GNSS“, се добавя следната позиция:

„Грешка в комуникацията с външното устройство за GNSS“	— най-продължителното събитие за всеки от последните 10 дни на възникване, — 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.“
--	---	--

iii) в точка 5 се добавя следното тире:

„— неизправност на интерфейса с ITS (ако е приложимо)“;

е) спецификациите на ASN.1 в приложение 3 се изменят, както следва:

i) след ред 206 се добавят следните редове 206а — 206е:

```

206a
206b     DriverID ::= SEQUENCE{
206c     issuingMemberState OCTET STRING (SIZE(3)),
206d     cardNumber OCTET STRING (SIZE(16))
206e }“;

```

ii) редове 262 — 264 се заменят със следното:

```

,262     driveRecognize BIT STRING ('00'B UNION '01'B),
263     driverCardDriver1 BIT STRING ('00'B UNION '01'B),
264     driverCardDriver2 BIT STRING ('00'B UNION '01'B), “;

```

iii) ред 275 се заменя със следното:

```
„275 outOfScopeCondition BIT STRING ('00'B UNION '01'B),,,;
```

iv) редове 288 — 310 се заменят със следното:

```
„288 driver1WorkingState BIT STRING ('000'B UNION '001'B UNION '010'B UNION
289 '011'B UNION '100'B UNION '101'B ...),
290 driver2WorkingState BIT STRING ('000'B UNION '001'B UNION '010'B UNION
291 '011'B UNION '100'B UNION '101'B ...),
292
293 driver1TimeRelatedStates BIT STRING ('0000'B UNION '0001'B
294 UNION '0010'B UNION '0011'B UNION '0100'B UNION '0101'B UNION
295 '0110'B UNION '0111'B UNION '1000'B UNION '1001'B UNION '1010'B
296 UNION '1011'B UNION '1100'B UNION '1101'B ...),
297
298
299 driver2TimeRelatedStates BIT STRING ('0000'B UNION '0001'B
300 UNION '0010'B UNION '0011'B UNION '0100'B UNION '0101'B UNION
301 '0110'B UNION '0111'B UNION '1000'B UNION '1001'B UNION '1010'B
302 UNION '1011'B UNION '1100'B UNION '1101'B ...),
303
304
305
306 overSpeed BIT STRING ('00 'B UNION '01 'B),
307 driver1Identification DriverID,
308 driver2Identification DriverID,
309
310“
```

v) редове 362 и 363 се заменят със следното:

```
„362 driver1MaximumDailyDrivingTime BIT STRING (SIZE(4)),
363 driver2MaximumDailyDrivingTime BIT STRING (SIZE(4)),“;
```

vi) след ред 410 се добавят следните редове 410a и 410b:

```
„410a comErrorWithExternalGNSSFacility
410b CommunicationErrorWithTheExternalGNSSFacility,“;
```

vii) след ред 539 се добавят следните редове 539a — 539j:

```
„539a CommunicationErrorWithTheExternalGNSSFacility ::= SEQUENCE{
539b beginDate GeneralizedTime,
539c endDate GeneralizedTime,
539d cardsType SEQUENCE OF UTF8String,
539e cardsNumber SEQUENCE OF INTEGER,
539f issuingMemberState SEQUENCE OF NationAlpha,
539g cardsGeneration SEQUENCE OF INTEGER,
539h numberOfSimilarEvent INTEGER
539i }
539j“;
```

39) Допълнение 14 се изменя, както следва:

а) точка 5.5 в съдържанието се заменя със следното:

„5.5 Подкрепа за спазването на Директива (ЕС) 2015/719 ..... 490“;

б) в точка 2 третият абзац се заменя със следното:

„В този сценарий наличното време за връзка е ограничено, тъй като *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 (ЕС) 2015/719), като тези действия могат да бъдат отделни или последователни по преценка на компетентните контролни органи.“;

в) точка 5.1 се изменя, както следва:

i) в раздел DSC\_19 дванадесетото тире се заменя със следното:

— Антената на DSRC-VU трябва да е разположена на място, което осигурява оптимална DSRC връзка между превозното средство и антената на крайпътния четец, при положение че четецът е монтиран на разстояние 15 метра пред превозното средство и на височина 2 метра, като се търси средата по хоризонталата и по вертикалата на предното стъкло. За леки превозни средства е подходящо монтиране в горната част на предното стъкло. За всички останали превозни средства антената за DSRC трябва да се монтира близо до долната или до горната част на предното стъкло.“;

ii) в раздел DSC\_22 първият абзац се заменя със следното:

„Размерната спецификация на антената не е определена 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 трябва ефикасно да работи за случаите на употреба, описани в точки 4.1.2 и 4.1.3.“;

г) в точка 5.4.3 последователност номер 7 се заменя със следното:

„7 REDCR > DSRC-VU Изпраща GET.request за данни, различни от Attribute (ако е уместно)“

д) в точка 5.4.4, раздел DCS\_40, определението на модула ASN.1 се изменя, както следва:

i) първият ред в последователността TachographPayload се заменя със следното:

„tp15638VehicleRegistrationPlate LPN – Vehicle Registration Plate as per EN 15509<sup>1</sup>“

ii) добавя се следната бележка под линия 1:

„1. Ако LPN съдържа буквен показател (AlphabetIndicator) LatinAlphabetNo2 или latinCyrillicAlphabet, запитващото устройство на пътя преобразува специалните символи, като прилага специалните правила от приложение Д към стандарт ISO/DIS 14 906.2.“;

iii) в реда с определението за „Timestamp of current record“ горният индекс 2 се заличава;

iv) определението за RtmTransferAck в модула ASN.1 се заменя със следното:

```
„RtmTransferAck ::= INTEGER {  
    Ok (1),  
    NoK (2)  
} (1..255)“;
```

е) в точка 5.4.5 позиция RTM12 в таблица 14.3 се заменя със следното:

<p><b>„RTM12</b> <b>Неиз-</b> <b>правност на</b> <b>датчика</b></p>	<p>Бордовото устройство генерира целочислена стойност за елемента RTM12 на данните.</p> <p>Бордовото устройство присвоява на променливата sensorFault стойността:</p> <ul style="list-style-type: none"> <li>— 1, ако през последните 10 дни е било регистрирано събитие от типа '35'H за неизправност на датчика,</li> <li>— 2, ако през последните 10 дни е било регистрирано събитие за неизправност на приемника на сигнали от GNSS (вътрешно или външно с изброени (enum) стойности '36'H или '37'H),</li> <li>— 3, ако през последните 10 дни е било регистрирано събитие от типа '0E'H за грешка в комуникацията с външното устройство за GNSS,</li> <li>— 4, ако през последните 10 дни са били регистрирани неизправности както по датчика, така и по приемника на сигнали от GNSS,</li> <li>— 5, ако през последните 10 дни са били регистрирани както неизправност по датчика, така и грешка в комуникацията с външното устройство за GNSS,</li> <li>— 6, ако през последните 10 дни са били регистрирани както неизправност по приемника на сигнали от GNSS, така и грешка в комуникацията с външното устройство за GNSS,</li> <li>— 7, ако през последните 10 дни са били регистрирани всички три вида неизправности по датчика. В ПРОТИВЕН СЛУЧАЙ се присвоява стойност 0, ако през последните 10 дни не са били регистрирани събития.</li> </ul>	<p>— за неизправност на датчика — един октет съгласно речника на данните</p>	<p>sensorFault INTEGER “ (0..255);”</p>
---	---	--	---

ж) в точка 5.4.6 раздел DSC\_43 се заменя със следното:

„DSC\_43 При всеки обмен на данни по DSRC те трябва да бъдат кодирани съгласно PER (Packed Encoding Rules) UNALIGNED, с изключение на TachographPayload и OwsPayload; които трябва да бъдат кодирани съгласно OER (Octet Encoding Rules), определени в стандарт ISO/IEC 8825-7, Rec. ITU-T X.696.“;

з) в точка 5.4.7, в таблица 14.9, четвърта графа, текстът в клетката с описанието на Rtm-ContextMark; се заменя със следното:

„Object Identifier на поддържащия 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.“;

и) точки 5.5 и 5.5.1 се заменят със следното:

#### „5.5. Подкрепа за спазването на Директива (ЕС) 2015/719

##### 5.5.1. Преглед

DSC\_59 С цел да се подпомогне спазването на Директива (ЕС) 2015/719 относно максимално допустимите маси и размери на тежкотоварни превозни средства протоколът за трансакциите по изтегляне на данни от бордова система за претегляне (OWS) по интерфейсна връзка към DSRC на 5,8 GHz ще е същият, както използваният за данните за RTM (вж. раздел 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.“;



й) в точка 5.6.1, раздел DSC\_68, буква а) се заменя със следното:

„а) Връзката между бордовото устройство и DSRC-VU, която не е вътрешна за бордовото устройство, трябва да бъде по отворен стандарт, за да е възможно договарянето с различни доставчици за получаването на бордови устройства и DSRC-VU, както и на DSRC-VU от различни партии. Бордовото устройство се свързва с DSRC-VU по някой от следните начини:“;

к) в точка 5.7.1 раздел DSC\_77 се заменя със следното:

„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 бордовото устройство към паметта на DSRC-VU се извършва с типа EventFaultType и изброена (enum) стойност, зададена като събитие 'OCH — Грешка в комуникацията с устройството за връзка от разстояние, заедно с времеви печат.“

40) Допълнение 15 се изменя, както следва:

а) в точка 2.2 първият абзац се заменя със следното:

„Подразбира се, че първото поколение тахографски карти са оперативно съвместими с първото поколение бордови устройства в съответствие с приложение IB към Регламент (ЕИО) № 3821/85, както и че второто поколение тахографски карти са оперативно съвместими с второто поколение бордови устройства в съответствие с приложение IB от настоящия регламент. В допълнение към това се прилагат следните изисквания:“;

б) в точка 2.4.1 раздел MIG\_11 се изменя, както следва

i) първото тире се заменя със следното:

„— неподписаните елементарни файлове IC и ICC (незадължително),“;

ii) третото тире се заменя със следното:

„— останалите елементарни файлове с приложни данни (в рамките на DF Tachograph), изисквани по протокола за изтегляне на данни от карти от първо поколение. Информацията трябва да бъде защитена с цифров подпис в съответствие с механизмите за сигурност за първото поколение.

Подобно изтегляне не трябва да включва елементарни файлове с приложни данни, които присъстват само във второ поколение карти на водачи (и карти за монтаж и настройки) — елементарни файлове с приложни данни в рамките на DF Tachograph\_G2.“;

в) в точка 2.4.3 раздели MIG\_014 и MIG\_015 се заменят със следното

„MIG\_014 С изключение на случаите на проверка на водача от контролни органи на държави извън ЕС, 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 към настоящото приложение.

MIG\_015 С цел проверка на водача да може да се извършва от контролни органи на държави извън ЕС, по избор може да бъде възможно данни от бордово устройство от второ поколение да се изтеглят, като се използват първо поколение механизми за сигурност. Изтеглените данни трябва да имат същия формат като данните, изтеглени от бордово устройство от първо поколение. Тази възможност трябва да може да бъде избрана чрез команди в менюто.“



## ПРИЛОЖЕНИЕ II

Приложение II към Регламент (ЕС) 2016/799 се изменя, както следва:

1) В глава I, точка 1 буква б) се заменя със следното:

„б) номер на одобрението, съответстващ на номера на сертификата за одобрение, изготвен за прототипа на уреда за регистриране на данните за движението, тахографския лист или тахографската карта, който се поставя в непосредствена близост до посочения правоъгълник.“

2) В глава III точка 5 се заменя със следното:

„5. Представено за одобряване на .....“

3) В глава IV точка 5 се заменя със следното:

„5. Представено за одобряване на .....“

---





ISSN 1977-0618 (електронно издание)  
ISSN 1830-3617 (печатно издание)



**Служба за публикации на Европейския съюз**  
2985 Люксембург  
ЛЮКСЕМБУРГ

**BG**