

РЕГЛАМЕНТ (ЕО) № 1360/2002 НА КОМИСИЯТА**от 13 юни 2002 година****относно привеждане за седми път в съответствие с техническия прогрес на Регламент (ЕИО) № 3821/85 на Съвета относно уредите за регистриране на данните за движението при автомобилен транспорт****(текст от значение за ЕИП)**

КОМИСИЯТА НА ЕВРОПЕЙСКИТЕ ОБЩНОСТИ,

като взе предвид Договора за създаване на Европейската общност,

като взе предвид Регламент (ЕИО) № 3821/85 на Съвета от 20 декември 1985 г. относно уредите за регистриране на данните за движението при автомобилен транспорт ⁽¹⁾, последно изменен с Регламент (ЕО) № 2135/98 ⁽²⁾, и по-специално членове 17 и 18 от него,

като има предвид, че:

- (1) Необходимо е да се приведат в съответствие с техническия прогрес техническите спецификации на приложение I Б на Регламент (ЕИО) № 3821/85, като се обърне особено внимание на глобалната сигурност на системата и на възможността за взаимна работа на уредите за регистриране на данните за движението с картите на водача.
- (2) Привеждането в съответствие на уредите изисква привеждане в съответствие на приложение II към Регламент (ЕИО) № 3821/85, което определя маркировките и сертификатите за одобрение.
- (3) Тъй като комитетът, създаден по силата на член 18 на Регламент (ЕИО) № 3821/85, не е дал своето становище относно предвидените в предложението мерки, Комисията предаде на Съвета предложение относно тези мерки.
- (4) Тъй като до изтичането на срока, предвиден в член 18, параграф 5 на Регламент (ЕИО) № 3821/95, Съветът не се е произнесъл, необходимо е Комисията да приеме тези мерки,

ПРИЕ НАСТОЯЩИЯ РЕГЛАМЕНТ:

Член 1

Приложението на Регламент (ЕО) № 2135/98 се заменя с приложението на настоящия регламент.

Член 2

Приложение II към Регламент (ЕИО) № 3821/85 се изменя, както следва:

- 1) глава I, точка 1, параграф първи се изменя, както следва:
 - условното обозначение „GR“ за Гърция се замества от „23“,
 - условното обозначение „IRL“ за Ирландия се замества от „24“,
 - добавя се условното обозначение „12“ за Австрия,
 - добавя се условното обозначение „17“ за Финландия,
 - добавя се условното обозначение „5“ за Швеция.
- 2) глава I, точка 1, параграф втори се изменя, както следва:
 - думите „или от тахографската карта“ се вмъкват след думите „лист със запис на данни“.
- 3) глава I, точка 2 се изменя, както следва:
 - думите „и върху всяка тахографска карта“ се вмъкват след думите „лист със запис на данни“.
- 4) В глава II към заглавието се добавя следната формулировка: „ПРОДУКТИ, ОТГОВАРЯЩИ НА ИЗИСКВАНИЯТА НА ПРИЛОЖЕНИЕ I“.

⁽¹⁾ ОВ L 370, 31.12.1985 г., стр. 8.⁽²⁾ ОВ L 274, 9.10.1998 г., стр. 1.

5) Добавя се следната глава III:

„III. СЕРТИФИКАТ ЗА ОДОБРЕНИЕ ЗА ПРОДУКТИТЕ, ОТГОВАРЯЩИ НА ИЗИСКВАНИЯТА НА ПРИЛОЖЕНИЕ I Б

Държава, която е предоставила одобрение, издава на лицето, искащо сертификат за одобрение, модела, който фигурира по-долу. Копия от този документ трябва да се използват, за да се информират останалите държави-членки за издадените одобрения и, при необходимост, за оттеглените такива.

СЕРТИФИКАТ ЗА ОДОБРЕНИЕ ЗА ПРОДУКТИТЕ, ОТГОВАРЯЩИ НА ИЗИСКВАНИЯТА НА ПРИЛОЖЕНИЕ I Б

Име на компетентния орган

Уведомяване относно ⁽³⁾:

- одобрение на
- оттегляне на одобрение на
- модел на уреди за регистриране на данните за движението
- компонент от уреди за регистриране на данните за движението ⁽⁴⁾
- карта на водач
- цехова карта
- карта на предприятие
- карта на контролор

Одобрение №

1. Фабрична или търговска марка
2. Име на модела
3. Име на производителя
4. Адрес на производителя
5. Представено за одобрение на
6. Лаборатория(и)
7. Дата на провеждане и брой на изпитанията
8. Дата на одобрението
9. Дата на оттегляне на одобрението
10. Модел на компонента(ите) на уредите за регистриране на данните за движението, за която компонентът е изработен и трябва да се използва
11. Място
12. Дата
13. Приложени описателни документи

14. Забележки (по-специално относно местоположението на пломбиранията, ако е необходимо)

.....
(попис)

⁽³⁾ Поставя се отметка в съответната кутийка.

⁽⁴⁾ Уточнява се компонентът, предмет на уведомяването.“

Член 3

Настоящият регламент влиза в сила на двадесетия ден след този на неговото публикуване в *Официален вестник на Европейските общности*.

Настоящият регламент е задължителен в своята цялост и е пряко приложим във всички държави-членки.

Съставено в Брюксел на 13 юни 2002 година.

За Комисията
Loyola DE PALACIO
Заместник-председател

ПРИЛОЖЕНИЕ

„ПРИЛОЖЕНИЕ I Б:

ИЗИСКВАНИЯ, ПРИЛАГАНИ КЪМ КОНСТРУКЦИЯТА, ИЗПИТАНИЯТА, МОНТИРАНЕТО И ИНСПЕКТИРАНЕТО

СЪДЪРЖАНИЕ

I	ОПРЕДЕЛЕНИЯ	10
II.	ОБЩИ ХАРАКТЕРИСТИКИ И ФУНКЦИИ НА УРЕДИТЕ ЗА РЕГИСТРИРАНЕ НА ДАННИТЕ ЗА ДВИЖЕНИЕТО	14
	1. Общи характеристики	14
	2. Функции	14
	3. Режими на функциониране	15
	4. Правила относно сигурността	16
III.	КОНСТРУКТИВНИ И ФУНКЦИОНАЛНИ ИЗИСКВАНИЯ ОТНОСНО УРЕДИТЕ ЗА РЕГИСТРИРАНЕ НА ДАННИТЕ ЗА ДВИЖЕНИЕТО	16
	1. Проследяване на инспектирането и на изваждането на картите	16
	2. Измерване на скоростта и на изминатото разстояние	16
	2.1. Измерване на изминатото разстояние	17
	2.2. Измерване на скоростта	17
	3. Измерване на времето	17
	4. Проследяване на дейностите, извършвани от водача	18
	5. Наблюдение на положението при кормуване.....	18
	6. Ръчно въвеждане на данни от водача	18
	6.1. Записване на местоположението в началото и/или в края на дневния период на работа...	18
	6.2. Ръчно записване на дейностите, извършвани от водача	18
	6.3. Записване на особените условия	20
	7. Управление на блокировките от страна на предприятието при достъпа до данните	20
	8. Проследяване на контролните дейности.....	20
	9. Откриване на събития и/или на аномалии.....	20
	9.1. Събитие „поставяне на невалидна карта“	20
	9.2. Събитие „конфликт, предизвикан от картата“.....	21
	9.3. Събитие „припокриване на времеви период“	21
	9.4. Събитие „кормуване без съответната карта“	21
	9.5. Събитие „поставяне на карта по време на кормуване“	21
	9.6. Събитие „неправилно приключена последна сесия“	21
	9.7. Събитие „превишаване на допустимата скорост“	21

9.8.	Събитие „прекъсване на електрическото захранване“	22
9.9.	Събитие „грешка в данните относно движението“	22
9.10.	Събитие „опит за нарушаване на сигурността“	22
9.11.	Аномалия „карта“	22
9.12.	Аномалия „уреди за регистриране на данните за движението“	22
10.	Автотестове и вградени	22
11.	Четене на паметта	22
12.	Запис и съхраняване в паметта	23
12.1.	Данни за идентификация на уредите	23
12.1.1.	Данни за идентификация на блока, монтиран на превозното средство	23
12.1.2.	Данни за идентификация на датчика за движение	23
12.2.	Елементи, свързани със сигурността	24
12.3.	Данни, свързани с вкарването и изваждането на картата на водача	24
12.4.	Данни относно дейността на водача	25
12.5.	Местоположение в началото и/или в края на дневните периоди на работа	25
12.6.	Километраж	25
12.7.	Подробни записи на скоростта	25
12.8.	Данни относно събитията	25
12.9.	Данни относно аномалиите	27
12.10.	Данни относно еталонирането	28
12.11.	Данни относно сверяването на часовника	28
12.12.	Данни относно контролните дейности	28
12.13.	Данни относно блокировките от страна на предприятието при достъпа до данните	29
12.14.	Данни относно прехвърлянето на данни	29
12.15.	Данни относно особените условия	29
13.	Четене на тахографските карти	29
14.	Запис и съхраняване върху тахографски карти	29
15.	Изобразяване на данните	30
15.1.	Изобразяване по подразбиране	30
15.2.	Изобразяване на предупреждение	31
15.3.	Меню за достъп	31
15.4.	Изобразяване на други данни	31
16.	Отпечатване	31
17.	Предупреждения	32
18.	Прехвърляне на данни към външни медии	33
19.	Данни, прехвърлени към допълнителни външни устройства	33
20.	Еталониране	34
21.	Сверяване на часовника	34

22.	Характеристики	34
23.	Използвани материали.....	34
24.	Надписи	35
IV.	КОНСТРУКТИВНИ И ФУНКЦИОНАЛНИ ИЗИСКВАНИЯ ОТНОСНО ТАХОГРАФСКИТЕ КАРТИ ...	35
1.	Видими данни	35
2.	Правила относно сигурността	38
3.	Стандарти	38
4.	Спецификации, свързани с околната среда и електричеството	38
5.	Съхраняване на данните	38
5.1.	Идентифициране на картата и данни относно сигурността	39
5.1.1.	Идентифициране на приложенията	39
5.1.2.	Идентифициране на микропроцесора	39
5.1.3.	Идентифициране на картите с вграден чип.....	39
5.1.4.	Елементи, свързани със сигурността	39
5.2.	Карта на водача	39
5.2.1.	Идентифициране на картата	39
5.2.2.	Идентифициране на притежателя на картата	40
5.2.3.	Данни относно свидетелството за управление	40
5.2.4.	Данни относно използваното превозно средство	40
5.2.5.	Данни относно дейността на водача	40
5.2.6.	Местоположение в началото и/или в края на дневните периоди на работа	41
5.2.7.	Данни относно събитията	41
5.2.8.	Данни относно аномалиите.....	42
5.2.9.	Данни относно контролните дейности	42
5.2.10.	Данни относно сесиите за всяка карта	42
5.2.11.	Данни относно особените условия	42
5.3.	Цехова карта	43
5.3.1.	Елементи, свързани със сигурността	43
5.3.2.	Идентифициране на картата	43
5.3.3.	Идентифициране на притежателя на картата	43
5.3.4.	Данни относно използваното превозно средство	43
5.3.5.	Данни относно дейността на водача	43
5.3.6.	Данни относно края и/или началото на дневните периоди на работа	43
5.3.7.	Данни относно събитията и аномалиите	43
5.3.8.	Данни относно контролните дейности	43
5.3.9.	Данни относно еталонирането и сверяването на	44
5.3.10.	Данни относно особените условия	44
5.4.	Карта на контрольор	44

5.4.1.	Идентифициране на картата	44
5.4.2.	Идентифициране на притежателя на картата	44
5.4.3.	Данни относно контролните дейности	44
5.5.	Карта на предприятие	45
5.5.1.	Идентифициране на картата	45
5.5.2.	Идентифициране на притежателя на картата	45
5.5.3.	Данни относно дейността на предприятието	45
V.	МОНТИРАНЕ НА УРЕДИТЕ ЗА РЕГИСТРИРАНЕ НА ДАННИТЕ ЗА ДВИЖЕНИЕТО	45
1.	Монтиране	45
2.	Монтажна табелка	46
3.	Пломбиране	46
VI.	КОНТРОЛ, ИНСПЕКТИРАНЕ И РЕМОНТИ	47
1.	Одобряване на монтьорите или цеховете	47
2.	Проверка на новите или поправените инструменти.	47
3.	Инспектиране на монтиранията	47
4.	Периодични инспекции	47
5.	Измерване на грешките	48
6.	Поправки.....	48
VII.	ИЗДАВАНЕ НА КАРТИТЕ	48
VIII.	ТИПОВО ОДОБРЕНИЕ НА УРЕДИТЕ ЗА РЕГИСТРИРАНЕ НА ДАННИ ЗА ДВИЖЕНИЕТО И НА ТАХОГРАФСКИТЕ КАРТИ	48
1.	Общи положения.....	48
2.	Сертификат относно сигурността	49
3.	Сертификат за функциониране	49
4.	Сертификат за възможност за взаимна работа	49
5.	Сертификат за типово одобрение	50
6.	Извънредна процедура: първи тестове за възможност за взаимна работа	50

Допълнение 1. Речник на данните

Допълнение 2. Характеристики на тахографските карти

Допълнение 3. Пиктограми

Допълнение 4. Тиражиране на хартиен носител

Допълнение 5. Изобразяване

Допълнение 6. Външни интерфейси

Допълнение 7. Протоколи за предаване на данните

Допълнение 8. Протоколи за еталониране

Допълнение 9. Типово одобрение — Списък на минимално изискваните изпитания

Допълнение 10. Общи цели относно сигурността

Допълнение 11. Общи механизми относно сигурността

I. ОПРЕДЕЛЕНИЯ

За целите на настоящото приложение се разбира:

а) **под „активиране“:**

фазата, по време на която уредите за регистриране на данните за движението стават напълно функционални и могат да извършват всички функции, включително и тези, които са свързани със сигурността;

Активирането на уредите за регистриране на данните за движението изисква използването на цехова карта и въвеждането на нейния идентификационен код.

б) **под „удостоверяване“:**

функция, предназначена да установи и провери определена самоличност;

в) **под „автентичност“:**

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

г) **под „вграден тест“:**

изпитания, които могат да се извършват при заявка, чрез действие на оператора или посредством външна апаратура.

д) **под „календарен ден“:**

ден, който обхваща времето от 00.00 часа до 24.00 часа; всички календарни дни са свързани с координираното универсално време (HUC);

е) **под „еталониране“:**

осъвременяването или потвърждаването на параметрите на превозното средство, които трябва да се запазят в паметта; параметрите на превозното средство включват неговото идентифициране (идентификационен номер, регистрационен номер и държавата-членка, извършила регистрацията) и характеристиките на превозното средство [w, k, l, размер на гумите, регулировка на ограничителя на скоростта (при необходимост), час по координираното универсално време, километраж];

Еталонирането на уреди за регистриране на данните за движението изисква използването на цехова карта.

ж) **под „номер на карта“:**

16-позиционен цифрово-буквен код, който представлява уникалният идентификационен номер на тахографска карта в определена държава-членка; този номер съдържа индекс за пореден номер (при необходимост), индекс за замяна и индекс за подновяване на валидността;

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

з) **под „индекс за пореден номер на картата“:**

14-позиционен цифрово-буквен знак от картовия номер, използван за различаване на картите, издадени на определено дружество или организация, имаща право да използва няколко тахографски карти; това дружество или организация се идентифицира посредством 13-те първи позиции на картовия номер;

и) **под „индекс за подновяване на валидността на картата“:**

16-позиционен цифрово-буквен знак от картовия номер, който нараства при всяко подновяване на валидността на картата на тахографа;

й) **под „индекс за замяна на картата“:**

15-позиционен цифрово-буквен знак от картовия номер, който нараства при всяка замяна на тахографската карта;

к) **под „характеристичен коефициент на превозното средство“:**

цифровата характеристика, която посочва стойността на изходния сигнал, излъчен от тази част на превозното средство, която го свързва с уредите за регистриране на данните за движението (изходящ вал на скоростната кутия или ос) докато превозното средство изминава разстояние от един километър при стандартни условия на изпитание (виж глава VI.5). Характеристичният коефициент се изразява в импулси на километър (w: ... imp/km);

л) **под „карта на предприятие“:**

тахографска карта, издадена от властите на определена държава-членка на собственика или на ползвателя на превозни средства, оборудвани с уреди за регистриране на данните за движението;

Тази карта идентифицира предприятието и позволява изобразяването, прехвърлянето и отпечатването на данните, съхранени в уредите за регистриране на данните за движението, достъпът до които е блокиран от това предприятие.

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

цифровата характеристика, която дава стойността на входния сигнал, необходим за указване и записване на изминатото разстояние от един километър; тази константа се изразява в импулси на километър ($w = \dots \text{imp/km}$);

н) **„времето за непрекъснато кормуване“ се изчислява от уредите за регистриране на данните за движението като ⁽¹⁾:**

сумата от времената на кормуване, натрупани от определен водач от края на последния му период НА РАЗПОЛОЖЕНИЕ или на ПРЕКЪСВАНЕ/ПОЧИВКА или на период С НЕИЗВЕСТНА ДЕЙНОСТ ⁽²⁾ от 45 или повече минути (този период може да бъде разделен на няколко периода от 15 или повече минути). При изчисленията се държи сметка при необходимост за предишните дейности, записани на картата на водача. Когато водачът не е вкарал картата си, изчисленията се основават на данните, записани в паметта по време на периода, когато не е била вкарана никаква карта, като се съотнасят към съответното четящо устройство;

о) **под „карта на контролор“:**

тахографска карта, издадена от властите на определена държава-членка на компетентен контролен орган;

Тази карта идентифицира контролния орган и евентуално лицето, отговарящо за контрола, като позволява достъп до данните, съхранени в паметта или на картата на водача, с цел тяхното прочитане, отпечатване и/или прехвърляне.

п) **под „общо време на прекъсване“ се има предвид изчислената от уредите за регистриране на данните за движението продължителност като ⁽¹⁾:**

общото време на прекъсване в работата е сумата от периодите НА РАЗПОЛОЖЕНИЕ или на ПРЕКЪСВАНЕ/ПОЧИВКА или на периодите на НЕИЗВЕСТНА ДЕЙНОСТ ⁽²⁾ от 15 или повече минути на определен водач от края на последния му период НА РАЗПОЛОЖЕНИЕ или на ПРЕКЪСВАНЕ/ПОЧИВКА или на НЕИЗВЕСТНА ДЕЙНОСТ ⁽²⁾ от 45 или повече минути (този период може да бъде разделен на няколко периода от 15 или повече минути).

При изчисленията се държи сметка при необходимост за предишните дейности, записани на картата на водача. Периодите на неизвестна дейност с отрицателно времетраене (начало на периода с неизвестна дейност > края на периода с неизвестна дейност) поради припокриване на времеви периоди между две различни апаратури за контрол не се вземат предвид при изчисленията.

Когато водачът не е вкарал картата си, изчисленията се основават на данните, записани в паметта по време на периода, когато не е била вкарана никаква карта, като се отнасят към съответното четящо устройство;

р) **под „памет“:**

устройство за съхраняване на данни в електронен вид, монтирано в уредите за регистриране на данните за движението;

с) **под „електронен подпис“:**

данните, свързани с блок от данни или негова криптографска трансформация, което позволява на получателя на този блок да получи доказателство за неговата автентичност и цялост;

т) **под „прехвърляне на данни“:**

копирането с цифров подпис на част или на цялата съвкупност от данни, съхранени в паметта на блока, монтиран на превозното средство или в паметта на тахографската карта;

Прехвърлянето на данни не може в никакъв случай да променя или изтрива данните.

⁽¹⁾ Този начин на изчисление на времето на непрекъсната работа и на общото време на прекъсване в работата позволява на уредите за регистриране на данните за движението да извършат своевременно предупреждение относно времетраенето на непрекъсната работа. Той не предопределя юридическото тълкуване на тези времетраения.

⁽²⁾ Периодите на НЕИЗВЕСТНА ДЕЙНОСТ на водача съответстват на периодите, през които картата на водача не е била вкарана в уредите за регистриране на данните за движението и относно които не е извършено никакво ръчно въвеждане на данни относно дейността на водача.

- у) **под „карта на водача“:**
тахографска карта, издадена от властите на определена държава-членка на определен водач;
Картата на водача показва самотичността на водача и позволява съхраняването на данни относно дейностите, извършвани от него.
- ф) **под „реална окръжност на търкаляне на гумите“:**
средната стойност от разстоянията, изминати от всяко от колелата, задвижващи превозното средство (двигателните колела) по време на едно пълно завъртане. Измерването на тези разстояния се извършва при стандартни условия (виж глава VI.5) и се изразява под формата $l = \dots$ мм. Производителите на превозни средства могат да заменят измерването на тези разстояния с теоретично изчисление, което взема предвид разпределянето на теплото на превозното средство върху осите в състояние без товар и в движение ⁽¹⁾. Методите на това теоретично изчисление трябва да бъдат одобрени от националния компетентен орган;
- х) **под „събитие“:**
анормална операция, открита от уредите за регистриране на данните за движението и която може да бъде причинена от опит за неоторизирана намеса;
- ц) **под „аномалия“:**
анормална операция, открита от уредите за регистриране на данните за движението и която може да бъде причинена от неправилно функциониране или повреда на уредите;
- ч) **под „монтиране“:**
монтирането на уредите за регистриране на данните за движението на превозно средство;
- ш) **под „датчик за движение“:**
елемент от уредите за регистриране на данните за движението, излъчващ сигнал, характеризиращ скоростта и/или изминатото разстояние от превозното средство;
- щ) **под „невалидна карта“:**
карта, която се възприема като дефектна или при която първоначалното удостоверяване е неуспешно, или на която датата за начало на валидността все още не е достигната, или при която е преминала датата на валидност;
- аа) **под „извън обсег“:**
всички случаи, при които използването на уредите за регистриране на данните за движението не е необходимо, съгласно Регламент (ЕИО) № 3820/85 на Съвета;
- бб) **под „превишаване на допустимата скорост“:**
надвишаването на допустимата за съответното превозно средство скорост през всеки период над 60 секунди, по време на който измерената скорост на превозното средство надвишава фиксираната в Директива 92/6/ЕИО от 10 февруари 1992 г. относно монтирането и използването и границите на Общността на ограничителите на скоростта на някои категории моторни превозни средства ⁽²⁾, гранична стойност, използвана за регулиране на устройството за ограничаване на скоростта;
- вв) **под „периодично инспектиране“:**
поредица от контролни операции, предназначени да удостоверят, че уредите за регистриране на данните за движението функционират правилно и че нейните регулировки отговарят на параметрите на превозното средство;
- гг) **под „принтер“:**
компонент на уредите за регистриране на данните за движението, който позволява отпечатването на данните, съхранени в нея;
- дд) **под „уред за регистриране на данните за движението“:**
съвкупността от оборудване, предназначено да бъде монтирано на пътните превозни средства с цел да указва, записва и съхранява автоматично или полуавтоматично данни относно движението на тези превозни средства и относно някои периоди на работа на водачите;

⁽¹⁾ Директива 97/27/ЕО на Европейския парламент и на Съвета от 22 юли 1997 г. относно масите и размерите на някои категории моторни превозни средства и техните ремаркета, която изменя и допълва Директива 70/156/ЕИО (ОВ L 233, 25.08.1997 г., стр. 1).

⁽²⁾ ОВ L 57, 2.3.1992 г., стр. 27.

е) под „подновяване“:

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

жж) под „поправка“:

всяка поправка на датчик за движение или на блок, монтиран на превозното средство, която налага прекъсването на връзката с неговото електрическо захранване или с други компоненти на уредите за регистриране на данните за движението, или която налага той да бъде отворен;

зз) под „замяна“:

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

ии) под „сертифициране относно сигурността“:

процесът, състоящ се в удостоверяването от страна на организация за сертифициране ITSEC ⁽¹⁾, че уредите за регистриране на данните за движението (или компонент от тази апаратура) или тахографската карта отговарят на изискванията за сигурност, определени в допълнение 10, отнасящо се до общите цели относно сигурността;

ий) под „автотест“:

автоматичните тестове, извършвани периодично от уредите за регистриране на данните за движението с цел откриване на съществуващи аномалии;

кк) под „тахографска карта“:

карта с памет, предназначена да бъде използвана от уреди за регистриране на данните за движението; тахографските карти позволяват идентифицирането от страна на уредите за регистриране на данните за движението на притежателя на картата (или на групата, към която той принадлежи), както и прехвърлянето и съхраняването на данни; една тахографска карта може да принадлежи към един от следните типове:

- карта на водача,
- карта на контрольор,
- цехова карта,
- карта на предприятие;

лл) под „типово одобрение“:

процес, провеждан от определена държава-членка и целящ да удостовери, че уредите за регистриране на данните за движението (или на компонент от тях) или тахографската карта отговарят на изискванията на настоящия регламент;

мм) под „размери на гумите“:

указването на размерите на гумите (външни задвижващи колела) съгласно Директива 92/23/ЕИО ⁽²⁾;

нн) под „идентификация на превозното средство“:

номерата, позволяващи идентифицирането на превозното средство: регистрационният номер с указване на държавата-членка, извършила регистрацията, и идентификационен номер на превозното средство ⁽³⁾;

оо) под „блок, монтиран на превозното средство (UEV)“:

уредите за регистриране на данните за движението с изключение на датчика за движение и кабелите за връзка с този датчик; блокът, монтиран на превозното средство, може да бъде под формата на един-единствен елемент или на няколко компонента, които са разположени на различни места в превозното средство, при положение, че отговаря на изискванията относно сигурността на настоящия регламент;

⁽¹⁾ Препоръка 95/144/ЕО на Съвета от 7 април 1995 г. относно общите критерии за оценка на сигурността на информационните технологии (ОВ L 93, 26.04.1995 г., стр. 27).

⁽²⁾ ОВ L 129, 14.05.1992 г., стр. 95.

⁽³⁾ Директива 76/114/ЕИО, 18.12.1975 г. (ОВ L 24, 30.01.1976 г., стр. 1).

пп) **под „седмица“ за целите на изчисленията в уредите за регистриране на данните за движението:**

период между 00.00 часа по координираното универсално време в понеделник и 24.00 часа в неделя;

рр) **под „цехова карта“:**

тахографска карта, издадена от властите на определена държава-членка на производител на уреди за регистриране на данните за движението, на монтажист, на производител на превозни средства или на цех, одобрен от тази държава-членка;

цеховата карта идентифицира лицето, на което и издадена, и позволява изпитването и еталонирането на уредите за регистриране на данните за движението, и/или прехвърлянето на данни от тази апаратура.

II. ОБЩИ ХАРАКТЕРИСТИКИ И ФУНКЦИИ НА УРЕДИТЕ ЗА РЕГИСТРИРАНЕ НА ДАННИТЕ ЗА ДВИЖЕНИЕТО

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

1. Общи характеристики

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

001 Апаратурата за контрол включва кабели, датчик за движение и блок, който е монтиран на превозното средство.

002 Блокът, който е монтиран на превозното средство, включва блок за обработка на данните, електронна памет, часовник, работещ в реално време, два конектора за карти с памет (водач и помощник-водач), принтер, дисплей, визуално устройство за предупреждение, конектор за еталониране/прехвърляне на данни, както и устройства, позволяващи въвеждането на данни от потребителя.

Уредите за регистриране на данните за движението могат да бъдат свързани с други устройства чрез допълнителни конектори.

003 Всяко вмъкване или свързване на каква да е функция или устройство/а, одобрено/и или не, в или към уреди за регистриране на данните за движението, не трябва да предизвиква интерференции или да бъде в състояние да предизвиква интерференции с правилното и сигурно функциониране на уредите за регистриране на данните за движението, нито с устройствата, упоменати в регламента.

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

004 Уредите за регистриране на данните за движението дават изборителни права за достъп до данните и функциите според типа и/или самоличността на потребителя.

Уредите за регистриране на данните за движението записват и съхраняват данни в своята памет и на тахографските карти.

Тези функции се осигуряват при спазване на Директива 95/46/ЕО на Европейския парламент и на Съвета от 24 октомври 1995 г. за защита на физическите лица при обработването на лични данни и за свободното движение на тези данни ⁽¹⁾.

2. Функции

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

- надзор над поставянията и изважданията на картите,
- измерване на скоростта и на изминатото разстояние,
- измерване на времето,
- проследяване на дейностите, извършвани от водача,
- наблюдение на положението при кормуване,
- ръчно въвеждане на данни от водача:
 - местоположение в началото и/или в края на дневните периоди на работа,
 - ръчно въвеждане на дейностите, извършвани от водача,
 - записване на особените условия,

⁽¹⁾ ОВ L 281, 23.11.1995 г., стр. 31.

- управление на блокировките от страна на предприятието при достъпа до данните,
- проследяване на контролните дейности,
- откриване на събития и/или на аномалии,
- вградени автотестове,
- четене на данните, съхранени в паметта,
- записване и съхраняване на данните в паметта,
- четене на тахографските карти,
- записване и съхраняване на данните в тахографските карти,
- изобразяване на данните,
- отпечатване,
- предупреждаване,
- прехвърляне на данни към външни медии,
- извеждане на данни към допълнителни външни устройства,
- еталониране,
- сверяване на часовника.

3. Режими на функциониране

006 Уредите за регистриране на данните за движението трябва да осигуряват следните четири режима на функциониране:

- оперативен режим,
- контролен режим,
- режим на еталониране,
- режим „Предприятие“.

007 Апаратурата за контрол трябва да преминава към следните режими на функциониране според валидната тахографска карта, поставена в картовия интерфейс:

Режим на функциониране		Четящо устройство „водач“				
		Няма карта	Карта на водача	Карта на контрольор	Цехова карта	Карта на предприятие
Четящо устройство „помощник-водач“	Няма карта	Оперативен	Оперативен	Контролен	Еталониране	Предприятие
	Карта на водача	Оперативен	Оперативен	Контролен	Еталониране	Предприятие
	Карта на контрольор	Контролен	Контролен	Контролен (*)	Оперативен	Оперативен
	Цехова карта	Еталониране	Еталониране	Оперативен	Еталониране (*)	Оперативен
	Карта на предприятие	Предприятие	Предприятие	Оперативен	Оперативен	Предприятие (*)

008 (*) При подобен случай уредите за регистриране на данните за движението използват единствено тахографската карта, поставена в четящото устройство „водач“.

- 009 Уредите за регистриране на данните за движението трябва да отхвърлят невалидните карти, като обаче позволява изобразяването, отпечатването или прехвърлянето на данните, находящи се на карта с изтекъл срок.
- 010 Всички функции, изброени в II.2, трябва да бъдат налични при всички режими на функциониране, с изключение на:
- функцията за еталониране, която е достъпна единствено в режим на еталониране,
 - функцията за сверяване на часовника, която е ограничена в режимите, различни от режим на еталониране,
 - ръчното въвеждане на данни от водача, което е достъпно единствено в оперативен режим и в режим на еталониране,
 - функцията за управление на блокировките от страна на предприятието при достъпа до данните, която е достъпна единствено в режим предприятие,
 - проследяването на контролните дейности, което е достъпно единствено в контролен режим,
 - функцията за прехвърляне на данни, която не е достъпна в оперативен режим (освен в случаите, предвидени в изискване 150).
- 011 Уредите за регистриране на данните за движението могат да извличат всяка информация с цел нейното изобразяване, отпечатване или прехвърляне към външни интерфейси, освен:
- в оперативен режим, при който всяко идентифициране на самоличност [фамилно име и лично/и име/на], което не отговаря на поставената тахографската карта, ще бъде маскирано и всеки номер на карта, който не отговаря на вкараната тахографска карта, ще бъде частично маскиран (една буква на всеки две, отляво надясно),
 - в оперативен режим, при който данните относно водача (изисквания 081, 084 и 087) могат да бъдат извлечени единствено за периодите, които не са блокирани от друго предприятие (като това, което се идентифицира с първите 13 цифри от номера на картата на предприятието),
 - когато в уредите за регистриране на данните за движението не е поставена никаква карта, могат да бъдат извлечени данните относно водача единствено за същия ден и осемте предишни календарни дни.

4. Сигурност

Системата за сигурност цели да предпази паметта така, че да възпрепятства неоторизиран достъп до нея или на промяна на данните и да открие опитите за такава промяна, да предпазва целостта и автентичността на данните, които се обменят между датчика за движение и блока, монтиран на превозното средство, както и между уредите за регистриране на данните за движението и тахографските карти, и също така да проверява целостта и автентичността на прехвърляните данни.

- 012 С цел да се подсигури сигурността на системата, уредите за регистриране на данните за движението трябва да отговаря на изискванията, уточнени в общите цели относно сигурността, отнасящи се до датчика за движение и блока, който е вграден на превозното средство (допълнение 10).

III. КОНСТРУКТИВНИ И ФУНКЦИОНАЛНИ ИЗИСКВАНИЯ ОТНОСНО УРЕДИТЕ ЗА РЕГИСТРИРАНЕ НА ДАННИТЕ ЗА ДВИЖЕНИЕТО

1. Проследяване на вкарването и на изваждането на картите

- 013 Уредите за регистриране на данните за движението трябва да осигуряват проследяване на поставянията и на изважданията на картите.
- 014 При поставянето на карта уредите за регистриране на данните за движението проверяват нейната валидност и идентифицират типа ѝ.
- 015 Уредите за регистриране на данните за движението трябва да бъдат така конструирани, че тахографските карти да бъдат блокирани в правилно положение в картовия интерфейс.
- 016 Изваждането на тахографската карта е възможно единствено когато превозното средство е в спряло положение и след като релевантните данни за съхранени на нея. Изваждането на тахографската карта изисква адекватно действие на потребителя.

2. Измерване на скоростта и на изминатото разстояние

- 017 Тази функция осигурява непрекъснато измерване и позволява указването на стойността в километри, съответстваща на общото разстояние, изминато от превозното средство.
- 018 Тази функция осигурява непрекъснато измерване и позволява указването на скоростта на превозното средство.

- 019 Функцията за измерване на скоростта на превозното средство трябва също така да указва дали превозното средство е в движение или в покой. Смята се, че превозното средство е в движение, щом функцията засече повече от 1 имп./сек. за период от не по-малко от 5 секунди, които импулси идват от датчика за движение, в противен случай се приема, че превозното средство е в покой.

Устройствата за указване на скоростта и изминатите километри, монтирани на всяко превозно средство, оборудвано с отговаряща на настоящия регламент уреди за регистриране на данните за движението, трябва да отговарят на изискванията относно максималния толеранс, фиксирани в настоящото приложение (глави III, (2) (1) и III (2) (2).

2.1. Измерване на изминатото разстояние

- 020 Изминатото разстояние може да бъде измервано така, че:
- или да взема предвид и движението напред, и движението на заден ход,
 - или да взема предвид единствено движението напред.
- 021 Апаратурата за контрол трябва да измерва изминатото разстояние от 0 до 9999 999,9 км.
- 022 Измереното разстояние трябва да бъде в границите на следния толеранс (разстояния от най-малко 1000 м):
- ± 1 % преди монтирането,
 - ± 2 % по време на монтирането и на периодичните инспекции,
 - ± 4 % по време на работа.
- 023 Разделителната способност при измерване на разстоянието трябва да бъде по-висока или равна на 0,1 км.

2.2. Измерване на скоростта

- 024 Уредите за регистриране на данните за движението трябва да измерват скоростта от 0 до 220 км/ч.
- 025 С цел да гарантира максимален толеранс относно указаната скорост от ± 6 км/ч по време на работа и като се взема предвид:
- толеранс от ± 2 км/ч относно колебанията на входящия сигнал (колебания, дължащи се на гумите и т.н.),
 - толеранс от ± 1 км/ч по отношение на измерванията, извършени по време на монтирането и на периодичните инспекции,
- уредите за регистриране на данните за движението трябва, при скорости в диапазона от 20 до 180 км/ч и при характеристични коефициенти на превозното средство в диапазона от 4000 и 25 000 имп/км, да може да измерва скоростта с толеранс от ± 1 км/ч (при постоянна скорост).
- Забележка: Точността при съхраняването на данните налага наличието на допълнителен толеранс от $\pm 0,5$ км/ч по отношение на скоростта, записана в уредите за регистриране на данните за движението.
- 025a Скоростта трябва да бъде измервана правилно, в рамките на нормалния толеранс, две секунди след смяна на предавката, когато скоростта се е променила с ритъм, достигащ до 2 м/сек².
- 026 Разделителната способност при измерване на скоростта трябва да бъде по-висока или равна на 1 км/ч.

3. Измерване на времето

- 027 Функцията за измерване на времето трябва да осигурява непрекъснато измерване и изобразяването в цифров вид на датата и на часа по координираното универсално време.
- 028 Датата и часът по координираното универсално време трябва да бъдат използвани от целите уреди за регистриране на данните за движението (при записването на данни, отпечатването на хартия, обмена на данни, тяхното изобразяване, ...).
- 029 С цел визуализиране на местното време е необходимо да може да се променя часовата разлика на изобразяваното време посредством стъпка от по 30 минути.
- 030 Неточността на устройството за измерване на времето не трябва да надвишава ± 2 секунди на ден при условията на типовото одобрение.
- 031 Разделителната способност при измерване на времето трябва да бъде по-висока или равна на 1 секунда.
- 032 Измерването на времето не трябва да бъде повлияно при прекъсване с продължителност, по-малка от 12 месеца, на външното електрическо захранване, при условията на одобрение.

4. Проследяване на дейностите, извършвани от водача

- 033 Тази функция трябва да осигурява постоянно и отделно наблюдение над дейностите, извършвани от един водач и един помощник-водач.
- 034 Дейността, извършвана от водача, трябва да бъде ШОФИРАНЕ, РАБОТА, НА РАЗПОЛОЖЕНИЕ или ПРЕКЪСВАНЕ/ПОЧИВКА.
- 035 Необходимо е водачът и/или помощник-водачът да може да избира ръчно дейността РАБОТА, НА РАЗПОЛОЖЕНИЕ или ПРЕКЪСВАНЕ/ПОЧИВКА.
- 036 Когато превозното средство е в движение, дейността ШОФИРАНЕ трябва да бъде автоматично избрана за водача и дейността НА РАЗПОЛОЖЕНИЕ трябва да бъде автоматично избрана за помощник-водач.
- 037 Когато превозното средство спре, дейността РАБОТА трябва да бъде автоматично избрана за водача.
- 038 Ако първата промяна на дейността настъпи през 120-те секунди след автоматичното избиране на дейността РАБОТА поради спирането на превозното средство, тя трябва да бъде смятана като настъпила в момента на спиране на превозното средство (и следователно трябва да анулира преминаването към дейността РАБОТА).
- 039 Тази функция трябва да предава промените в дейността към функциите, осигуряващи записването на информацията, с разделителна способност от една минута.
- 040 Като се взема предвид една календарна минута, всяка дейност КОРМУВАНЕ, извършваща се по време на част от такава минута, се приема като цяла минута, по време на която се извършва дейността КОРМУВАНЕ.
- 041 Като се взема предвид една календарна минута, всяка дейност КОРМУВАНЕ, извършваща се по време на предишната минута и на минутата, която следва непосредствено след нея, се приема като цяла минута, по време на която се извършва дейността КОРМУВАНЕ.
- 042 Като се взема предвид една календарна минута, която не се смята за минута на извършване на дейност КОРМУВАНЕ по смисъла на горните изисквания, цялата минута се счита като част от дейността, която съпада с най-дългата непрекъсната дейност, извършваща се по време на минутата (или на най-скорешната дейност при наличие на няколко дейности с еднаква продължителност).
- 043 Тази функция трябва също така да позволява постоянното проследяване на непрекъснатото работно време и на общото време на прекъсване на водача.

5. Наблюдение на положението при кормуване

- 044 Тази функция трябва да осигурява постоянно и автоматично наблюдение на положението при кормуване.
- 045 Положението при кормуване ЕКИПАЖ трябва да бъде избрано, когато две валидни карти на водач са поставени в уредите, а положението при кормуване САМ трябва да бъде избрано при всички останали случаи.

6. Ръчно въвеждане на данни от водача

6.1. Записване на местоположението в началото и/или в края на дневния период на работа

- 046 Тази функция трябва да позволява записването на местоположението в началото и/или в края на дневния период на работа на водача и/или на помощник-водача.
- 047 Под местоположение се разбира страната и, при необходимост, съответната област.
- 048 При изваждането на карта на водач (или на цехова карта), уредите за регистриране на данните за движението трябва да покани водача/помощник-водача да въведе „Местоположение, в което завършва дневният период на работа“.
- 049 Апаратурата за контрол трябва да позволява пренебрегването на това съобщение.
- 050 Трябва да бъде възможно въвеждането на местоположението в началото и/или в края на дневния период на работа без карта или в момент, различен от момента на вкарване или изваждане на определена карта.

6.2. Ръчно въвеждане на дейностите, извършвани от водача

- 050a По време на поставянето на карта на водача (или на цехова карта) и единствено в този момент уредите за регистриране на данните за движението трябва:
- да напомнят на притежателя на картата датата и часа на последното изваждане на картата му,
 - да поискат от притежателя на картата да укаже дали поставянето на картата представлява продължаването на текущия период на дневна работа.

Апаратурата за контрол трябва да позволява на притежателя на картата да пренебрегне този въпрос или да отговори утвърдително или отрицателно:

- при положение, че притежателят на картата пренебрегне този въпрос, уредите за регистриране на данните за движението трябва да поканят водача да укаже „местоположението, в което започва дневният период на работа“. Апаратурата за контрол трябва да дава възможност да не се указва нищо. Ако е указано местоположение, то се записва в паметта, както и на тахографската карта, и се свързва с часа на поставяне на картата,
 - при положение, че притежателят на картата отговори утвърдително или отрицателно на този въпрос, уредите за регистриране на данните за движението трябва да поканят притежателя на картата да въведе ръчно вида на своите дейности, както и датата и часа на началото и края на всяка от тях, като се избира единствено между дейностите РАБОТА, НА РАЗПОЛОЖЕНИЕ, ПРЕКЪСВАНЕ/ПОЧИВКА, и единствено по време на периода между последното изваждане на картата и настоящото ѝ поставяне и без да се позволява припокриване по време на тези дейности. Прилагат се следните процедури:
 - при положение, че притежателят на картата отговори утвърдително на този въпрос, уредите за регистриране на данните за движението трябва да го поканят да въведе ръчно вида на своите дейности в хронологичен ред за периода между последното изваждане на картата и настоящото ѝ поставяне. Процесът завършва, когато въведенният ръчно час за края на определена дейност съответства на часа на поставяне на картата,
 - при положение, че притежателят на картата отговори отрицателно на този въпрос, уредите за регистриране на данните за движението:
 - трябва да поканят притежателя на картата да въведе ръчно вида на своите дейности в хронологичен ред от часа на изваждане на картата до края на съответния период на дневна работа (или на дейностите, свързани с въпросното превозно средство, при положение, че периодът на дневна работа продължава на лист със запис на данни). Така че уредите за регистриране на данните за движението, преди да позволят на притежателя на картата да въведе ръчно всяка от дейностите, трябва да го поканят да укаже дали часът за край на последната записана дейност представлява край на последния период на работа (виж забележката по-долу),
- Забележка: При положение, че притежателят на картата не декларира часа на завършване на последния период на работа и въведе ръчно дейност, часът на завършване на която отговаря на часа на поставяне на картата, уредите за регистриране на данните за движението:
- приемат, че периодът на дневна работа е завършил при започването на първия период на ПОЧИВКА (или който остава С НЕИЗВЕСТНА ДЕЙНОСТ) след изваждането на картата или в момента на това изваждане, ако не е въведен никакъв период на почивка (и ако няма период, който да остава с С НЕИЗВЕСТНА ДЕЙНОСТ),
 - приемат, че часът на начало (виж по-долу) съответства на часа на поставяне на картата,
 - изпълнява описаните по-долу етапи,
- след това, ако часът на завършване на въпросния период на работа се различава от часа на изваждане на картата или ако местоположението за край на дневния период на работа не е въведено в този момент, апаратурата трябва да покани притежателя на картата да „потвърди или да въведе местоположението за край на съответния период на дневна работа“ (уредите за регистриране на данните за движението трябва да позволяват да не се въвежда нищо); ако местоположението за край на дневния период на работа е въведено, то трябва да се запише на тахографската карта само ако е различно от въведеното по време на изваждането на картата (при необходимост), и да бъде свързано с часа на прекратяване на периода на работа,
 - след това апаратурата трябва да покани притежателя на картата „да въведе час на начало“ на текущия период на дневна работа (или на дейностите, свързани със съответното превозно средство в случаите, когато притежателят на картата преди това е използвал лист със запис на данни по време на този период), и поканва притежателя на картата „да въведе местоположение на начало на периода на дневна работа“ (уредите за регистриране на данните за движението трябва да позволяват да не се въвежда нищо); ако местоположението е въведено, то трябва да се запише на тахографската карта и да бъде свързано с горепосочения час на започване; ако този час съответства на часа на поставяне на картата, местоположението също така се записва в паметта,
 - след това, ако този час на започване е различен от часа на поставяне на картата, съобщение трябва да покани притежателя на картата да въведе ръчно вида на своите дейности в хронологичен ред от този час на започване до часа на поставяне на картата; процесът завършва, когато часът на прекратяване на определена въведена ръчно дейност съответства на часа на поставяне на картата,
 - в този случай уредите за регистриране на данните за движението трябва да позволяват на притежателя на картата да променя всяка въведена дейност, включително нейното валидиране, чрез избиране на специална команда, която не позволява каквато и да е по-нататъшна промяна,
 - ако един утвърдителен или отрицателен отговор не е последван от въвеждане на дейности, уредите за регистриране на данните за движението трябва да приемат, че притежателят на картата е пренебрегнал въпроса.

По време на тази процедура уредите за регистриране на данните за движението трябва да изчакват въвеждането на данни в продължение на следните периоди:

- при липса на взаимодействие с интерфейса човек/машина на апаратурата в продължение на една минута (с визуално и евентуално звуково предупреждение след 30 секунди), или,
- в момента на изваждането на картата или на поставяне на друга карта на водача (или на цехова карта), или,
- в момента на тръгване на превозното средство,

като в този случай уредите за регистриране на данните за движението приемат за валидна всяка вече въведена информация.

6.3. *Записване на особените условия*

050b Апаратурата за контрол трябва да позволява на водача да въвежда в реално време следните две особени условия:

- „ИЗВЪН ОБСЕГ“ (начало, край),
- „ПЪТУВАНЕ С ФЕРИБОТ/ВЛАК“.

Не може да съществува „ПЪТУВАНЕ С ФЕРИБОТ/ВЛАК“, когато условието „ИЗВЪН ОБСЕГ“ е отворено.

Отвореното условие „ИЗВЪН ОБСЕГ“ трябва задължително да бъде затворено автоматично в случай на изваждане или на поставяне на карта на водач.

7. *Управление на блокировките от страна на предприятието при достъпа до данните*

- 051 Тази функция трябва да позволява управлението на блокировките, поставени от определено предприятие, с цел да ограничат и запазят единствено за него достъпа до данните в режим „предприятие“.
- 052 Блокировките от страна на предприятието се състоят в дата и час на начало (блокиране) и дата и час на край (отблокиране), свързани с идентифицирането на дружеството чрез номера на картата на предприятието (по време на блокирането).
- 053 Блокирането и отблокирането са възможни единствено в реално време.
- 054 Отблокирането може да се извърши единствено от предприятието, което е извършило блокирането (така, както то се идентифицира с първите 13 цифри на номера на картата на предприятието), или,
- 055 отблокирането се извършва автоматично, когато друго предприятие извършва блокиране.
- 055a В случай че едно предприятие извършва блокиране и ако предишното блокиране е било извършено от същото предприятие, се приема, че предишното блокиране не е отблокирано и че е все така в сила.

8. *Проследяване на контролните дейности*

- 056 Тази функция осигурява проследяването на дейностите по ИЗОБРАЗЯВАНЕ, ОТПЕЧАТВАНЕ и ПРЕХВЪРЛЯНЕ НА ДАННИ от блока, монтиран на превозното средство, или от картата, провеждани в контролен режим.
- 057 Тази функция осигурява също така проследяването на дейностите по КОНТРОЛ НА СКОРОСТТА в контролен режим. Приема се, че се извършва контрол на скоростта, когато в контролен режим се изпраща съобщение „превишаване на допустимата скорост“ към принтера или екрана, или когато данни, свързани със „събития или аномалии“ се прехвърлят от паметта на блока, монтиран на превозното средство.

9. *Откриване на събития и/или на аномалии*

- 058 Тази функция открива следните събития и/или аномалии:

9.1. *Събитие „Поставяне на невалидна карта“*

- 059 Това събитие се предизвиква от поставянето на невалидна карта и/или когато валидността на определена вкарана карта изтича.

9.2. **Събитие „Конфликт, предизвикан от картата“**

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

Конфликт, предизвикан от картата		Четящо устройство „водач“				
		Няма карта	Карта на водача	Карта на контрольор	Цехова карта	Карта на предприятие
Четящо устройство „помощник-водач“	Няма карта					
	Карта на водача				X	
	Карта на контрольор			X	X	X
	Цехова карта		X	X	X	X
	Карта на предприятие			X	X	X

9.3. **Събитие „Припокриване на времев период“**

061 Това събитие се предизвиква когато датата/часът на последното изваждане на определена карта на водач така, както те са изобразени на картата, са по-късни от датата/часа, които се отчитат в момента от уредите за регистриране на данните за движението, в която картата е поставена.

9.4. **Събитие „Кормуване без съответната карта“**

062 Това събитие се предизвиква от всяка от отбелязаните с хикс комбинации от тахографски карти в долната таблица, когато дейността на водача става „КОРМУВАНЕ“, или в случай на промяна на режима на функциониране, когато дейността на водача е КОРМУВАНЕ:

Кормуване без съответната карта		Четящо устройство „водач“				
		Няма карта	Карта на водача	Карта на контрольор	Цехова карта	Карта на предприятие
Четящо устройство „помощник-водач“	Няма карта	X		X		X
	Карта на водача	X		X	X	X
	Карта на контрольор	X	X	X	X	X
	Цехова карта	X	X	X		X
	Карта на предприятие	X	X	X	X	X

9.5. **Събитие „Поставяне на карта по време на кормуване“**

063 Това събитие се предизвиква от поставянето на тахографска карта в което и да е четящо устройство, когато дейността на водача е КОРМУВАНЕ.

9.6. **Събитие „Неправилно приключена последна сесия“**

064 Това събитие се предизвиква, когато уредите за регистриране на данните за движението открият при поставянето на карта, че въпреки разпоредбите на параграф III, (1), предишната сесия не е била приключена правилно (картата е била извадена, преди всички необходими данни да са били записани на нея). Това събитие се отнася единствено до картите на водача и цеховите карти.

9.7. **Събитие „Превишаване на допустимата скорост“**

065 Това събитие се предизвиква при всяко превишаване на допустимата скорост.

9.8. Събитие „Прекъсване на електрическото захранване“

- 066 Това събитие се предизвиква в режим, различен от режима на еталониране, при прекъсване за повече от 200 милисекунди на електрическото захранване на датчика за движение и/или на блока, монтиран на превозното средство. Прагът на прекъсване се фиксира от производителя. Прекъсването на електрическото захранване, дължащо се на пускането на двигателя в ход, не трябва да предизвиква появата на това събитие.

9.9. Събитие „Грешка в данните относно движението“

- 067 Това събитие се предизвиква при прекъсване на нормалния поток от данни между датчика за движение и блока, монтиран на превозното средство и/или в случай на грешка, свързана с целостта на данните или с удостоверяването им по време на техния обмен между датчика за движение и блока, монтиран на превозното средство.

9.10. Събитие „Опит за нарушаване на сигурността“

- 068 Това събитие се предизвиква при настъпване на всяко друго събитие, засягащо сигурността на датчика за движение и/или на блока, монтиран на превозното средство така, както е уточнено в рамките на общите цели за сигурност относно тези компоненти при режимите, различни от режима на еталониране.

9.11. Аномалия „Карта“

- 069 Тази аномалия се предизвиква при аномалия на тахографска карта по време на нейното функциониране.

9.12. Аномалия „Уреди за регистриране на данните за движението“

- 070 Тази аномалия се предизвиква при следните аномалии при режимите, различни от режима на еталониране:

- вътрешна аномалия на блока, монтиран на превозното средство,
- аномалия на принтера,
- аномалия при изобразяването на данните,
- аномалия при прехвърлянето на данните,
- аномалия на датчика.

10. Автотестове и вградени тестове

- 071 Апаратурата за контрол открива сама аномалиите чрез автотестове и вградени тестове според долната таблица:

Елемент за тестване	Автотест	Вграден тест
Програмно осигуряване (софтуер)		Цялост
Памет за данни	Достъп	Достъп, цялост на данните
Устройства за картов интерфейс	Достъп	Достъп
Клавиатура		Ръчен контрол
Принтер	(по избор на производителя)	Принтер
Дисплей		Визуален контрол
Прехвърляне на данни (извършван единствено по време на прехвърлянето)	Правилно функциониране	
Датчик	Правилно функциониране	Правилно функциониране

11. Четене на паметта

- 072 Апаратурата за контрол трябва да може да чете всички данни, съхранени в паметта й.

12. Запис и съхраняване в паметта

За целите на настоящия параграф:

- под „365 дни“ се разбират 365 календарни дена на средна дейност на водачите в определено превозно средство. Средната дейност на ден в едно превозно средство се определя като най-малко 6 водача или помощник-водача, 6 цикъла на поставяне/изваждане на карти и 256 смени на дейностите. Така че „365 дни“ включват най-малко 2190 водача/помощник-водача и 93 440 смени на дейностите,
- часовете се записват с точност от 1 минута, освен ако не е предвидено друго,
- километричните стойности се записват с точност от 1 километър,
- скоростите се записват с точност от 1 км/ч.

- 073 На данните, записани в паметта, не трябва да може да се повлияе при прекъсване на външното електрическо захранване с продължителност, по-малка от 12 месеца, при условията на типовото одобрение.
- 074 Уредите за регистриране на данните за движението трябва да могат да записват и съхраняват по подразбиране или при задаване следните данни в своята памет:

12.1. Данни за идентификация на уредите

12.1.1. Данни за идентификация на блока, монтиран на превозното средство

- 075 Апаратурата за контрол трябва да може съхранява в своята памет следните данни относно идентификацията на блока, монтиран на превозното средство:
- име на производителя,
 - адрес на производителя,
 - номер на компонентите,
 - сериен номер,
 - номер на версията на софтуера,
 - дата на инсталиране на версията на софтуера,
 - година на производство на уредите,
 - номер на одобрение.
- 076 Данните относно идентификацията на блока, монтиран на превозното средство, се записват и съхраняват еднократно от производителя на блока, освен данните относно софтуера и сертификационния номер, които могат да бъдат променени при инсталиране на нови версии на софтуера.

12.1.2. Данни за идентификация на датчика за движение

- 077 Датчикът за движение трябва да може да съхранява в паметта си следните идентификационни данни:
- име на производителя,
 - номер на компонентите,
 - сериен номер,
 - номер на одобрение,
 - идентификатор на вградения компонент за сигурност (например сериен номер на вътрешния микропроцесор),
 - идентификатор на операционната система (например номер на версията на софтуера).

- 078 Идентификационните данни относно датчика за движение се записват и съхраняват еднократно в датчика от неговия производител.
- 079 Блокът, монтиран на превозното средство, трябва да може да записва и съхранява в паметта си следните идентификационни данни относно датчика за движение, към който той е свързан:
- сериен номер,
 - номер на одобрение,
 - дата на първото свързване.

12.2. Елементи, свързани със сигурността

- 080 Апаратурата за контрол трябва да може да съхранява следните елементи, свързани със сигурността:
- европейски публичен ключ,
 - сертификат на държавата-членка,
 - сертификат на уредите,
 - частен ключ на уредите.

Елементите, свързани със сигурността на уредите за регистриране на данните за движението, се вграждат в уредите от производителя на блока, монтиран на превозното средство.

12.3. Данни, свързани с поставянето и изваждането на картата на водача

- 081 За всеки цикъл на поставяне-изваждане на определена карта на водача (или на цехова карта) уредите за регистриране на данните за движението записват и съхраняват в своята памет:
- фамилията и името (името и презимето) на притежателя на картата така, както те са съхранени на картата,
 - номера на картата, държавата-членка, която я е издала, и датата на валидност, така както са съхранени на картата,
 - датата и часа на поставянето,
 - километража на превозното средство в момента на поставяне на картата,
 - четящото устройство, в което е поставена картата,
 - датата и часа на изваждането ѝ,
 - километража на превозното средство в момента на изваждане на картата,
 - следната информация относно последното превозно средство, използвано от водача така, както тя е съхранена на картата:
 - номер и държава-членка, извършила регистрацията на превозното средство,
 - дата и час на изваждането на картата,
 - код, указващ дали притежателят на картата е въвел ръчно дейностите по време на поставянето на картата или не.
- 082 Паметта трябва да може да запазва тези данни в продължение най-малко на 365 дни.
- 083 Когато капацитетът за съхраняване на информация е изчерпан, новите данни заместват най-старите данни.

12.4. Данни относно дейността на водача

084 Апаратурата за контрол записва и съхранява в паметта си всяка промяна на дейността на водача и/или на помощник-водача, и/или всяка промяна на обстановката по време на кормуване, и/или всяко поставяне или изваждане на определена карта на водач или на цехова карта:

- обстановка по време на кормуване (ЕКИПАЖ, САМ),
- четящо устройство (ВОДАЧ, ПОМОЩНИК-ВОДАЧ),
- положение на картата в четящото устройство (ПОСТАВЕНА/НЕПОСТАВЕНА) (виж забележката),
- дейност (КОРМУВАНЕ, НА РАЗПОЛОЖЕНИЕ, РАБОТА, ПРЕКЪСВАНЕ/ПОЧИВКА),
- дата и час на промяната.

Забележка: ПОСТАВЕНА означава, че определена валидна карта на водач (или цехова карта) е поставена в четящото устройство. НЕПОСТАВЕНА означава обратното, тоест че никаква валидна карта на водач (или цехова карта) не е поставена в четящото устройство (например, поставена е карта на предприятие или не е поставена никаква карта).

Забележка: Въведените ръчно от водача данни относно дейността не се записват в паметта.

085 Паметта трябва да може да запазва данните относно дейността на водача в продължение най-малко на 365 дни.

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

12.5. Местоположение в началото и/или в края на дневните периоди на работа

087 Когато водачът/помощник-водачът въвежда местоположението в началото и/или в края на дневния период на работа, уредите за регистриране на данните за движението записват и съхраняват в паметта си:

- при необходимост, номера на картата на водача/помощник-водача и на държавата-членка, която е издала картата,
- датата и часа на поставянето (или датата и часа, свързани с поставянето, когато то се извършва по време на процедурата по ръчно поставяне),
- типа на въвежданата информация (начало или край на дневен период на работа, условия на въвеждане на информацията),
- въведени страна и област,
- километраж на превозното средство.

088 Паметта трябва да може да запазва данните относно началото и/или края на дневните периоди на работа в продължение на най-малко 365 дни (като се предполага, че ежедневно се извършват две въвеждания от всеки водач).

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

12.6. Километраж

090 Уредите за регистриране на данните за движението записват в своята памет километража на превозното средство и съответната дата на всеки календарен ден в полунощ.

091 Паметта трябва да може да запазва ежедневните записи, извършени в полунощ на брояча на километрите, в продължение най-малко на 365 дни.

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

12.7. Подробни записи на скоростта

093 Апаратурата за контрол записва и съхранява в паметта си моментната скорост на превозното средство и датата и часа за всяка секунда през най-малко 24-те последни часа, по време на които превозното средство е било в движение.

12.8. Данни, свързани със събитията

За целите на настоящата точка времето се записва с точност до секунда.

094

Апаратурата за контрол записва и съхранява в своята памет следните данни относно всяко засечено събитие, съгласно следните правила на съхранение на информацията:

Събитие	Правила на съхраняване	Данни, които се записват при всяко събитие
Конфликт с картите	— 10-те най-скорошни събития.	— дата и час на начало на събитието, — дата и час на край на събитието, — тип, номер и държава-членка, издала всяка една от двете карти, които са причина за конфликта.
Кормуване без съответната карта	— най-продължителното събитие за всеки от десетте последни дена на проява на това събитие, — петте най-продължителни събития по време на последните 365 дни.	— дата и час на начало на събитието, — дата и час на край на събитието, — тип, номер и държава-членка, издала картата, вкарана в началото и/или в края на събитието — брой подобни събития, възникнали същия ден.
Въвеждане на карта по време на кормуване	— последното събитие за всеки от десетте последни дена на проява на това събитие.	— дата и час на събитието, — тип, номер и държава-членка, издала картата, — брой подобни събития, възникнали същия ден.
Неправилно приключване на последната сесия	— 10-те най-скорошни събития.	— дата и час на поставянето на картата, — тип, номер и държава-членка, издала картата, — данни относно последната сесия така, както фигурират на картата: — дата и час на поставянето, — номер и държава-членка, извършила регистрацията на превозното средство.
Превишаване на допустимата скорост ⁽¹⁾	— най-сериозното събитие (тоест събитието, при което е достигната най-висока средна скорост) през десетте последни дена на проява на това събитие, — петте най-сериозни събития по време на последните 365 дни, — първото събитие, настъпило след последното еталониране.	— дата и час на начало на събитието, — дата и час на край на събитието, — максимална скорост, измерена по време на събитието, — средна аритметична скорост, измерена по време на събитието, — тип, номер и държава-членка, издала картата (при необходимост), — брой подобни събития, възникнали същия ден.

⁽¹⁾ Уредите за регистриране на данните за движението трябва също така да записват и съхраняват в паметта си:

- датата и часа на последния КОНТРОЛ ЗА ПРЕВИШАВАНЕ НА ДОПУСТИМАТА СКОРОСТ,
- датата и часа на първото превишаване на скоростта след този КОНТРОЛ ЗА ПРЕВИШАВАНЕ НА ДОПУСТИМАТА СКОРОСТ,
- броя на превишаванията на скоростта след последния КОНТРОЛ ЗА ПРЕВИШАВАНЕ НА ДОПУСТИМАТА СКОРОСТ.

Събитие	Правила на съхраняване	Данни, които се записват при всяко събитие
Прекъсване на електрическото захранване ⁽¹⁾	<ul style="list-style-type: none"> — най-продължителното събитие за всеки от десетте последни дена на проява на това събитие, — петте най-продължителни събития по време на последните 365 дни. 	<ul style="list-style-type: none"> — дата и час на начало на събитието, — дата и час на край на събитието, — тип, номер и държава-членка, издала картата, вкарана в началото и/или в края на събитието, — брой подобни събития, възникнали същия ден.
Грешка при данните относно движението	<ul style="list-style-type: none"> — най-продължителното събитие за всеки от десетте последни дена на проява на това събитие, — петте най-продължителни събития по време на последните 365 дни. 	<ul style="list-style-type: none"> — дата и час на начало на събитието, — дата и час на край на събитието, — тип, номер и държава-членка, издала картата, поставена в началото и/или в края на събитието, — брой подобни събития, възникнали същия ден.
Опит за нарушаване на сигурността	<ul style="list-style-type: none"> — 10-те най-скорошни събития за всеки тип събитие. 	<ul style="list-style-type: none"> — дата и час на начало на събитието (при необходимост), — дата и час на край на събитието, — тип, номер и държава-членка, издала картата, поставена в началото и/или в края на събитието, — тип събитие.

095 ⁽¹⁾ Тези данни могат да бъдат записани единствено по време на възстановяването на електрическото захранване, като часовете могат да бъдат отчетени с точност до една минута.

12.9. Данни относно аномалиите

За целите на настоящата точка времето се записва с точност до секунда.

096 Уредите за регистриране на данните за движението трябва да се опитват да записват и съхраняват в своята памет следните данни относно всяка засечена аномалия съгласно следните правила на съхранение на информацията:

Аномалия	Правила на съхраняване	Данни, които се записват при всяка аномалия
Аномалия на картата	<ul style="list-style-type: none"> — десетте последни аномалии на картата на водача. 	<ul style="list-style-type: none"> — дата и час на начало на аномалията, — дата и час на край на аномалията, — тип, номер и държава-членка, издала картата.
Аномалия на уредите за регистриране на данните за движението	<ul style="list-style-type: none"> — десетте най-скорошни аномалии за всеки тип аномалия, — първата аномалия след последното еталониране. 	<ul style="list-style-type: none"> — дата и час на начало на аномалията, — дата и час на край на аномалията, — тип на аномалията, — тип, номер и държава-членка, издала картата, поставена в началото/в края на аномалията.

12.10. Данни относно еталонирането

- 097 Уредите за регистриране на данните за движението записват и съхраняват в своята памет данните, имащи отношение:
- към параметрите на еталонирането, известни в момента на активирането,
 - към нейното най-първо еталониране след активирането ѝ,
 - към нейното първо еталониране на превозното средство, на което се намира в момента (така, както то е идентифицирано от идентификационния номер на превозното средство),
 - към петте най-скорошни еталонирания (когато няколко еталонирания се извършват в рамките на един календарен ден, единствено последното се архивира).
- 098 За всяко от еталониранията се записват следните данни:
- предмет на еталонирането (активиране, първо инсталиране, инсталиране, периодичен контрол, друго),
 - име и адрес на монтажния цех,
 - номера на цеховата карта, държавата-членка, която я е издала, и датата на валидност на картата,
 - идентификация на превозното средство,
 - актуализирани или потвърдени параметри: w , k , l , размер на гумите, регулировка на ограничителя на скоростта, брояч на километрите (старо и ново показание), дата и час (старо и ново показание).
- 099 Датчикът за движение записва и съхранява в паметта си следните данни относно монтирането му:
- първо свързване към блок, монтиран на превозното средство (дата, час, сертификационен номер на блока, сериен номер на блока),
 - последно свързване към блок, монтиран на превозното средство (дата, час, сертификационен номер на блока, сериен номер на блока).

12.11. Данни относно сверяването на часовника

- 100 Апаратурата за контрол записва и съхранява в своята памет данните, имащи отношение към:
- последното сверяване на часовника,
 - 5-те най-значителни корекции от последното еталониране насам,
- извършени в режим на еталониране извън рамките на периодичното еталониране (определение е).
- 101 За всяко от сверяванията на часовника се записват следните данни:
- дата и час, старата стойност,
 - дата и час, новата стойност,
 - име и адрес на цеха,
 - номер на цеховата карта, държавата-членка, която я е издала, и датата на валидност на картата.

12.12. Данни относно контролните дейности

- 102 Уредите за регистриране на данните за движението записват и съхраняват в своята памет следните данни, имащи отношение към последните 20 контролни дейности:
- дата и час на извършения контрол,
 - номер на картата на контрольора и държавата-членка, която я е издала,
 - тип на контрола (изобразяване на данните и/или отпечатване на хартия и/или прехвърляне на данни от блока и/или прехвърляне на данни от картата).

103 При извършване на прехвърляне на данни се записват също така датите на най-отдалечения и на най-близкия ден във времето, данните относно които са прехвърлени.

12.13. Данни относно блокировките от страна на предприятието при достъпа до данните

104 Уредите за регистриране на данните за движението записват и съхраняват в своята памет следните данни, имащи отношение към последните 20 блокировки, извършени от предприятията:

- дата и час на блокировката,
- дата и час на отблокирането,
- номер на картата на предприятие и държавата-членка, която я е издала,
- име и адрес на предприятието.

12.14. Данни относно прехвърлянето на данни

105 Уредите за регистриране на данните за движението записват и съхраняват в своята памет следните данни, имащи отношение към последното прехвърляне на данни от паметта към външни медии в режим „Предприятие“ или „Еталониране“:

- дата и час на прехвърлянето на данни,
- номер на картата на предприятие или на цеховата карта и държава-членка, която я е издала,
- име и адрес на предприятието или на цеха.

12.15. Данни относно особените условия

105a Уредите за регистриране на данните за движението записват и съхраняват в своята памет следните данни, имащи отношение към особените условия:

- дата и час на въвеждането,
- тип на особеното условие.

105b Паметта трябва да може да запазва данните относно особените условия в продължение най-малко на 365 дни (като се предполага, че ежедневно се отваря и затваря едно условие на ден). Когато капацитетът за съхраняване на информация е изчерпан, новите данни заместват най-старите данни.

13. Четене на тахографските карти

106 Уредите за регистриране на данните за движението трябва при необходимост да могат да четат от тахографските карти данните, които са необходими за:

- идентифициране на типа на картата, на притежателя на картата, на използваното преди това превозно средство, на датата и часа на последното изваждане на картата и на дейността, която е била избрана в този момент,
- проверка, че последната сесия е била приключена правилно,
- изчисляване на времето на непрекъснато кормуване на водача, общото време на прекъсване и на общото време на кормуване за предишната и настоящата седмица,
- отпечатване на заявките за печат на данните, записани на карта на водач,
- прехвърляне на данни от карта на водач към външна медия.

107 При грешка в четенето уредите за регистриране на данните за движението правят нов опит, максимум до три пъти, и при наличие на повтарящ се неуспех на операцията обявява картата за дефектна и невалидна.

14. Запис и съхраняване върху тахографски карти

108 Апаратурата за контрол регулира „данните за сесията“ на картата на водача или на цеховата карта непосредствено след въвеждането на картата.

- 109 Уредите за регистриране на данните за движението актуализират данните, записани на валидна карта на водач, цехова карта или карта на контролор с всички необходими данни относно периода на вкарване на картата и отнасящи се до притежателя ѝ. Данните, записвани върху тези карти, са уточнени в раздел IV.
- 109a Апаратурата за контрол актуализира данните относно дейността на водача и местоположението (така, както са указани в параграфи 5.2.5 и 5.2.6 на глава IV), записани на валидните карта на водач и/или цехова карта, с ръчно въведените от притежателя на картата данни относно дейността на водача и местоположението.
- 110 Актуализирането на данните, записани на тахографските карти, се извършва по такъв начин, че когато това е необходимо, като се има предвид реалният капацитет на съхраняване на информация на картата, най-новите данни заместват най-старите данни.
- 111 При грешка в записването уредите за регистриране на данните за движението правят нов опит, максимум до три пъти, и при наличие на повтарящ се неуспех на операцията обявява картата за дефектна и невалидна.
- 112 Преди освобождаването на карта на водач и след като всички релевантни данни са съхранени на картата, уредите за регистриране на данните за движението нулират „данните за сесията“.

15. Изобразяване на данните

- 113 При изобразяването трябва да се виждат най-малко 20 символа.
- 114 Размерът на символите трябва да бъде най-малко 5 мм височина и 3,5 мм широчина.
- 114a Устройството за визуализиране трябва да приема латинските символи 1 и гръцките символи така, както са определени в части от 1 и 7 на стандарт ISO 8859, както е указано в допълнение 1 на глава IV „Набор от символи“. При изобразяването може да се използват опростени графи (например символите с ударения могат да се изобразяват без тях или малките букви могат да се изобразяват като главни букви).
- 115 При изобразяването трябва да се използва незаслепяващо осветяване.
- 116 Показанията трябва да се виждат от външната страна на уредите за регистриране на данните за движението.
- 117 Уредите за регистриране на данните за движението трябва да могат да изобразяват:
- данни относно аномалиите,
 - данни относно предупрежденията,
 - данни относно достъпа до менютата,
 - други данни, поискани от потребителя.
- Уредите за регистриране на данните за движението могат да изобразяват допълнителна информация при положение, че тя се отличава ясно от горепосочените информации.
- 118 При изобразяването на данните на уредите за регистриране на данните за движението трябва да се използват пиктограмите или комбинациите от пиктограми, изброени в допълнение 3. Могат да се използват допълнителни пиктограми или комбинации от пиктограми при положение, че те се отличават ясно от горепосочените пиктограми или комбинации от пиктограми.
- 119 Устройството за изобразяване трябва винаги да бъде включено, когато превозното средство е в движение.
- 120 Уредите за регистриране на данните за движението могат да имат ръчна или автоматична функция за изключване на устройството за изобразяване на данните, когато превозното средство е в покой.

Форматът на изобразяване на данните е указан в допълнение 5.

15.1. Изобразяване по подразбиране

- 121 Когато не трябва да се изобразява никаква друга информация, уредите за регистриране на данните за движението изобразяват по подразбиране следните показания:
- местно време (координирано универсално време + корекция, фиксирана от водача),
 - режим на функциониране,
 - активната в момента дейност на водача и на помощник-водача,

- информация относно водача:
 - ако неговата дейност в момента е КОРМУВАНЕ, времето на непрекъснато кормуване и общото време на прекъсване,
 - ако неговата дейност в момента не е КОРМУВАНЕ, продължителността на активната в момента дейност (от момента на избирането ѝ) и общото време на прекъсване,
 - информация относно помощник-водача:
 - продължителността на неговата дейност (от момента на избирането ѝ).
- 122 Изобразяването на данните относно всеки водач трябва да бъде ясно, просто и недвусмислено. Когато данните относно водача и помощник-водача не могат да бъдат изобразени едновременно, уредите за регистриране на данните за движението трябва да изобразяват по подразбиране информацията, отнасяща се до водача, и трябва да позволяват на потребителя да изобрази информацията относно помощник-водача.
- 123 Когато широчината на изобразяването не е достатъчна за визуализиране по подразбиране на режима на функциониране, уредите за регистриране на данните за движението трябва да изобразяват за кратко време новия режим при всяка негова промяна.
- 124 Уредите за регистриране на данните за движението трябва да изобразяват за кратко време името на притежателя на картата при въвеждане на нова карта.
- 124а Когато е отворено условие „ИЗВЪН ОБСЕГ“, съответната пиктограма трябва да се появи, за да укаже, че това условие е отворено (активната в момента дейност на водача може да не се изобразява в същото време).

15.2. **Изобразяване на предупреждение**

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

15.3. **Меню за достъп**

- 126 Уредите за регистриране на данните за движението трябва да съдържат командите, които са необходими в рамките на съответното меню за достъп.

15.4. **Изобразяване на други данни**

- 127 Трябва да бъде възможно изобразяването по заявка на:
 - датата и часа по координираното универсално време,
 - режима на функциониране (ако не е указан по подразбиране),
 - времето на непрекъснато кормуване и общото време на прекъсване за водача,
 - времето на непрекъснато кормуване и общото време на прекъсване за помощник-водача,
 - времето на непрекъснато кормуване на водача за предишната и настоящата седмица,
 - времето на непрекъснато кормуване на помощник-водача за предишната и настоящата седмица,
 - съдържанието на една от съответните 6 разпечатки на хартиен носител, което да бъде в същия формат като разпечатката на хартиения носител.
- 128 Изобразяването на съдържанието на разпечатката на хартия е последователно, ред по ред. Ако широчината на изобразяването е по-малка от 24 символа, потребителят може да визуализира цялата информация чрез съответен способ (на няколко реда, изобразяване във вид на безконечен списък, ...) Редовете при отпечатването на хартия, предвидени за ръчното изписване на информация, могат да бъдат изпуснати.

16. **Отпечатване**

- 129 Апаратурата за контрол трябва да може да отпечатва информацията, записана в паметта ѝ и/или на тахографските карти така, че да могат да се получат следните разпечатвания на хартия:
 - записаните на картата дейности на водача,
 - записаните на блока, монтиран на превозното средство, дейности на водача,

- записаните на картата събития и аномалии,
- записаните на блока, монтиран на превозното средство, събития и аномалии,
- техническите данни,
- превишаванията на допустимата скорост.

Подробностите относно формата и съдържанието, които трябва да се спазват при тези отпечатвания на хартия, са уточнени в допълнение 4.

В края на разпечатването на хартия може да фигурират допълнителни данни.

Могат също така да се извършват и други разпечатвания на хартия с помощта на уредите за регистриране на данните за движението при положение, че те са ясно различими от шестте изброени по-горе.

- 130 Разпечатванията на хартия „Дейности на водача, фигуриращи на картата“ и „Събития и аномалии, фигуриращи на картата“ могат да се извършват единствено когато в уредите за регистриране на данните за движението е въведена карта на водач или цехова карта. Уредите за регистриране на данните за движението актуализират данните, записани на въпросната карта, преди да стартира отпечатването.
- 131 За да извърши разпечатване на хартия на „Дейности на водача, фигуриращи на картата“ или на „Събития и аномалии, фигуриращи на картата“ уредите за регистриране на данните за движението трябва:
- или да изберат автоматично картата на водача или цеховата карта, ако само една от тези карти е поставена в нея,
 - или да има команда, позволяваща избирането на картата-източник на данните, или да избере картата, поставена в четящото устройство „водач“, ако тези две карти са поставени в уредите за регистриране на данните за движението.
- 132 Принтерът трябва да може да отпечата 24 символа на ред.
- 133 Минималният размер на символите е 2,1 мм височина и 1,5 мм широчина.
- 133a Принтерът трябва да приема латинските символи 1 и гръцките символи, определени в части 1 и 7 на стандарт ISO 8859, както е указано в допълнение I на глава IV, „Набор от символи“.
- 134 Принтерите трябва също така да са с такава конструкция, че степента на четливост на разпечатването на хартия да бъде достатъчна, за да се избегне всяка двусмисленост при четене.
- 135 Разпечатките на хартия трябва да запазват размерите и съдържанието си при нормалните условия на влажност (10 – 90 %) и на температура.
- 136 Хартията, използвана от уредите за регистриране на данните за движението, трябва да има съответен знак за типово одобрение и указание за типа/овете апаратура/и за контрол, с който/които може да бъде използвана. Разпечатките на хартия трябва да остават лесно четливи и разпознаваеми при нормалните условия на съхранение, що се отнася до светлинния интензитет, влажността и температурата, в продължение на най-малко една година.
- 137 Също така трябва да бъде възможно да се пише на ръка върху тези документи, например при полагане на подписа на водача.
- 138 При прекъсване на захранването с хартия по време на разпечатването и след новото зареждане с хартия, уредите за регистриране на данните за движението трябва да започнат отново разпечатването отначало или то да продължи оттам, откъдето е прекъсвало, като ясно прави връзка с частта, разпечатана до този момент.

17. Предупреждения

- 139 Апаратурата за контрол трябва да предупреждава водача, когато открие някакво събитие и/или аномалия.
- 140 Предупреждението относно прекъсване на захранването с електричество може да бъде забавено до момента на възстановяване на захранването.
- 141 Уредите за регистриране на данните за движението предупреждават водача 15 минути преди и по време на надвишаването на непрекъснатото време на кормуване от 4 часа и 30 минути.
- 142 Предупрежденията трябва да бъдат визуални. Освен визуалните предупреждения могат да се извършват и звукови предупреждения.

- 143 Визуалните предупреждения трябва да бъдат ясно различни от потребителя, да се появяват в зрителното поле на водача и да бъдат лесно четливи както през деня, така и през нощта.
- 144 Визуалните предупреждения могат да бъдат вградени в уредите за регистриране на данните за движението, или да бъдат изведени извън тях.
- 145 В последния случай те трябва да съдържат символа „Т“ и да бъдат с оранжев цвят.
- 146 Предупрежденията трябва да имат продължителност не по-малка от 30 секунди, освен ако потребителят удостовери приемането им чрез натискане на който и да е бутон от уредите за регистриране на данните за движението. Това първо удостоверяване на приемането на предупреждението не трябва да изтрива изобразяването на причината за съобщението, визирано в следващия параграф.
- 147 Причината за съобщението трябва да бъде изобразена на уредите за регистриране на данните за движението и да остане видима, докато потребителят удостовери приемането ѝ с помощта на специален код или команда на уредите за регистриране на данните за движението.
- 148 Могат да се предвидят допълнителни предупреждения при положение, че те не водят до объркване с тези, които са определени по-горе.

18. Прехвърляне на данни към външни медии

- 149 Уредите за регистриране на данните за движението трябва да позволяват прехвърлянето по заявка на данни, съхранени в паметта ѝ или върху карта на водач, към външни медии, посредством връзка за еталониране/прехвърляне на данни. Уредите за регистриране на данните за движението актуализират данните, записани на въпросната карта, преди да стартира прехвърлянето.
- 150 Освен това, опционално, уредите за регистриране на данните за движението може при всички режими на функциониране да прехвърлят данни посредством друга връзка към предприятие, идентификацията на което се извършва чрез този канал. В подобен случай така прехвърлените данни се подчиняват на правата за достъп, приложими в режим „предприятие“.

- 151 Прехвърлянето на данни не трябва нито да изтрива, нито да променя записаните данни.

Електрическият интерфейс за еталониране и прехвърляне на данни е уточнен в допълнение 6.

Протоколите за прехвърляне на данни са уточнени в допълнение 7.

19. Данни, прехвърляни към допълнителни външни устройства

- 152 Когато уредите за регистриране на данните за движението няма функции за изобразяване на скоростта и/или километража, апаратурата трябва да излъчва изходящи сигнали, позволяващи изобразяването на скоростта на превозното средство и/или общото разстояние, изминато от превозното средство.

- 153 Блокът, монтиран на превозното средство, трябва също така да позволява прехвърлянето на следните данни посредством независима серийна връзка, използвана специално за тази цел, от опционална шина за връзка CAN [ISO 11898 „Пътни превозни средства — обмен на цифрова информация — Управление на високоскоростна комуникационна мрежа (CAN)“] така, че тези данни да могат да бъдат обработени от други електронни устройства, монтирани на превозното средство:

- дата и час по координираното универсално време,
- скорост на превозното средство,
- общо разстояние, изминато от превозното средство (брояч на километрите),
- активната в момента дейност на водача и на помощник-водача,
- евентуално указание, че определена тахографска карта е въведена в четящото устройство „Водач“ и в четящото устройство „Помощник-водач“ и (при необходимост) информацията относно идентифицирането на тези карти (номер и държава-членка, която ги е издала).

Освен този минимален списък, могат да бъдат прехвърлени и други данни.

Когато контактният ключ на превозното средство е в положение ВКЛЮЧЕН ДВИГАТЕЛ, тези данни могат да бъдат прехвърляни постоянно. Когато контактният ключ е в положение СПРЯН ДВИГАТЕЛ, прехвърлянето продължава най-малко за данните, отнасящи се до промените на дейността на водача и на помощник-водача и/или поставянето или изваждането на определена тахографска карта. Ако тези данни не са били прехвърлени, когато контактният ключ на превозното средство е бил в положение СПРЯН ДВИГАТЕЛ, те се прехвърлят, когато контактният ключ се постави отново в положение ВКЛЮЧЕН ДВИГАТЕЛ.

20. Еталониране

- 154 Функцията за еталониране позволява:
- автоматичното свързване на датчика за движение с блока, монтиран на превозното средство,
 - цифровото адаптиране на константата k на уредите за регистриране на данните за движението към характеристичния коефициент w на превозното средство (превозните средства, имащи две или повече предавателни отношения спрямо осите, трябва да бъдат снабдени с комутатор, позволяващ приравняването на тези различни отношения към отношението, за което апаратурата на превозното средство е адаптирана),
 - сверяване на часовника (без ограничение),
 - коригиране на километража,
 - актуализиране на данните за идентификация на датчика за движение, съхранени в паметта,
 - актуализиране или потвърждаване на други параметри, известни на уредите за регистриране на данните за движението: идентифициране на превозното средство, w , l , размер на гумите и регулиране на ограничителя на скоростта при необходимост.
- 155 Свързването на датчика за движение с блока, монтиран на превозното средство се състои най-малкото в:
- актуализиране на данните за монтирането на датчика за движение, намиращи се в него (при необходимост),
 - копиране в паметта на блока, монтиран на превозното средство, на данните за идентификация на датчика за движение.
- 156 Функцията за еталониране трябва да позволява въвеждането на необходимите данни посредством връзката за еталониране/прехвърляне на данни съгласно протокола за еталониране, определен в допълнение 8. Функцията за еталониране може също така да позволява въвеждането на необходимите данни посредством други връзки.

21. Сверяване на часовника

- 157 Функцията за сверяване на часовника трябва да позволява регулирането на часа в границите от една минута на интервали, не по-малки от 7 дена.
- 158 Функцията за сверяване на часовника трябва да позволява регулирането на часа без ограничение в режим на еталониране.

22. Характеристики

- 159 Блокът, монтиран на превозното средство, трябва да може да функционира правилно при диапазон от температури от $-20\text{ }^{\circ}\text{C}$ до $+70\text{ }^{\circ}\text{C}$, а датчикът за движение — при диапазон от температури от $-40\text{ }^{\circ}\text{C}$ до $+135\text{ }^{\circ}\text{C}$. Съдържанието на паметта трябва да бъде запазвано до температури от $-40\text{ }^{\circ}\text{C}$.
- 160 Апаратурата за контрол трябва да може да функционира правилно при диапазон от влажност от 10 % до 90 %.
- 161 Апаратурата за контрол трябва да бъде предпазена от свръхнапрежения, размяна на полюсите на електрическото й захранване и от къси съединения.
- 162 Апаратурата за контрол трябва да отговаря на Директива 95/54/ЕО от 31 октомври 1995 ⁽¹⁾, извършваща привеждане в съответствие с техническия прогрес на Директива 72/245/ЕИО на Съвета ⁽²⁾ относно електромагнитната съвместимост, и трябва да бъде предпазена от електростатични и преходни разряди.

23. Материали

- 163 Всички елементи, съставляващи уредите за регистриране на данните за движението, трябва да бъдат от материали с достатъчна стабилност и механична здравина и да имат стабилни електрически и магнитни характеристики.
- 164 Всички вътрешни части на уредите трябва да бъдат защитени от влага и прах при нормални условия на употреба.
- 165 Блокът, монтиран на превозното средство, трябва да отговаря на равнище на защита IP 40, а датчикът за движение — на равнище на защита IP 64 по смисъла на стандарт IEC 529.

⁽¹⁾ ОВ L 266, 8.11.1995 г., стр. 1.

⁽²⁾ ОВ L 152, 6.7.1972 г., стр. 15.

166 Уредите за регистриране на данните за движението трябва да отговарят на техническите спецификации, прилагани в областта на ергономичността на конструкцията.

167 Уредите за регистриране на данните за движението трябва да бъдат защитени от случайни повреди.

24. Информация, изобразявана допълнително

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

- до цифрата, указваща изминатото разстояние, мерната единица на това разстояние, представена от съкращението „км“;
- до цифрата, показваща скоростта, указанието „км/ч“.

Апаратурата за контрол може също така да бъде свързана по начин, който да позволява изобразяването на скоростта в мили в час, като в този случай мерната единица на скоростта ще е указана от съкращението „mph“.

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

- име и адрес на производителя на уредите,
- фабричен номер, даден от производителя, и година на производство на апаратурата,
- сериен номер на апаратурата,
- знак за одобрение на уредите.

170 Когато наличното пространство е недостатъчно за изобразяване на всички горепосочени информации, указателната табелка трябва да указва най-малко името и фирмения знак на производителя и номера на компонента.

IV. КОНСТРУКТИВНИ И ФУНКЦИОНАЛНИ ИЗИСКВАНИЯ ОТНОСНО ТАХОГРАФСКИТЕ КАРТИ

1. Видими данни

Заглавният лист трябва да съдържа:

171 думите „Карта на водач“ или „Карта на контролор“ или „Цехова карта“ или „Карта на предприятие“, отпечатани с големи букви на официалния(ите) език(езици) на държавата-членка, която е издала картата, според типа карта.

172 същите думи на другите официални езици на Общността, отпечатани на гърба на картата:

ES	TARJETA DEL CONDUCTOR	TARJETA DE CONTROL	TARJETA DEL CENTRO DE ENSAYO	TARJETA DE LA EMPRESA
DK	FØRERKORT	KONTROLKORT	VÆRKSTEDSKORT	VIRKSOMHEDSKORT
DE	FAHRERKARTE	KONTROLLKARTE	WERKSTATTKARTE	UNTERNEHMENSKARTE
EL	ΚΑΡΤΑ ΟΔΗΓΟΥ	ΚΑΡΤΑ ΕΛΕΓΧΟΥ	ΚΑΡΤΑ ΚΕΝΤΡΟΥ ΔΟΚΙΜΩΝ	ΚΑΡΤΑ ΕΠΙΧΕΙΡΗΣΗΣ
EN	DRIVER CARD	CONTROL CARD	WORKSHOP CARD	COMPANY CARD
FR	CARTE DE CONDUCTEUR	CARTE DE CONTROLEUR	CARTE D'ATELIER	CARTE D'ENTREPRISE
GA	CÁRTA TIOMÁNAÍ	CÁRTA STIÚRTHA	CÁRTA CEARDLAINNE	CÁRTA COMHLACHTA
IT	CARTA DEL CONDUCENTE	CARTA DI CONTROLLO	CARTA DELL'OFFICINA	CARTA DELL'AZIENDA
NL	BESTUURDERS KAART	CONTOLEKAART	WERKPLAATSKAART	BEDRIJFSKAART
PT	CARTÃO DE CONDUTOR	CARTÃO DE CONTROLO	CARTÃO DO CENTRO DE ENSAIO	CARTÃO DE EMPRESA
FI	KULJETTAJA KORTILLA	VALVONTA KORTILLA	TESTAUSASEMA KORTILLA	YRITYSKORTILLA
SV	FÖRARKORT	KONTROLLKORT	VERKSTADSKORT	FÖRETAGSKORT

- 174 кода на държавата-членка, която е издала картата, отпечатан в бяло на син фон в правоъгълник, обграден от 12 жълти звезди. Кодовете са следните:
- B Белгия
 - DK Дания
 - D Германия
 - GR Гърция
 - E Испания
 - F Франция
 - IRL Ирландия
 - I Италия
 - L Люксембург
 - NL Нидерландия
 - A Австрия
 - P Португалия
 - FIN Финландия
 - S Швеция
 - UK Великобритания

- 175 особени обозначения относно издадената карта, номерирани, както следва:

	Карта на водача	Карта на контролър	Карта на предприятие или цехова карта
1.	фамилно име на водача	име на органа, извършващ контрол	име на предприятието или на цеха
2.	първо(и) име(на) на водача	фамилно име на контролър (при необходимост)	фамилно име на притежателя на картата (при необходимост)
3.	дата на раждане на водача	Първо/и име/на на контролър (при необходимост)	Първо/и име/на на притежателя на картата (при необходимост)
4. а)	дата на начало на валидността на картата		
б)	дата на изтичане валидността на картата (при необходимост)		
в)	име на органа, който е издал картата (може да бъде отпечатано на страница 2)		
г)	номер, различен от указания в точка 5, по административни причини (опционално)		
5. а)	Номер на свидетелството за управление (към датата на издаване на картата на водача)		
5. б)	Номер на картата		
6.	Снимка на водача	Снимка на контролър (опционално)	-
7.	Подпис на водача	Подпис на притежателя на картата (опционално)	
8.	Обичайно място на пребиваване или пощенски адрес на притежателя на картата (опционално)	Пощенски адрес на органа, извършващ контрол	Пощенски адрес на предприятието или на цеха





- 176 датите се указват под следната форма „дд/мм/гггг“ или „дд.мм.гггг“;

на обратната страна трябва да има:

- 177 легенда на номерата, указани на лицевата страна;

- 178 с изрично писмено съгласие на притежателя на картата информацията, която не е свързана с администрирането на картата, може също така да бъде указана при положение, че не променя с нищо използването на модела като тахографска карта.

МОДЕЛ НА НА ТАХОГРАФСКИТЕ КАРТИ НА ЕВРОПЕЙСКАТА ОБЩНОСТ

ЛИЦЕ	ГРЪБ
<div style="text-align: center;">  </div> <p style="text-align: center;">DRIVER CARD MEMBER STATE</p> <p>1. 2. 3. 4a. 4b. 4c. (4d.) 5a. 5b. 7. (8.)</p> <div style="border: 1px solid black; width: 60px; height: 60px; margin: 10px auto; text-align: center; line-height: 60px;">6.</div>	<p>1. Surname 2. First name(s) 3. Birth date 4a. Date of start of validity of card 4b. Administrative expiry date of card 4c. Issuing authority (4d.) No for national administrative purposes 5a. Driving licence number 5b. Card number 6. Photograph 7. Signature (8.) Address</p> <p style="text-align: center;"><i>Please return to:</i></p> <div style="border: 1px solid black; padding: 2px; text-align: center;">NAME OF AUTHORITY AND ADDRESS</div>
<div style="text-align: center;">  </div> <p style="text-align: center;">CONTROL CARD MEMBER STATE</p> <p>1. (2.) (3.) 4a. (4b.) 4c. (4d.) 5b. (7.) 8.</p> <div style="border: 1px solid black; width: 60px; height: 60px; margin: 10px auto; text-align: center; line-height: 60px;">(6.)</div>	<p>1. Control Body (2.) Surname (3.) First name(s) 4a. Date of start of validity of card (4b.) Administrative expiry date of card 4c. Issuing authority (4d.) No for national administrative purposes 5b. Card number (6.) Photograph (7.) Signature 8. Address</p> <p style="text-align: center;"><i>Please return to:</i></p> <div style="border: 1px solid black; padding: 2px; text-align: center;">NAME OF AUTHORITY AND ADDRESS</div>
<div style="text-align: center;">  </div> <p style="text-align: center;">WORKSHOP CARD MEMBER STATE</p> <p>1. (2.) (3.) 4a. 4b. 4c. (4d.) 5b. (7.) 8.</p> <div style="text-align: right; margin-top: 10px;"> CARTA DELL'OFFICINA WERKPLAATSKAART </div>	<p>1. Workshop Name (2.) Surname (3.) First name(s) 4a. Date of start of validity of card 4b. Administrative expiry date of card 4c. Issuing authority (4d.) No for national administrative purposes 5b. Card number 7. Signature 8. Address</p> <p style="text-align: center;"><i>Please return to:</i></p> <div style="border: 1px solid black; padding: 2px; text-align: center;">NAME OF AUTHORITY AND ADDRESS</div>
<div style="text-align: center;">  </div> <p style="text-align: center;">COMPANY CARD MEMBER STATE</p> <p>1. (2.) (3.) 4a. 4b. 4c. (4d.) 5b. (7.) 8.</p>	<p>1. Company Name (2.) Surname (3.) First name(s) 4a. Date of start of validity of card 4b. Administrative expiry date of card 4c. Issuing authority (4d.) No for national administrative purposes 5b. Card number (7.) Signature 8. Address</p> <p style="text-align: center;"><i>Please return to:</i></p> <div style="border: 1px solid black; padding: 2px; text-align: center;">NAME OF AUTHORITY AND ADDRESS</div>

179 Тахографските карти трябва да бъдат отпечатани на фон със следните цветове:

- карта на водача: бял,
- карта на контролър: син,
- цехова карта: червен,
- карта на предприятието: жълт.

180 Тахографските карти трябва да имат следните елементи на защита срещу подправяне и неотризирана промяна на данните:

- фонов защитен печат с фин релеф и преливащи се цветове,
- припокриване на фоновия защитен печат и на снимката,
- поне една двуцветна линия с микропечат.

- 181 След консултация с Комисията държавите-членки могат да добавят цветовете и надписи, като например националните символи и защитни елементи, без това да накърнява другите разпоредби на настоящото приложение.

2. Сигурност

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

- 182 С цел тази сигурност да съществува реално, тахографските карти трябва да отговарят на изискванията за сигурност, уточнени в общите цели относно сигурността, отнасящи се до тахографските карти (допълнение 10).
- 183 Тахографските карти трябва да могат да бъдат четени от други устройства, като например микрокомпютри.

3. Стандарти

- 184 Тахографските карти трябва да отговарят на следните стандарти:

- ISO/CEI 7810 — Идентификационни карти — физически характеристики,
- ISO/CEI 7816 — Идентификационни карти — Карти с вградена(и) интегрална/и схема/и с контакти:
 - Част 1: Физически характеристики,
 - Част 2: Размери и местоположение на контактите,
 - Част 3: Електрически сигнали и протоколи за предаване на информация,
 - Част 4: Междумодулни команди за обмен на данни,
 - Част 8: Междумодулни команди, свързани със сигурността,
- ISO/CEI 10373 Идентификационни карти — методи на изпитание.

4. Спецификации, свързани с околната среда и електричеството

- 185 Тахографските карти трябва да могат да функционират правилно при всички климатични условия, които нормално се наблюдават на територията на Общността и в минимален температурен диапазон от -25°C до $+70^{\circ}\text{C}$, с моментни пикове до $+85^{\circ}\text{C}$, като „моментни“ означава продължителност под 4 часа и не повече от 100 пъти по време на живота на картата.
- 186 Тахографските карти трябва да могат да функционират правилно при диапазон от влажност от 10 % до 90 %.
- 187 Тахографските карти трябва да могат да функционират правилно през период от пет години, ако те се използват съгласно спецификациите, свързани с околната среда и електричеството.
- 188 По време на своето функциониране тахографските карти трябва да отговарят на Директива 95/54/ЕО на Комисията от 31 октомври 1995 г. относно електромагнитната съвместимост ⁽¹⁾ и трябва да бъдат защитени от електростатични разряди.

5. Съхраняване на данните

За целите на настоящия параграф,

- часовете се записват с точност от 1 минута, освен ако не е предвидено друго,
- километражът на превозното средство се записва с точност до километър,
- скоростите на превозното средство се записват с точност до един километър в час.

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

⁽¹⁾ ОВ L 266, 8.11.1995 г., стр. 1.

- 189 Настоящият параграф уточнява минималния капацитет за съхраняване на данните от различните приложни файлове. Тахографските карти трябва да могат да указват на уредите за регистриране на данните за движението реалния капацитет за съхранение на тези файлове.

Всички допълнителни данни, за които се приема, че могат да бъдат съхранени на тахографската карта във връзка с други евентуално присъстващи на картата приложения, трябва да бъдат съхранени съгласно Директива 95/46/ЕО ⁽¹⁾.

5.1. **Идентифициране на картата и данни относно сигурността**

5.1.1. *Идентифициране на приложенията*

- 190 Тахографските карти трябва да могат да съхраняват следните данни относно идентифициране на приложенията:

- идентифициране на тахографското приложение,
- идентифициране на типа тахографска карта.

5.1.2. *Идентифициране на микропроцесора*

- 191 Тахографските карти трябва да могат да съхраняват следните данни относно идентифицирането на интегралните схеми:

- сериен номер на интегралната схема,
- данни относно производството на интегралната схема.

5.1.3. *Идентифициране на картите с вграден чип*

- 192 Тахографските карти трябва да могат да съхраняват следните данни относно идентифицирането на картите с логика:

- сериен номер на картата (включително данни относно производството),
- сертификационен номер на картата,
- персонално идентифициране на картата,
- идентифициране на интегратора,
- идентификатор на интегралната схема.

5.1.4. *Елементи, свързани със сигурността*

- 193 Тахографските карти трябва да могат да съхраняват следните данни относно идентифицирането на картата:

- европейски публичен ключ,
- сертификат на държавата-членка,
- сертификат на картата,
- частен ключ на картата.

5.2. **Карта на водача**

5.2.1. *Идентифициране на картата*

- 194 Картата на водача трябва да може да съхранява следните данни относно идентифицирането на картата:

- номер на картата,
- държава-членка, изпала картата, името на компетентния орган, извършил издаването, дата на издаването;
- дата на начало на валидността на картата, дата на край на валидността.

⁽¹⁾ ОВ L 281, 23.11.1995 г., стр. 31.

5.2.2. *Идентифициране на притежателя на картата*

- 195 Картата на водача трябва да може да съхранява следните данни относно идентифицирането на притежателя на картата:
- фамилно име на притежателя,
 - име и презиме на притежателя на картата,
 - дата на раждане,
 - обичайно използван език.

5.2.3. *Данни относно свидетелството за управление*

- 196 Картата на водача трябва да може да съхранява следните данни относно свидетелството за управление:
- държава-членка, издала свидетелството за управление, име на компетентния орган, извършил издаването,
 - номер на свидетелството за управление (на датата на издаване на картата).

5.2.4. *Данни относно използваното превозно средство*

- 197 Картата на водача трябва да може да съхранява за всеки календарен ден, в който тя се използва, и за всеки период на използване на определено превозно средство през този ден (периодът на използване включва всички последователни цикли на поставяне/изваждане на картата в превозното средство, като се има предвид самата карта), следните данни:
- дата и час на първото използване на превозното средство (тоест първото въвеждане на картата за този период на употреба на превозното средство, или 00.00 часа, ако периодът на използване обхваща този час),
 - километраж на превозното средство в този момент,
 - дата и час на последното използване на превозното средство (тоест последното изваждане на картата за този период на употреба на превозното средство, или 23.59 часа, ако периодът на използване обхваща този час),
 - километраж на превозното средство в този момент,
 - номер и държава-членка, извършила регистрацията на превозното средство.

- 198 Картата на водача трябва да може да съхранява 84 фиша от този тип.

5.2.5. *Данни относно дейността на водача*

- 199 Картата на водача трябва да може да съхранява следните данни за всеки календарен ден, в който тя се използва, или в който водачът е въвел ръчно дейностите си:
- дата,
 - брояч на присъствените дни (който се увеличава с една единица за всеки от тези календарни дни),
 - общо разстояние, изминато от водача през този ден,
 - положение на водача в 00.00 часа,
 - промени в дейността на водача; и/или промени в обстановката при кормуване, и/или въвеждане или изваждане на картата на водача:
 - обстановка по време на кормуване (ЕКИПАЖ, САМ),
 - четящо устройство (ВОДАЧ, ПОМОШНИК-ВОДАЧ),
 - положение на картата спрямо четящото устройство (ПОСТАВЕНА, НЕПОСТАВЕНА),
 - дейност (КОРМУВАНЕ, НА РАЗПОЛОЖЕНИЕ, РАБОТА, ПРЕКЪСВАНЕ/ПОЧИВКА),
 - час на промяната.

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

- 201 Данните, изброени в изисквания 197 и 199, трябва да бъдат съхранени по начин, позволяващ дейностите да бъдат открити по реда на тяхното настъпване дори в случай на времево припокриване.
- 5.2.6. *Местоположение в началото/в края на дневните периоди на работа*
- 202 Картата на водача трябва да позволява съхраняването на следните данни относно местоположенията на начало и/или на край на дневните периоди на работа, въведени от водача:
- дата и час на въвеждането (или дата и час, свързани с въвеждането, когато то се извършва по време на процедурата по ръчно въвеждане),
 - тип на въвеждането (начало или край, условия на въвеждането),
 - въведени страна и област,
 - километраж на превозното средство.
- 203 Картата на водача трябва да може да съхранява най-малко 42 двойки от този тип.
- 5.2.7. *Данни относно събитията*
- За целите на настоящата точка времето се записва с точност до секунда.
- 204 Картата на водача трябва да позволява съхраняването на данните, свързани със следните събития, засечени от уредите за регистриране на данните за движението по времето, когато картата е поставена:
- припокриване на времеви отрязък (когато картата е причина за събитието),
 - поставяне на карта по време на кормуване (когато това събитие засяга картата),
 - неправилно приключване на предишна сесия (когато това събитие засяга картата),
 - прекъсване на електрическото захранване,
 - грешка в данните относно движението,
 - опит за нарушаване на сигурността.
- 205 Картата на водача трябва да позволява съхраняването на следните данни относно тези събития:
- код на събитието,
 - дата и час на начало на събитието (или на поставянето на картата в случай, че събитието се е извършвало в този момент),
 - дата и час на край на събитието (или на изваждането на картата в случай, че събитието се е извършвало в този момент),
 - номер и държава-членка, извършила регистрацията на превозното средство, в което се е извършило събитието.
- Забележка: Относно събитието „Припокриване на времеви период“:
- датата и часът на началото на събитието трябва да съответстват на датата и часа на изваждане на картата от предишното превозно средство,
 - датата и часът на края на събитието трябва да съответстват на датата и на часа на поставянето на картата в настоящото превозно средство,
 - данните относно превозното средство трябва да съответстват на настоящото превозно средство, в което събитието се е случило.
- Забележка: Относно събитието „Неправилно приключване на предишната сесия“:
- датата и часът на началото на събитието трябва да съответстват на датата и на часа на поставянето на картата, съответствашо на неправилно приключената сесия,
 - датата и часа на края на събитието трябва да съответстват на датата и на часа на поставяне на картата за сесията, по време на която събитието е засечено (текуща сесия),
 - данните относно превозното средство трябва да съответстват на превозно средство, в което сесията не е била приключена правилно.

206 Картата на водача трябва да позволява съхраняването на данните относно 6-те последни събития от всеки тип (тоест 36 събития).

5.2.8. Данни относно аномалиите

За целите на настоящата точка времето се записва с точност до секунда.

207 Картата на водача трябва да позволява съхраняването на данните, свързани със следните аномалии, засечени от уредите за регистриране на данните за движението по времето, когато картата е поставена:

- аномалия на картата (когато картата е причина за аномалията),
- аномалия на уредите за регистриране на данните за движението.

208 Картата на водача трябва да позволява съхраняването на следните данни относно тези аномалии:

- код на аномалията,
- дата и час на начало на аномалията (или на поставянето на картата, в случай че аномалията се е извършвала в този момент),
- дата и час на край на аномалията (или на изваждането на картата, в случай че аномалията се е извършвала в този момент),
- номер и държава-членка, извършила регистрацията на превозното средство, в което се е случила аномалията.

209 Картата на водача трябва да позволява съхраняването на данните относно 12-те последни аномалии от всеки тип (тоест 24 аномалии).

5.2.9. Данни относно контролните дейности

210 Картата на водача трябва да позволява съхраняването на следните данни относно контролните дейности:

- дата и час на извършения контрол,
- номер на картата на контрольора и държавата-членка, която я е издала,
- тип на контрола [изобразяване на данните и/или отпечатване и/или прехвърляне на данни от блока, монтиран на превозното средство и/или прехвърляне на данни от картата (виж забележката)],
- прехвърлен период, при необходимост,
- номер и държава-членка, извършила регистрацията на превозното средство, в което се е извършил контролът.

Забележка: Изискванията за сигурност предполагат, че прехвърлянето от определена карта се записва само ако се извърши посредством уреди за регистриране на данните за движението.

211 Картата на водача трябва да позволява съхраняването на тези данни.

5.2.10. Данни относно сесията за всяка карта

212 Картата на водача трябва да позволява съхраняването на следните данни относно превозното средство, в което е отворена текущата сесия:

- дата и час на отваряне на сесията (тоест на поставяне на картата), с точност до една секунда,
- номер и държава-членка, извършила регистрацията на превозното средство.

5.2.11. Данни относно особените условия

212a Картата на водача трябва да позволява съхраняването на следните данни, свързани с особените условия, въведени, докато картата е поставена (независимо за кое четящо устройство):

- дата и час на въвеждането,
- тип на особеното условие.

- 212 б Картата на водача трябва да позволява съхраняването на 56 фиша от този тип.
- 5.3. Цехова карта**
- 5.3.1. *Елементи, свързани със сигурността*
- 213 Цеховата карта трябва да позволява съхраняването на персонален идентификационен номер.
- 214 Цеховата карта трябва да позволява съхраняването на криптографските ключове, необходими за свързването на датчика за движение към блока, монтиран на превозното средство.
- 5.3.2. Идентифициране на картата**
- 215 Цеховата карта трябва да позволява съхраняването на следните данни относно идентифицирането на картата:
- номер на картата,
 - държавата-членка, издала картата, името на компетентния орган, извършил издаването, дата на издаването;
 - дата на начало на валидността на картата и дата на край на валидността.
- 5.3.3. Идентифициране на притежателя на картата**
- 216 Цеховата карта трябва да позволява съхраняването на следните данни относно идентифицирането на притежателя на картата:
- име на цеха,
 - адрес на цеха,
 - фамилно име на притежателя,
 - име и презиме на притежателя,
 - обичайно използван език.
- 5.3.4. Данни относно използваното превозно средство**
- 217 Цеховата карта трябва да позволява съхраняването на данните относно използваните превозни средства по същия начин като картата на водача.
- 218 Картата на водача трябва да позволява съхраняването на най-малко 4 фиша от този тип.
- 5.3.5. Данни относно дейността на водача**
- 219 Цеховата карта трябва да позволява съхраняването на данните относно дейността на водача по същия начин като картата на водача.
- 220 Цеховата карта трябва да позволява съхраняването на данните относно дейността на водача за най-малко един ден средна дейност на водача.
- 5.3.6. Данни относно края и/или началото на дневните периоди на работа**
- 221 Цеховата карта трябва да позволява съхраняването на данните относно началото и/или края на дневните периоди на работа по същия начин като картата на водача.
- 222 Картата на водача трябва да позволява съхраняването на най-малко 3 двойки данни.
- 5.3.7. Данни относно събитията и аномалиите**
- 223 Цеховата карта трябва да позволява съхраняването на данните относно събитията и аномалиите по същия начин като картата на водача.
- 224 Цеховата карта трябва да позволява съхраняването на трите последни събития от всеки тип (тоест 18 събития) и на шестте последни аномалии от всеки тип (тоест 12 аномалии).
- 5.3.8. Данни относно контролните дейности**
- 225 Цеховата карта трябва да позволява съхраняването на данните относно контролните дейности по същия начин като картата на водача.

5.3.9. Данни относно еталонирането и сверяването на часовника

- 226 Цеховата карта трябва да позволява съхраняването на данните, свързани с еталонирането и/или регулирането на времето, когато картата е поставена в апаратурата.
- 227 Всеки фиш за еталониране трябва да съдържа следните данни:
- предмет на еталонирането (първо инсталиране, инсталиране, периодичен контрол, друго),
 - идентификация на превозното средство,
 - актуализирани или потвърдени параметри [w, k, l, размер на гумите, регулировка на ограничителя на скоростта, брояч на километрите (старо и ново показание), дата и час (старо и ново показание)],
 - идентификация на уредите за регистриране на данните за движението (фабричен и сериен номер на блока, монтиран на превозното средство, сериен номер на датчика за движение).
- 228 Цеховата карта трябва да позволява съхраняването най-малко на 88 фиша от този тип.
- 229 Цеховата карта трябва да има брояч, указващ общия брой на еталониранията, извършени с картата.
- 230 Цеховата карта трябва да има брояч, указващ общия брой на еталониранията, извършени от последното прехвърляне на данни.

5.3.10. Данни относно особените условия

- 230a Цеховата карта трябва да позволява съхраняването на данните относно особените условия по същия начин като картата на водача. Картата на водача трябва да позволява съхраняването на два файла, съдържащи такива данни.

5.4. Карта на контролор

5.4.1. Идентифициране на картата

- 231 Картата на контролора трябва да позволява съхраняването на следните данни относно идентифицирането на картата:
- номер на картата,
 - държава-членка, издала картата, име на компетентния орган, извършил издаването, дата на издаването,
 - дата на начало на валидността на картата, дата на край на валидността (при необходимост).

5.4.2. Идентифициране на притежателя на картата

- 232 Картата на контролора трябва да позволява съхраняването на следните данни относно притежателя на картата:
- име на контролния орган,
 - адрес на контролния орган,
 - фамилно име на притежателя,
 - име и презиме на притежателя,
 - обичайно използван език.

5.4.3. Данни относно контролните дейности

- 233 Картата на контролора трябва да позволява съхраняването на следните данни относно контролните дейности:
- дата и час на извършения контрол,
 - тип на контрола (изобразяване на данните и/или отпечатване и/или прехвърляне на данни от блока, монтиран на превозното средство и/или от картата),

- прехвърлен период (при необходимост),
 - номер и държава-членка, извършила регистрацията на контролираното превозно средство,
 - номер на контролираната карта на водача и държавата-членка, която я е издала.
- 234 Картата на контролора трябва да позволява съхраняването най-малко на 230 фиша от този тип.

5.5. **Карта на предприятие**

5.5.1. *Идентифициране на картата*

- 235 Картата на предприятие трябва да позволява съхраняването на следните данни относно идентифицирането на картата:
- номер на картата,
 - държава-членка, издала картата, име на компетентния орган, извършил издаването, дата на издаването,
 - дата на начало на валидността на картата, дата на край на валидността (при необходимост).

5.5.2. *Идентифициране на притежателя на картата*

- 236 Картата на предприятие трябва да позволява съхраняването на следните данни относно идентифицирането на притежателя на картата:
- име на предприятието,
 - адрес на предприятието.

5.5.3. *Данни относно дейността на предприятието*

- 237 Картата на предприятие трябва да позволява съхраняването на следните данни относно дейностите на предприятието:
- дата и час на дейността,
 - тип на дейността (блокиране и/или отблокиране на блока, монтиран на превозното средство, прехвърляне на данни от блока и/или от картата),
 - прехвърлен период (при необходимост),
 - номер и държава-членка, извършила регистрацията на превозното средство,
 - номер на картата и държава-членка, която я е издала (при прехвърляне на данни от картата).
- 238 Картата на предприятие трябва да позволява съхраняването на 230 фиша от този тип.

V. МОНТИРАНЕ НА УРЕДИТЕ ЗА РЕГИСТРИРАНЕ НА ДАННИТЕ ЗА ДВИЖЕНИЕТО

1. **Монтиране**

- 239 Новите уреди за регистриране на данните за движението се доставят неактивирани на монтьорите или на производителите на превозното средство заедно с всички параметри относно еталонирането, фигуриращи в списъка на глава III, параграф 20, настроени на съответните актуализирани стойности по подразбиране. Когато не е възможно да се въведе никаква определена стойност, се използва серия от въпросителни относно буквените параметри и от нули относно цифровите параметри.
- 240 Преди своето активиране уредите за регистриране на данните за движението трябва да дадат достъп до функцията за еталониране, дори и да не е в режим на еталониране.
- 241 Преди своето активиране уредите за регистриране на данните за движението не трябва нито да записват, нито да съхраняват данните, визирани в точки III.от12.3 до 12.9 и точки III от 12.12 до 12.14.
- 242 По време на монтирането производителите на превозното средство трябва да настроят предварително всички известни параметри.

- 243 Производителите на превозното средство или монтьорите трябва да активират уредите за регистриране на данните за движението, преди превозното средство да напусне помещенията, в които е извършено монтирането.
- 244 Активирането на уредите за регистриране на данните за движението трябва да започне автоматично при първото поставяне на цехова карта в кое да е от картовите устройства.
- 245 Специфичните операции по свързването на датчика за движение с блока, монтиран на превозното средство, при необходимост се извършват автоматично преди или по време на активирането.
- 246 След активирането уредите за регистриране на данните за движението прилага изцяло контрола относно достъпа до функциите и данните.
- 247 Функциите за записване и съхраняване трябва да бъдат напълно оперативни след активирането.
- 248 Монтирането трябва да бъде последвано от еталониране. Първото еталониране трябва да съдържа въвеждане на регистрационния номер на превозното средство и да се направи през следващите 2 седмици след монтирането или получаването на регистрационния номер, ако неговото получаване стане по-късно от монтирането.
- 248a Апаратурата за контрол трябва да бъде така поставена в превозното средство, че водачът да има достъп до необходимите функции от седалката си.

2. Монтажна табелка

- 249 След проверката на монтираните уреди за регистриране на данните за движението, е необходимо да се постави във вътрешността, от страни или на апаратурата монтажна табелка, която да е видима и лесно достъпна. След всяко инспектиране от страна на лицензиран цех или монтьор, на мястото на старата табелка се поставя нова такава.
- 250 Табелката трябва да съдържа следните обозначения:
- име, адрес или търговско наименование на лицензирания монтьор или цех,
 - характеристичен коефициент на превозното средство във вида „ $w = \dots \text{ imp/km}$ “,
 - константа на уредите за регистриране на данните за движението във вида „ $k = \dots \text{ imp/km}$ “,
 - реална окръжност на търкаляне на гумите във вида „ $l = \dots \text{ mm}$ “,
 - размер на гумите,
 - дата, на която характеристичният коефициент на превозното средство е бил определен и е измерена реалната окръжност на търкаляне на гумите,
 - идентификационен номер на превозното средство.

3. Пломбиране

- 251 Следните компоненти трябва да бъдат пломбирани:
- всеки куплунг, който, ако се разкачи, би предизвикал неоткриваеми промени или неоткриваема загуба на данни,
 - монтажната табелка, освен ако тя е прикрепена по такъв начин, че не може да бъде отделена, без да разруши обозначенията, които има на нея.
- 252 Предвидените пломбирания могат да се премахнат:
- в случай на неотложна необходимост,
 - с цел монтиране, регулиране или поправяне на ограничителя на скоростта или на всяко друго устройство, което има отношение към сигурността на пътя, при положение че уредите за регистриране на данните за движението продължават да функционират правилно и сигурно и при положение, че той се пломбира отново от лицензиран монтьор или цех (съгласно раздел VI) веднага след монтирането на ограничителя на скоростта или на всяко друго устройство, което има отношение към сигурността на пътя, или в течение на следващите 7 дена в другите случаи.

- 253 При всяко счупване на тези пломби се съставя писмена декларация, указваща причините за това действие и се връчва на компетентния орган.

VI. КОНТРОЛ, ИНСПЕКТИРАНЕ И ПОПРАВКИ

Предписанията относно обстоятелствата, при които пломбиранията могат да бъдат махнати, както е указано в член 12, параграф 5 на Регламент (ЕИО) № 3821/85, последно изменен от Регламент (ЕО) № 2135/98, са определени в глава V, (3) на настоящото приложение.

1. Одобрение на монтьорите или цеховете

Държавите-членки лицензират, контролират редовно и сертифицират организациите, натоварени със следните задачи:

- монтирания,
- извършване на контрол,
- инспекции,
- поправки.

По смисъла на член 12, параграф 1 от настоящия регламент, цеховите карти се издават единствено на монтьорите и/или цеховете, които са одобрени да извършват активирането и/или еталонирането на апаратурите за контрол, съгласно настоящото приложение и които, освен при надлежно мотивиран случай:

- не могат да получат карта на предприятие, и
- при които останалите професионални дейности не са от вид, който да попречи на общата сигурност на системата така, както тя е уточнена в допълнение 10.

2. Проверка на новите или поправените устройства

- 254 Всяко ново или поправено устройство трябва да бъде проверено дали функционира правилно и дали прави точни извадки и записи, в границите, фиксирани в глава III.2.1 и III.2.2.

3. Инспектиране на монтиранията

- 255 По време на монтирането на превозното средство, всички инсталирани компоненти (включително уредите за регистриране на данните за движението) трябва да отговарят на разпоредбите относно максималния толеранс, фиксирани в глава III.2,1 и III.2.2.

4. Периодични инспекции

- 256 Извършват се периодични инспекции на апаратурите, монтирани на превозните средства, след всяка поправка или след всяка промяна на характеристикния коефициент на превозното средство или на реалната окръжност на търкаляне на гумите, или когато часовникът, показващ координираното универсално време, е неточен с повече от 20 минути, или когато е променен регистрационният номер, или най-малко един път на всеки две години (24 месеца).

- 257 Тези инспекции включват следните проверки:

- правилно функциониране на уредите за регистриране на данните за движението, включително функцията за съхраняване на данни на тахографските карти,
- отговаряне на разпоредбите на глава III.2.1 и III.2.2 относно максималния толеранс при монтиране,
- наличие на знак за типово одобрение на уредите за регистриране на данните за движението,
- наличие на монтажната табелка,
- липса на нарушаване на целостта на пломбиранията на уредите и на другите компоненти от тях,
- размер на гумите и реална окръжност на търкаляне на гумите.

258 Тези инспекции включват еталониране.

5. Измерване на грешките

259 Измерването на грешките при монтиране и при употреба трябва да се извършва при следните условия, които се приемат като стандартни условия за изпитание:

- ненатоварено превозно средство в движение,
- налягане на гумите, отговарящо на препоръките на производителя,
- износване на гумите в границите, разрешени от националното законодателство,
- движение на превозното средство:
 - превозното средство трябва да се движи напред под действие на собствения си двигател, по права линия и върху равна повърхност със скорост от $50 + 5$ км/ч. Измереното разстояние трябва да бъде най-малко 1000 м,
 - при положение че имат еквивалентна точност, други методи, като например използването на съответен изпитателен стенд, могат също така да бъдат използвани за това изпитание.

6. Поправки

260 Цеховете и работилниците трябва да могат да прехвърлят данните от уредите за регистриране на данните за движението, за да ги възстановят на съответното транспортно предприятие.

261 Одобрените цехове и работилници издават на транспортните предприятия сертификат, удостоверяващ, че данните не могат да бъдат прехвърлени, когато повреда в уредите за регистриране на данните за движението не позволява такова прехвърляне на съхранените данни, дори и след поправката ѝ в самия цех. Цеховете запазват копие от всеки издаден сертификат в продължение най-малко на една година.

VII. ИЗДАВАНЕ НА КАРТИТЕ

Процедурите, прилагани от държавите-членки при издаване на картите, трябва да отговарят на следните изисквания:

- 262 Картовият номер при първото издаване на тахографска карта трябва да съдържа индекс за пореден номер (при необходимост), индекс за замяна и индекс за подновяване, фиксиран на „0“.
- 263 Картовите номера на всички тахографски карти, които не са поименни и са издадени от един контролен орган или от един цех или едно транспортно предприятие, трябва да включват 13 идентични цифри, следвани от пореден номер.
- 264 Една тахографска карта, издадена за замяна на друга съществуваща тахографска карта, трябва да има едناкъв номер с номера на картата, която заменя, с изключение на индекса за замяна, който трябва да се увеличи с една единица (в серия от 0 до 9, от А до Z).
- 265 Тахографска карта, издадена за замяна на друга съществуваща тахографска карта, трябва да има еднаква дата на валидност с картата, която заменя.
- 266 Една тахографска карта, издадена за подновяване на друга съществуваща тахографска карта, трябва да има еднакъв номер с номера на картата, която подновява, с изключение на индекса за подновяване, който трябва да се увеличи с една единица (в серия от 0 до 9, от А до Z).
- 267 Замяната на една съществуваща тахографска карта с цел промяна на административните данни трябва да следва правилата, прилагани при подновяване, ако тя се извършва в рамките на една и съща държава-членка, или правилата, прилагани при първо издаване, ако тя се извършва в друга държава-членка.
- 268 При карта на контролор или цехова карта, която не е поименна, графата „Фамилно име на притежателя на картата“ трябва да бъде попълнено с името на цеха или на контролния орган.

VIII. ТИПОВО ОДОБРЕНИЕ НА УРЕДИТЕ ЗА РЕГИСТРИРАНЕ НА ДАННИТЕ ЗА ДВИЖЕНИЕТО И НА ТАХОГРАФСКИТЕ КАРТИ

1. Общи положения

За целите на настоящата глава под „Уреди за регистриране на данните за движението“ се имат предвид уредите за регистриране на данните за движението или техните компоненти. Не се изисква никакво типово одобрение относно кабела(ите), свързващ(и) датчика за движение с блока, монтиран на превозното средство. Хартията, използвана в уредите за регистриране на данните за движението, се приема като компонент на апаратурата.

- 269 Уредите за регистриране на данните за движението трябва да се представят за одобрение заедно с всички свои компоненти, както и с всяко допълнително устройство, което е вградено в тях.
- 270 Типовото одобрение на уреди за регистриране на данните за движението и на тахографски карти включва изпитания, свързани със сигурността, с функционирането и с възможността за взаимна работа. Положителните резултати на всеки от тези тестове се удостоверяват чрез съответен сертификат.
- 271 Органите на държавите-членки, извършващи типовото одобрение, не предоставят сертификат за типово одобрение съгласно член 5 на настоящия регламент при положение, че при тях няма:
- сертификат за сигурност,
 - сертификат за функциониране,
 - сертификат за възможност за взаимна работа,
- относно уредите за регистриране на данните за движението или тахографската карта, предмет на искането на типово одобрение.
- 272 Всяка промяна на софтуера или хардуера, или на материалите, използвани при производството, трябва да бъде заявена предварително на органа, който е предоставил типово одобрение на уредите. Този орган трябва да потвърди на производителя разширяването на типовото одобрение или може да поиска актуализиране или потвърждение на сертификатите относно функционирането, сигурността и/или възможността за взаимна работа.
- 273 Процедурите по актуализиране *in situ* на софтуера на уредите за регистриране на данните за движението трябва да бъдат одобрени от органа, който е предоставил типово одобрение на въпросната апаратура. Ъпгрейдването на софтуера не трябва да променя или да изтрива никаква информация относно дейността на водача, съхранена в уредите за регистриране на данните за движението. Софтуерът може да бъде ъпгрейдван единствено на отговорността на производителя на уредите за регистриране на данните за движението.

2. Сертификат за сигурност

- 274 Сертификатът за сигурност се издава съгласно разпоредбите на допълнение 10 към настоящото приложение.

3. Сертификат за функциониране

- 275 Всеки кандидат за типово одобрение трябва да предостави на органа, извършващ типовото одобрение в съответната държава-членка, всички компоненти и документацията, които този орган смята за необходими.
- 276 От производителя се издава сертификат за функциониране единствено ако апаратурата е получила положителни резултати на всички изпитания за функциониране, уточнени в допълнение 9.
- 277 Органът, извършващ типовото одобрение, издава сертификат за функциониране. Този сертификат съдържа, освен името на неговия притежател и името на модела, един подробен списък на извършените изпитания и на получените резултати.

4. Сертификат за възможност за взаимна работа

- 278 Изпитанията относно възможността за взаимна работа се извършват само от една лаборатория под контрола и отговорността на Европейската комисия.
- 279 Лабораторията записва исканията за провеждане на изпитания, подадени от производителите, по реда на времето на тяхното постъпване.
- 280 Исканията се записват официално, когато лабораторията разполага с:
- всички компоненти и необходимите документи за провеждане на изпитанията относно възможността за взаимна работа,
 - съответния сертификат за сигурност,
 - съответния сертификат за функциониране.
- Датата на вписване на искането се съобщава на производителя.
- 281 Лабораторията не провежда никакво изпитание относно възможността за взаимна работа на уреди за регистриране на данните за движението или на тахографска карта, която не е получила сертификат за сигурност и сертификат за функциониране.
- 282 Всеки производител, поискал провеждането на изпитанията относно възможността за взаимна работа, се ангажира да остави на лабораторията, натоварена с изпитанията, всички компоненти на апаратурата и документацията, необходима за целите на изпитанията.

- 283 Изпитанията относно възможността за взаимна работа се провеждат съгласно допълнение 9, параграф 5 към настоящото приложение на всички типове уреди за регистриране на данните за движението или тахографски карти:
- валидността на типовото одобрение на които не е изтекла,
 - типовото одобрение на които се извършва в момента и за които съществува валиден сертификат за възможност за взаимна работа.
- 284 Сертификатът за възможността за взаимна работа трябва да бъде издаден на производителя от лабораторията единствено след като са получени положителни резултати на всички изпитания относно възможността за взаимна работа.
- 285 При получаване на отрицателни резултати от изпитанията относно възможността за взаимна работа на едно или няколко записващи устройства или тахографска/и карта/и, както е предвидено в изискване 283, сертификатът за възможност за взаимна работа не се издава, докато съответният производител не извърши необходимите промени и устройството или картата не започнат да изпълняват изискванията на всички изпитания относно възможността за взаимна работа. Лабораторията определя характера на проблема с помощта на съответния производител и се опитва да му помогне при търсенето на техническо решение. При положение, че производителят е променил продукта си, той трябва да се увери, като се обърне към компетентните власти, във валидността на сертификата за сигурност и на сертификата за функциониране.
- 286 Сертификатът за възможността за взаимна работа важи 6 месеца. Той изтича в края на този период, ако производителят не е получил съответния сертификат за типово одобрение. Той се предава от производителя на органа, извършващ типовото одобрение в държавата-членка, която е издала сертификата за функциониране.
- 287 Всеки елемент, който би могъл да предизвика аномалия при взаимната работа, не би трябвало да се използва за извличане на печалби, нито за завземане на доминиращо положение на пазара.

5. Сертификат за типово одобрение

- 288 Органът, извършващ типовото одобрение в държавата-членка, може да предоставя сертификата за типово одобрение при положение, че при него са депозирани трите изисквани сертификата.
- 289 Копие от сертификата за типово одобрение трябва да бъде предадено от сертифициращия орган на лабораторията, натоварена с изпитанията относно възможността за взаимна работа, в момента на издаването на този документ на производителя.
- 290 Лабораторията, натоварена с изпитанията относно възможността за взаимна работа, трябва да актуализира на Интернет-сайт с публичен достъп списъка на моделите апаратури за контрол или тахографски карти:
- за които е било регистрирано искане за провеждане на изпитанията относно възможността за взаимна работа,
 - които са получили сертификат за възможност за взаимна работа (дори и ако той е временен),
 - които са получили сертификат за типово одобрение.

6. Извънредна процедура: първи сертификат за възможност за взаимна работа

- 291 За период от 4 месеца, след като една първа двойка от уреди за регистриране на данните за движението/тахографски карти (карта на водач, цехова карта, карта на контролор и на предприятието) е била призната за възможност за взаимна работа, всички издадени сертификати за възможност за взаимна работа (включително и този първи сертификат) имащи отношение към заявките, получени през този период, се считат за временни.
- 292 След изтичане на този период, ако всички въпросни продукти са с призната възможност за взаимна работа, сертификатите им за възможност за взаимна работа стават окончателни.
- 293 Ако по време на този период се появяват аномалии, свързани с възможността за взаимна работа, лабораторията, натоварена с провеждането на изпитанията, определя причината за наблюдаваните проблеми с помощта на всички заинтересовани производители и ги призовава да направят необходимите промени.
- 294 Ако по време на този период проблемите, свързани с възможността за взаимна работа, не се отстранят, лабораторията, натоварена с провеждането на изпитанията, в сътрудничество със заинтересованите производители и с органите, извършващи одобрението, определя причините за тези аномалии и определя промените, които всеки заинтересован производител трябва да извърши. Търсенето на технически решения може да продължи не по-дълго от два месеца, след което Комисията, при липса на общо решение и след консултация с лабораторията, натоварена с извършването на изпитанията относно възможността за взаимна работа, решава на коя/кои апаратура/и и карти ще се издаде окончателен сертификат за възможност за взаимна работа, като уточнява причините за своя избор.
- 295 Всяко искане за извършване на изпитанията относно възможността за взаимна работа, заведено от лабораторията във времето от края на периода от 4 месеца след издаване на първия временен сертификат за възможност за взаимна работа до датата на вземане на решение от Комисията, визирана в изискване 294, се отлага до решаване на първоначалните проблеми, свързани с възможността за взаимна работа. Тези искания след това се обработват по реда на тяхното завеждане.

Допълнение 1

РЕЧНИК НА ДАНИТЕ

СЪДЪРЖАНИЕ

1.	Въведение	56
1.1.	Метод на установяване на определенията на типа данни	56
1.2.	Изходна база	56
2.	Определения на типовете данни	57
2.1.	ActivityChangeInfo	57
2.2.	Address	58
2.3.	BCDString.....	58
2.4.	CalibrationPurpose	58
2.5.	CardActivityDailyRecord	59
2.6.	CardActivityLengthRange	59
2.7.	CardApprovalNumber	59
2.8.	CardCertificate	59
2.9.	CardChipIdentification.....	59
2.10.	CardConsecutiveIndex	60
2.11.	CardControlActivityDataRecord	60
2.12.	CardCurrentUse	60
2.13.	CardDriverActivity	60
2.14.	CardDrivingLicenceInformation	61
2.15.	CardEventData	61
2.16.	CardEventRecord	61
2.17.	CardFaultData	62
2.18.	CardFaultRecord	62
2.19.	CardIccIdentification	62
2.20.	CardIdentification.....	63
2.21.	CardNumber	63
2.22.	CardPlaceDailyWorkPeriod	63
2.23.	CardPrivateKey	64
2.24.	CardPublicKey	64
2.25.	CardRenewalIndex	64
2.26.	CardReplacementIndex	64
2.27.	CardSlotNumber	64
2.28.	CardSlotsStatus.....	64
2.29.	CardStructureVersion	65

2.30.	CardVehicleRecord	65
2.31.	CardVehiclesUsed.....	65
2.32.	Certificate	66
2.33.	CertificateContent	66
2.34.	CertificateHolderAuthorisation	66
2.35.	CertificateRequestID.....	67
2.36.	CertificationAuthorityKID	67
2.37.	CompanyActivityData	67
2.38.	CompanyActivityType.....	68
2.39.	CompanyCardApplicationIdentification.....	68
2.40.	CompanyCardHolderIdentification	68
2.41.	ControlCardApplicationIdentification	69
2.42.	ControlCardControlActivityData	69
2.43.	ControlCardHolderIdentification.....	69
2.44.	ControlType	70
2.45.	CurrentDateTime	70
2.46.	DailyPresenceCounter	70
2.47.	Datef	71
2.48.	Distance	71
2.49.	DriverCardApplicationIdentification	71
2.50.	DriverCardHolderIdentification	71
2.51.	EntryTypeDailyWorkPeriod.....	72
2.52.	EquipmentType	72
2.53.	EuropeanPublicKey	72
2.54.	EventFaultType.....	72
2.55.	EventFaultRecordPurpose	73
2.56.	ExtendedSerialNumber.....	74
2.57.	FullCardNumber	74
2.58.	HighResOdometer	74
2.59.	HighResTripDistance	74
2.60.	HolderName	74
2.61.	K-ConstantOfRecordingEquipment.....	75
2.62.	KeyIdentifier	75
2.63.	L-TyreCircumference	75
2.64.	Language	75
2.65.	LastCardDownload	75
2.66.	ManualInputFlag	75
2.67.	ManufacturerCode	76

2.68.	MemberStateCertificate	76
2.69.	MemberStatePublicKey	77
2.70.	Name	77
2.71.	NationAlpha	77
2.72.	NationNumeric	78
2.73.	NoOfCalibrationRecords	79
2.74.	NoOfCalibrationSinceDownload	79
2.75.	NoOfCardPlaceRecords	79
2.76.	NoOfCardVehicleRecords	79
2.79.	NoOfCompanyActivityRecords	79
2.78.	NoOfControlActivityRecords	80
2.79.	NoOfEventsPerType	80
2.80.	NoOfFaultsPerType	80
2.81.	OdometerValueMidnight	80
2.82.	OdometerShort	80
2.83.	OverspeedNumber	80
2.84.	PlaceRecord	80
2.85.	PreviousVehicleInfo	81
2.86.	PublicKey	81
2.87.	RegionAlpha	81
2.88.	RegionNumeric	81
2.89.	RSAPublicModulus	82
2.90.	RSAPrivateExponent	82
2.91.	RSAPublicExponent	82
2.92.	SensorApprovalNumber	82
2.93.	SensorIdentification	82
2.94.	SensorInstallation	83
2.95.	SensorInstallationSecData	83
2.96.	SensorOSIdentifier	83
2.97.	SensorPaired	83
2.98.	SensorPairingDate	84
2.99.	SensorSerialNumber	84
2.100.	SensorSCIdentifier	84
2.101.	Signature	84
2.102.	SimilarEventsNumber	84
2.103.	SpecificConditionType	84
2.104.	SpecificConditionRecord	84
2.105.	Speed	85

2.106.	SpeedAuthorised	85
2.107.	SpeedAverage	85
2.108.	SpeedMax	85
2.109.	TDesSessionKey	85
2.110.	TimeReal	85
2.111.	TyreSize	85
2.112.	VehicleIdentificationNumber	86
2.113.	VehicleRegistrationIdentification.....	86
2.114.	VehicleRegistrationNumber.....	86
2.115.	VuActivityDailyData	86
2.116.	VuApprovalNumber	86
2.117.	VuCalibrationData	86
2.118.	VuCalibrationRecord	87
2.119.	VuCardIWDData	87
2.120.	VuCardIWRecord	88
2.121.	VuCertificate.....	88
2.122.	VuCompanyLocksData	88
2.123.	VuCompanyLocksRecord	89
2.124.	VuControlActivityData	89
2.125.	VuControlActivityRecord	89
2.126.	VuDataBlockCounter	89
2.127.	VuDetailedSpeedBlock.....	89
2.128.	VuDetailedSpeedData	90
2.129.	VuDownloadablePeriod	90
2.130.	VuDownloadActivityData	90
2.131.	VuEventData.....	90
2.132.	VuEventRecord.....	91
2.133.	VuFaultData	91
2.134.	VuFaultRecord	91
2.135.	VuIdentification	92
2.136.	VuManufacturerAddress	92
2.137.	VuManufacturerName	92
2.138.	VuManufacturingDate	92
2.139.	VuOverSpeedingControlData	93
2.140.	VuOverSpeedingEventData	93
2.141.	VuOverSpeedingEventRecord	93
2.142.	VuPartNumber	93
2.143.	VuPlaceDailyWorkPeriodData.....	94

2.144.	VuPlaceDailyWorkPeriodRecord	94
2.145.	VuPrivateKey	94
2.146.	VuPublicKey	94
2.147.	VuSerialNumber	94
2.148.	VuSoftInstallationDate	94
2.149.	VuSoftwareIdentification	94
2.150.	VuSoftwareVersion	95
2.151.	VuSpecificConditionData	95
2.152.	VuTimeAdjustmentData	95
2.153.	VuTimeAdjustmentRecord	95
2.154.	Характеристичен коефициент W на превозното средство	95
2.155.	WorkshopCardApplicationIdentification	96
2.156.	WorkshopCardCalibrationData	96
2.157.	WorkshopCardCalibrationRecord	96
2.158.	WorkshopCardHolderIdentification	97
2.159.	WorkshopCardPIN	97
3.	Определения на диапазоните от стойности и на размерите	98
3.1.	Определения, отнасящи се до картите на водача	98
3.2.	Определения, отнасящи се до цеховите карти	98
3.3.	Определения, отнасящи се до картите на контрольора	98
3.4.	Определения, отнасящи се до картите на предприятията	98
4.	Набор от символи	98
5.	Кодиране	98

1. ВЪВЕДЕНИЕ

В настоящото допълнение се дава поредица от уточнения относно форматите, типовете и структурата на данните, използвани от уредите за регистриране на данните за движението и тахографските карти.

1.1. Метод на установяване на определенията на типа данни

В настоящото допълнение се използва Нотиране на абстрактен синтаксис № 1 (ASN.1) за определяне на различните типове данни. Тази система позволява дефинирането на прости и структурирани данни, без да се нуждае от използването на специфичен синтаксис за трансфер (правила на кодиране), които да зависят от съответното приложение и среда.

Правилата за наименоване от тип ASN.1 се фиксират съгласно стандарт ISO/CEI 8824-1. От това следва, че:

- в рамките на възможното значението на определен тип данни става имплицитно ясно от името, което е дадено на този тип,
- ако определен тип данни се състои от други типове данни, името на този тип се представя винаги под формата на една-единствена последователност от буквени символи, започваща с главна буква, въпреки че това име може да съдържа неопределен брой главни букви, които напомнят за значението на данните,
- по принцип имената на типа данни са във връзка с името на типовете данни, от които са съставени, с оборудването, в което данните се запамятват, и с функцията, която е асоциирана към въпросните данни.

Ако използването на тип ASN.1, който вече е определен в рамките на друг стандарт, се налага заедно с уредите за регистриране на данните за движението, този тип ASN.1 се дефинира в настоящото допълнение.

С цел да се позволи прилагането на няколко типа правила за кодиране, някои типове ASN.1, упоменати в настоящото допълнение, са в зависимост от идентификатори на диапазона от стойности. Тези идентификатори се определят в параграф 3.

1.2. Изходна база

Следващите съкращения се използват в настоящото допълнение:

ISO 639	Код за представяне на имената на езиците. Първо издание: 1988 г.
EN 726-3	Системи от идентификационни карти — Карти и телекомуникационни терминали с интегрална/и схема/и — Част 3: Изисквания, независещи от приложенията, на които картите трябва да отговарят. Декември 1994 г.
ISO 3779	Пътни превозни средства — Идентификационен номер на превозното средство (NIIdV) — Съдържание и структура. Трето издание: 1983 г.
ISO/IEC 7816-5	Информационна технология — Идентификационни карти — Карти с вградена/и интегрална/и схема/и с контакти — Част 5: Система за номериране и процедура по записване на идентификаторите на приложения. Първо издание: 1994 г. + Изменение 1: 1996 г.
ISO/IEC 8824-1	Информационна технология — Нотиране на абстрактен синтаксис № 1 (ASN.1): Спецификация на базовото нотиране. Второ издание: 1998 г.
ISO/IEC 8825-2	Информационна технология — Правила за кодиране по (ASN.1): Спецификация на правилата за кондензирано кодиране (RCC). Второ издание: 1998 г.
ISO/IEC 8859-1	Информационна технология — Набори от графични символи, кодирани в байтове — Част 1: Латинска азбука № 1. Първо издание: 1998 г.
ISO/IEC 8859-7	Информационна технология — Набори от графични символи, кодирани в байтове — Част 7: Латинска/гръцка азбука. Първо издание: 1987 г.
ISO 16844-3	Пътни превозни средства — Тахографски системи — Интерфейси на датчиците за движение. WD 3-20/05/99.

'aa'В	Дейност (ирелевантно, ако „р“ = 1 и „с“ = 0, освен при забележката по-долу):
'00'В:	ПРЕКЪСВАНЕ/ПОЧИВКА
'01'В:	НА РАЗПОЛОЖЕНИЕ
'10'В:	РАБОТА
'11'В:	КОРМУВАНЕ
'tttttttttt'В	Час на промяната: брой минути, изтекли след 00.00 часа на съответния ден.

Забележка в случай на „Изваждане на картата“:

Когато картата е извадена:

- „s“ се прилага и указва четящото устройство, чиято карта е била извадена,
- „с“ трябва да бъде поставено на 0,
- „р“ трябва да бъде поставено на 1,
- „aa“ трябва да копира текущата дейност, избрана в същия момент.

Нишо не пречи битовете „с“ и „aa“ на думата (записана на карта) да бъдат изтрети вследствие на ръчно въвеждане с цел отразяване на постъпването на съответните данни.

2.2. Address

Адрес.

```
Address ::= SEQUENCE {
    codePage                INTEGER (0..255),
    address                  OCTET STRING (SIZE (35))
}
```

codePage (страница с кодове) специфицира частта от стандарта ISO/CEI 8859, използвана за кодирането на адреса,

address указва адрес, кодирането на който се извършва съгласно съответната страница с кодове от стандарта ISO/CEI 8859.

2.3. BCDString

BCDString се прилага при представяне в двоичен код на данни, съставени от десетични числа (DCB). Този тип данни се използва за представяне на десетично число чрез един полубайт (4 бита). BCDString се основава на прилагането на стандарта ISO/CEI 8824-1 „CharacterStringType“ (тип символен низ).

```
BCDString ::= CHARACTER STRING (WITH COMPONENTS {
    identification (WITH COMPONENTS {
        fixed PRESENT }) })
```

BCDString използва нотирането „hstring“. Лявата шестнадесетична цифра се смята като най-значещият полубайт на първия байт. За да се получи кратно число байтове, е необходимо да се вмъкне съответният брой десни нулеви полубайтове от позицията, която заема най-значещият полубайт на първия байт.

Допустими цифри: 0, 1, ... 9.

2.4. CalibrationPurpose

Код, указващ причината за записване на комплект от параметри за еталониране. Този тип данни е свързан с изисквания 097 и 098.

```
CalibrationPurpose ::= OCTET STRING (SIZE (1))
```

Определяне на стойност:

'00'Н запазена стойност,

'01'Н активиране: записване на параметрите за еталониране, известни в момента на активирането на блока, монтиран на превозното средство,

- '02'H първо инсталиране: първо еталониране на блока след активирането му,
- '03'H инсталиране: първо еталониране на блока, монтиран на разглежданото превозно средство,
- '04'H периодично инспектиране.

2.5. CardActivityDailyRecord

Информации, записани на картата и отнасящи се до дейностите, които водачът е извършвал през определен календарен ден. Този тип данни е свързан с изисквания 199 и 219.

```
CardActivityDailyRecord ::= SEQUENCE {
    activityPreviousRecordLength      INTEGER(0..CardActivityLengthRange),
    activityRecordLength              INTEGER(0..CardActivityLengthRange),
    activityRecordDate                 TimeReal,
    activityDailyPresenceCounter       DailyPresenceCounter,
    activityDayDistance                Distance,
    activityChangeInfo                 SET SIZE(1..1440) OF ActivityChangeInfo
}
```

activityPreviousRecordLength указва общата дължина на предишния ежедневен запис, изразена в байтове. Максималната стойност съответства на дължината на НИЗА ОТ БАЙТОВЕ, съдържащ тези записи (виж CardActivityLengthRange, параграф 3). Когато тези данни съответстват на най-стария ежедневен запис, стойността на activityPreviousRecordLength трябва да бъде нулирана.

activityRecordLength указва общата дължина на този запис, изразена в байтове. Максималната стойност съответства на дължината на НИЗА ОТ БАЙТОВЕ, съдържащ тези записи.

activityRecordDate указва датата на записа.

activityDailyPresenceCounter указва състоянието на брояча на присъствените дни за разглеждания ден и карта.

activityDayDistance указва общото изминато разстояние през разглеждания ден.

activityChangeInfo указва комплекта от данни ActivityChangeInfo, който се отнася до разглежданите водач и ден. Този низ от байтове не може да съдържа повече от 1440 стойности (една промяна на дейност в минута). Този комплект от данни съдържа винаги ActivityChangeInfo, който кодира положението на водача в 00.00 часа.

2.6. CardActivityLengthRange

Брой на байтовете, които една карта на водача или цехова карта може да предназначи за съхраняването на записите относно дейностите на водача.

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

Определяне на стойност: виж параграф 3.

2.7. CardApprovalNumber

Номер на типово одобрение на картата.

```
CardApprovalNumber ::= IA5String(SIZE(8))
```

Определяне на стойност: не е указана.

2.8. CardCertificate

Сертификат, свързан с публичния ключ на определена карта.

```
CardCertificate ::= Certificate
```

2.9. CardChipIdentification

Информации, записани на картата, и отнасящи се до идентифицирането на вградения чип (CI) на тази карта (изискване 191).

```
CardChipIdentification ::= SEQUENCE {
    icSerialNumber                OCTET STRING (SIZE(4)),
    icManufacturingReferences     OCTET STRING (SIZE(4))
}
```


activityPointerOldestDayRecord указва с точност началото на записването в паметта (броя на байтовете, броени от началото на низа) на най-стария ежедневен запис, който съдържа низът activityDailyRecords. Максималната стойност съответства на дължината на низа.

activityPointerNewestRecord указва с точност началото на записването в паметта (броя на байтовете, броени от началото на низа) на най-новия ежедневен запис, който съдържа низът activityDailyRecords. Максималната стойност съответства на дължината на низа.

activityDailyRecords указва мястото, отделено за записването на данните относно дейностите на водача (структура на данни: CardActivityDailyRecord) за всеки календарен ден, през който картата е била използвана.

Определение на стойност: този низ от байтове се попълва периодично от записи от типа на CardActivityDailyRecord. По време на първото използване началото на записването на първото извлечение съвпада с първия байт на низа. Следващите записи се запамятват в края на предишния. Когато низът се запълни, записването продължава, като се извършва отново на първия байт на низа, без да се държи сметка за прекъсванията, които са в състояние да засегнат каквото и да е елемент от информацията. Преди да се въведат нови данни за дейността в низа (като се разшири съществуващият activityDailyRecord или като се вкара нов activityDailyRecord), които заместват най-старите данни за дейността, е необходимо да се актуализира activityPointerOldestDayRecord, за да се получи информация за новото местоположение в паметта, което заема от този момент най-старият пълен всекидневен запис, и да се нулира activityPreviousRecordLength на този (нов) най-стар пълен всекидневен запис.

2.14. CardDrivingLicenceInformation

Информации, записани на карта на водача и отнасящи се до свидетелството за управление на притежателя на картата (изискване 196).

```
CardDrivingLicenceInformation ::= SEQUENCE {
    drivingLicenceIssuingAuthority      Name,
    drivingLicenceIssuingNation         NationNumeric,
    drivingLicenceNumber                IA5String(SIZE(16))
}
```

drivingLicenceIssuingAuthority указва компетентния орган, извършил издаването на свидетелството за управление.

drivingLicenceIssuingNation указва националността на компетентния орган, извършил издаването на свидетелството за управление.

drivingLicenceNumber указва номера на свидетелството за управление.

2.15. CardEventData

Информации, записани на карта на водача или на цехова карта и отнасящи се до събитията, свързани с притежателя на картата (изисквания 204 и 223).

```
CardEventData ::= SEQUENCE SIZE(6) OF {
    cardEventRecords                    SET SIZE(NoOfEventsPerType) OF
                                        CardEventRecord
}
```

CardEventData се състои от последователност от cardEventRecords (с изключение на записите относно евентуалните опити за нарушаване на сигурността, които са групирани в последния блок от данни на последователността), чието структуриране съответства на структурирането на EventFaultType, подредени по възходящ ред.

cardEventRecords се състои в комплект от записи на събития, съответстващ на определен тип събитие (или на тази категория от събития, в които се нареждат опитите за нарушаване на сигурността).

2.16. CardEventRecord

Информации, записани на карта на водача или на цехова карта и отнасящи се до определено събитие, свързано с притежателя на картата (изисквания 205 и 223).

```
CardEventRecord ::= SEQUENCE {
    eventType                           EventFaultType,
    eventBeginTime                       TimeReal,
    eventEndTime                         TimeReal,
    eventVehicleRegistration             VehicleRegistrationIdentification
}
```

eventType указва типа на събитието.

eventBeginTime указва датата и часа на началото на определено събитие.

eventEndTime указва датата и часа на края на определено събитие.

eventVehicleRegistration указва регистрационния номер, както и държавата-членка, извършила регистрацията на превозното средство, в което се е случило разглежданото събитие.

2.17. CardFaultData

Информации, записани на карта на водача или на цехова карта и отнасящи се до аномалиите, свързани с притежателя на картата (изисквания 207 и 223).

```
CardFaultData ::= SEQUENCE SIZE (2) OF {
    cardFaultRecords                               SET SIZE (NoOfFaultsPerType) OF
                                                    CardFaultRecord
}
```

CardFaultData представлява последователност, съдържаща комплект от записи на аномалиите, които засягат уредите за регистриране на данните за движението, последван от комплект от записи на аномалиите, които засягат използваната/ите карта/и.

cardFaultRecords представлява комплект от записи на аномалиите, които се подреждат в определена категория (уреди за регистриране на данните за движението или карта).

2.18. CardFaultRecord

Информации, записани на карта на водача или на цехова карта и отнасящи се до определена аномалия, свързана с притежателя на картата (изисквания 208 и 223).

```
CardFaultRecord ::= SEQUENCE {
    faultType                                     EventFaultType,
    faultBeginTime                               TimeReal,
    faultEndTime                                 TimeReal,
    faultVehicleRegistration                     VehicleRegistrationIdentification
}
```

faultType указва типа на аномалията.

faultBeginTime указва датата и часа на началото на определена аномалия.

faultEndTime указва датата и часа на края на определена аномалия.

faultVehicleRegistration указва регистрационния номер, както и държавата-членка, извършила регистрацията на превозното средство, в което се е случила разглежданата аномалия.

2.19. CardIccIdentification

Информации, записани на определена карта и отнасящи се до идентифицирането на тази карта с вграден чип (CI) (изискване 192).

```
CardIccIdentification ::= SEQUENCE {
    clockStop                                     OCTET STRING (SIZE(1)),
    cardExtendedSerialNumber                     ExtendedSerialNumber,
    cardApprovalNumber                           CardApprovalNumber
    cardPersonaliserID                           OCTET STRING (SIZE(1)),
    embedderIcAssemblerId                       OCTET STRING (SIZE(5)),
    icIdentifier                                 OCTET STRING (SIZE(2))
}
```

clockStop указва режима clockStop, определен в стандарт EN 726-3.

cardExtendedSerialNumber указва серийния номер на картата с вграден чип, както и нейния референтен производствен номер, определен от стандарт EN 726-3 така, както те са указани от типа данни ExtendedSerialNumber.

cardApprovalNumber указва номера на типовото одобрение на картата.

cardPersonaliserID указва индивидуалния ID на картата, определен в стандарт EN 726-3.

embedderIdAssemblerId указва идентификатора на интегратора/асемблатора на вградения чип, определен в стандарт EN 726-3.

icIdentifier указва идентификатора на чипа, вграден на картата, и на неговия производител, определен в стандарт EN 726-3.

2.20. CardIdentification

Информации, записани на определена карта и отнасящи се до нейното идентифициране (изисквания 194, 215, 231 и 235).

```
CardIdentification ::= SEQUENCE {
    cardIssuingMemberState      NationNumeric,
    cardNumber                  CardNumber,
    cardIssuingAuthorityName    Name,
    cardIssueDate               TimeReal,
    cardValidityBegin           TimeReal,
    cardExpiryDate              TimeReal
}
```

cardIssuingMemberState указва кода на държавата-членка, която е издала картата.

cardNumber указва картовия номер на разглежданата карта.

cardIssuingAuthorityName указва името на компетентния орган, извършил издаването на разглежданата карта.

cardIssueDate указва датата на издаването на картата на сегашния ѝ титуляр.

cardValidityBegin указва датата на първото влизане в сила на картата.

cardExpiryDate указва датата на край на валидността на картата.

2.21. CardNumber

Номер на карта съгласно определение ж).

```
CardNumber ::= CHOICE {
    SEQUENCE {
        driverIdentification      IA5String(SIZE(14)),
        cardReplacementIndex      CardReplacementIndex,
        cardRenewalIndex          CardRenewalIndex
    }
    SEQUENCE {
        ownerIdentification       IA5String(SIZE(13)),
        cardConsecutiveIndex      CardConsecutiveIndex,
        cardReplacementIndex      CardReplacementIndex,
        cardRenewalIndex          CardRenewalIndex
    }
}
```

driverIdentification указва индивидуалната идентификация на водач, водещ се на отчет в определена държава-членка.

ownerIdentification указва индивидуалната идентификация на предприятие, цех или контролен орган, установени в определена държава-членка.

cardConsecutiveIndex указва индекса за пореден номер на разглежданата карта.

cardReplacementIndex указва индекса за замяна на картата.

cardRenewalIndex указва индекса за подновяване на картата.

Първата последователност от селекцията позволява да се кодира номерът на картата на водача, втората последователност позволява да се кодират номерата на цеховата карта, на картата на контролор и на картата на предприятие.

2.22. CardPlaceDailyWorkPeriod

Информации, записани на карта на водача или на цехова карта и отнасящи се до местоположението в началото и/или в края на дневните периоди на работа (изисквания 202 и 221).

```
CardPlaceDailyWorkPeriod ::= SEQUENCE {
    placePointerNewestRecord          INTEGER(0..NoOfCardPlaceRecords-1),
    placeRecords                      SET SIZE(NoOfCardPlaceRecords) OF PlaceRe-
                                     cord
}
```

placePointerNewestRecord указва индекса на последния запис на местоположението, актуализиран от системата.

Определяне на стойност: число, съответстващо на номератора на записите на местоположението, започващо със серия от „0“ за първия случай от запис на местоположение в разглежданата структура.

placeRecords указва комплекта от записи, съдържащи данните относно въведените местоположения.

2.23. CardPrivateKey

Частен ключ на определена карта.

```
CardPrivateKey ::= RSAKeyPrivateExponent
```

2.24. CardPublicKey

Публичен ключ на определена карта.

```
CardPublicKey ::= PublicKey
```

2.25. CardRenewalIndex

Индекс за подновяване на определена карта [определение и]).

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

Определяне на стойност: (виж раздел VII на настоящото приложение).

'0' Първо издаване.

Възходящ ред: '0, ..., 9, A, ..., Z'.

2.26. CardReplacementIndex

Индекс за подмяна на определена карта [определение й]).

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

Определяне на стойност: (виж раздел VII на настоящото приложение).

'0' Оригинална карта.

Възходящ ред: '0, ..., 9, A, ..., Z'.

2.27. CardSlotNumber

Код, позволяващ да се прави разлика между двете четящи устройства за карти на един блок, монтиран на превозното средство.

```
CardSlotNumber ::= INTEGER {
    driverSlot          (0),
    co-driverSlot      (1)
}
```

Определяне на стойност: липса на допълнителна информация.

2.28. CardSlotsStatus

Код, указващ типа на картите, вкарани в двете четящи устройства на блока, монтиран на превозното средство.

```
CardSlotsStatus ::= OCTET STRING (SIZE(1))
```

Определяне на стойност — **Поредов байт**: 'ccccddd'В:

'cccc'В Идентифициране на типа на картата, поставена в четящото устройство, предназначено за помощник-водача,
'ddd'В Идентифициране на типа на картата, поставена в четящото устройство, предназначено за водача,

с помощта на следните кодове за идентификация:

'0000'В никаква карта не е поставена в четящото устройство,
'0001'В в четящото устройство е поставена карта на водача,
'0010'В в четящото устройство е поставена цехова карта,
'0011'В в четящото устройство е поставена карта на контролор,
'0100'В в четящото устройство е поставена карта на предприятие.

2.29. CardStructureVersion

Код, указващ версията на структурата, приложена в определена тахографска карта.

CardStructureVersion ::= OCTET STRING (SIZE (2))

Определяне на стойност: „aabb“Н:

'aa'Н Индекс на промените, извършени в структурата,
'bb'Н Индекс на промените, отнасящи се до използването на елементи на информация, определени за съответната структурата от значещия (най-левия) байт.

2.30. CardVehicleRecord

Информации, записани на карта на водача или на цехова карта и отнасящи се до даден период на използване на превозно средство през определен календарен ден (изисквания 197 и 217).

```
CardVehicleRecord ::= SEQUENCE {
    vehicleOdometerBegin          OdometerShort,
    vehicleOdometerEnd           OdometerShort,
    vehicleFirstUse              TimeReal,
    vehicleLastUse               TimeReal,
    vehicleRegistration          VehicleRegistrationIdentification,
    vuDataBlockCounter           VuDataBlockCounter
}
```

vehicleOdometerBegin указва стойността, отчетена от брояча на километрите на дадено превозно средство в началото на разглеждания период на използване.

vehicleOdometerEnd указва стойността, отчетена от брояча на километрите дадено превозно средство в края на разглеждания период на използване.

vehicleFirstUse указва датата и часа на началото на периода на използване на превозното средство.

vehicleLastUse указва датата и часа на края на периода на използване на превозното средство.

vehicleRegistration указва регистрационния номер, както и държавата-членка, извършила регистрацията на разглежданото превозно средство.

vuDataBlockCounter указва стойността, отчетена от брояча на блоковете с данни на блока, монтиран на превозното средство, по време на последното извличане на периода на използване на превозното средство.

2.31. CardVehiclesUsed

Информации, записани на карта на водача или на цехова карта и отнасящи се до превозните средства, използвани от притежателя на картата (изисквания 197 и 217).

```
CardVehiclesUsed ::= SEQUENCE {
    vehiclePointerNewestRecord    INTEGER(0..NoOfCardVehicleRecords-1),
    cardVehicleRecords           SET SIZE (NoOfCardVehicleRecords) OF
                                CardVehicleRecord
}
```

vehiclePointerNewestRecord указва индекса на последния запис на данните относно превозното средство, актуализиран от системата.

Определяне на стойност: Число, съответстващо на номератора на записите на превозното средство, започващо със серия от „0“ за първия случай от запис на превозното средство в разглежданата структура.

cardVehicleRecords указва комплекта от записи, съдържащи данните относно използваните превозни средства.

2.32. Certificate

Сертификат на публичен ключ, издаден от удостоверяващ орган.

```
Certificate ::= OCTET STRING (SIZE(194))
```

Определяне на стойност: Цифров подпис с частично извличане на съдържанието на сертификата по смисъла на Допълнение 11 „Общи механизми за сигурност“: подпис (128 байта) || остатък от публичния ключ (58 байта) || данни за удостоверяващия орган (8 байта).

2.33. CertificateContent

Съдържанието (което е достъпно) на сертификата на публичен ключ по смисъла на допълнение 11 „Общи механизми за сигурност“:

```
CertificateContent ::= SEQUENCE {
    certificateProfileIdentifier      INTEGER(0..255),
    certificationAuthorityReference  KeyIdentifier,
    certificateHolderAuthorisation   CertificateHolderAuthorisation,
    certificateEndOfValidity         TimeReal,
    certificateHolderReference       KeyIdentifier,
    publicKey                        PublicKey
}
```

certificateProfileIdentifier указва версията на съответния сертификат.

Определяне на стойност: „01h“ за тази версия.

certificationAuthorityReference идентифицира удостоверяващия орган, който е издал разглеждания сертификат. Тези данни се позовават също така на публичния ключ на този сертифициращ орган.

certificateHolderAuthorisation идентифицира правата на титуляра на сертификата.

certificateEndOfValidity указва датата на изтичане на административната валидност на сертификата.

certificateHolderReference идентифицира титуляра на сертификата. Тези данни се позовават също така на неговия публичен ключ.

publicKey указва публичния ключ, одобрен от този сертификат.

2.34. CertificateHolderAuthorisation

Идентифициране на правата на определен титуляр на сертификат.

```
CertificateHolderAuthorisation ::= SEQUENCE {
    tachographApplicationID        OCTET STRING(SIZE(6))
    equipmentType                   EquipmentType
}
```

tachographApplicationID указва идентификатора на тахографското приложение.

Определяне на стойност: „FFh“ „54h“ „41h“ „43h“ „48h“ „4Fh“. Този ID на приложението е ексклузивен неodobрен идентификатор на приложение, отговарящ на стандарт ISO/CEI 7816-5.

equipmentType идентифицира типа на оборудването, визиран от сертификата.

Определяне на стойност: съгласно типа данни EquipmentType. 0, ако сертификатът е издаден от някоя от държавите-членки.

2.35. CertificateRequestID

Индивидуално идентифициране на искане за издаване на сертификат. То може също така да изпълнява ролята на идентификатор на публичния ключ на блока, монтиран на превозното средство, в случай че серийният номер на блока, за който ключът е предназначен, е неизвестен по време на изработването на сертификата.

```
CertificateRequestID ::= SEQUENCE {
    requestSerialNumber          INTEGER(0..232-1)
    requestMonthYear             BCDString(SIZE(2))
    crIdentifier                 OCTET STRING(SIZE(1))
    manufacturerCode            ManufacturerCode
}
```

requestSerialNumber указва серийния номер на искането за издаване на сертификат, притежаван от производителя, както и месеца по-долу.

requestMonthYear идентифицира месеца и годината на искането за издаване на сертификат.

Определяне на стойност: Кодирани DCB на месеца (две цифри) и на годината (двете последни цифри).

crIdentifier е идентификатор, позволяващ да се прави разлика между искане за издаване на сертификат и разширен серийен номер.

Определяне на стойност: „FFh“.

Код на производителя: съответства на цифровия код на производителя, който е подал искането за издаване на сертификат.

2.36. CertificationAuthorityKID

Идентификатор на публичния ключ на определен сертифициращ орган (определена държава-членка или европейски сертифициращ орган).

```
CertificationAuthorityKID ::= SEQUENCE {
    nationNumeric                NationNumeric
    nationAlpha                  NationAlpha
    keySerialNumber              INTEGER(0..255)
    additionalInfo               OCTET STRING(SIZE(2))
    caIdentifier                 OCTET STRING(SIZE(1))
}
```

nationNumeric указва националния цифров код на удостоверяващия орган.

nationAlpha указва националния цифрово-буквен код на удостоверяващия орган.

keySerialNumber е серийен номер, позволяващ да се прави разлика между различните ключове на удостоверяващия орган, ако някои ключове са предмет на промени.

additionalInfo е поле от два байта, позволяващо въвеждането на допълнителни кодове (принадлежащи на удостоверяващия орган).

caIdentifier е идентификатор, позволяващ да се прави разлика между идентификатора на ключ, свързан с определен удостоверяващ орган, и други идентификатори на ключове.

Определяне на стойност: „01h“.

2.37. CompanyActivityData

Информации, записани на карта на предприятие и отнасящи се до дейностите, провеждани с тази карта (изискване 237).

```
CompanyActivityData ::= SEQUENCE {
    companyPointerNewestRecord    INTEGER(0..NoOfCompanyActivityRecords-1),
    companyActivityRecords        SET SIZE(NoOfCompanyActivityRecords) OF
        companyActivityRecord     SEQUENCE {
            companyActivityType    CompanyActivityType,
            companyActivityTime     TimeReal,
            cardNumberInformation   FullCardNumber,
        }
}
```

```

        vehicleRegistrationInformation      VehicleRegistrationIdentification,
        downloadPeriodBegin                TimeReal,
        downloadPeriodEnd                   TimeReal
    }
}

```

companyPointerNewestRecord указва индекса на последния запис на дейността на предприятието, актуализиран от системата.

Определяне на стойност: число, съответстващо на номератора на записа на дейността на предприятието, започващо със серия от „0“ за първия случай от запис на дейността на предприятието в разглежданата структура.

companyActivityRecords указва комплекта от данни, представляващи съвкупността от записите на дейността на предприятието.

companyActivityRecord указва последователността от информации, свързани с определена дейност на предприятието.

companyActivityType указва типа на дейността, провеждана от предприятието.

companyActivityTime указва датата и часа на дейността, провеждана от предприятието.

cardNumberInformation указва номера на картата и, при необходимост, държавата-членка, в която е издадена прехвърлената карта.

vehicleRegistrationInformation указва прехвърлената, блокирана или отблокирана информация за регистрационния номер и държавата-членка, извършила регистрацията на превозното средство.

downloadPeriodBegin и **downloadPeriodEnd** указват при необходимост периода, данните за който са били прехвърлени от блока, монтиран на превозното средство.

2.38. CompanyActivityType

Код, указващ дейност, провеждана от определено предприятие, прибягващо до използването на своята карта на предприятието.

```

CompanyActivityType ::= INTEGER {
    card downloading                (1),
    VU downloading                  (2),
    VU lock-in                      (3),
    VU lock-out                     (4)
}

```

2.39. CompanyCardApplicationIdentification

Информации, записани на карта на предприятие и отнасящи се до идентифицирането на приложението на картата (изискване 190).

```

CompanyCardApplicationIdentification ::= SEQUENCE {
    typeOfTachographCardId          EquipmentType,
    cardStructureVersion             CardStructureVersion,
    noOfCompanyActivityRecords       NoOfCompanyActivityRecords
}

```

typeOfTachographCardId указва типа на картата, която се използва.

cardStructureVersion указва версията на структурата, приложена в картата.

noOfCompanyActivityRecords указва броя на записите на дейността на предприятието, които картата може да съхрани.

2.40. CompanyCardHolderIdentification

Информации, записани на карта на предприятие и отнасящи се до идентифицирането на притежателя на картата (изискване 236).

```

CompanyCardHolderIdentification ::= SEQUENCE {
    companyName                     Name,
    companyAddress                   Address,
    cardHolderPreferredLanguage     Language
}

```

companyName указва името на предприятието на титуляра.

companyAddress указва адреса на предприятието на титуляра.

cardHolderPreferredLanguage указва предпочитания работен език на титуляра.

2.41. ControlCardApplicationIdentification

Информации, записани на карта на контролор и отнасящи се до идентифицирането на приложението на картата (изискване 190).

```
ControlCardApplicationIdentification ::= SEQUENCE {
    typeOfTachographCardId          EquipmentType,
    cardStructureVersion             CardStructureVersion,
    noOfControlActivityRecords       NoOfControlActivityRecords
}
```

typeOfTachographCardId указва типа на картата, която се използва.

cardStructureVersion указва версията на структурата, приложена в картата.

noOfControlActivityRecords указва броя на записите на дейността на предприятието, които картата може да съхрани.

2.42. ControlCardControlActivityData

Информации, записани на карта на предприятие и отнасящи се до дейностите по извършване на контрол, осъществени с помощта на тази карта (изискване 233).

```
ControlCardControlActivityData ::= SEQUENCE {
    controlPointerNewestRecord        INTEGER(0..NoOfControlActivityRecords-1),
    controlActivityRecords            SET SIZE (NoOfControlActivityRecords) OF
        controlActivityRecord        SEQUENCE {
            controlType                ControlType,
            controlTime                 TimeReal,
            controlledCardNumber        FullCardNumber,
            controlledVehicleRegistration VehicleRegistrationIdentification,
            controlDownloadPeriodBegin  TimeReal,
            controlDownloadPeriodEnd    TimeReal
        }
}
```

controlPointerNewestRecord указва индекса на последния запис на дейността по извършване на контрол, актуализиран от системата.

Определяне на стойност: число, съответстващо на номератора на запис на дейността по извършване на контрол, започващо със серия от „0“ за първия случай от запис на дейността по извършване на контрол в разглежданата структура.

controlActivityRecords указва комплекта от данни, представляващи съвкупността от записите на дейността по извършване на контрол.

controlActivityRecord указва последователността от информации, свързани с определена дейност по извършване на контрол.

controlType указва типа на извършения контрол.

controlTime указва датата и часа на извършения контрол.

controlledCardNumber указва номера на картата, както и държавата-членка, която е издала контролираната карта.

controlledVehicleRegistration указва регистрационния номер, както и държавата-членка, извършила регистрацията на превозното средство, подложено на контрол.

controlDownloadPeriodBegin и **controlDownloadPeriodEnd** указват при необходимост периода, данните за който са били прехвърлени.

2.43. ControlCardHolderIdentification

Информации, записани на карта на контролор и отнасящи се до идентифицирането на притежателя на картата (изискване 232).

```
ControlCardHolderIdentification ::= SEQUENCE {
    controlBodyName           Name,
    controlBodyAddress        Address,
    cardHolderName            HolderName,
    cardHolderPreferredLanguage Language
}
```

controlBodyName указва името на контролния орган, от който зависи притежателят на картата.

controlBodyAddress указва адреса на контролния орган, от който зависи притежателят на картата.

cardHolderName указва фамилията и името(името и презимето) на притежателя на картата на контролор.

cardHolderPreferredLanguage указва предпочитания работен език на притежателя на картата.

2.44. ControlType

Код, указващ дейностите, провеждани по време на контрол. Този тип данни е свързан с изисквания 102, 210 и 225.

```
ControlType ::= OCTET STRING (SIZE(1))
```

Определяне на стойност – Поредов байт: „сvрдxxxx“В (8 бита)

'с'В	прехвърляне на данните от картата:
	'0'В: няма прехвърляне на данните от картата по време на тази дейност по извършване на контрол,
	'1'В: прехвърляне на данните от картата по време на тази дейност по извършване на контрол
'v'В	прехвърляне на данните от блока, монтиран на превозното средство:
	'0'В: няма прехвърляне на данните от блока по време на тази дейност по извършване на контрол,
	'1'В: прехвърляне на данните от блока по време на тази дейност по извършване на контрол
'р'В	разпечатване:
	'0'В: няма разпечатване по време на тази дейност по извършване на контрол,
	'1'В: извършване на разпечатване по време на тази дейност по извършване на контрол
'д'В	изобразяване на данните:
	'0'В: няма изобразяване на данните по време на тази дейност по извършване на контрол,
	'1'В: изобразяване на данните по време на тази дейност по извършване на контрол
'хххх'В	Не се използва.

2.45. CurrentDateTime

Дата и час на уредите за регистриране на данните за движението.

```
CurrentDateTime ::= TimeReal
```

Определяне на стойност: липса на допълнителна информация.

2.46. DailyPresenceCounter

Брояч, записан на карта на водача или на цехова карта, стойността на който се увеличава с една единица за всеки календарен ден на вкарване на тази карта в четящото устройство на определен блок, монтиран на превозното средство. Този тип данни е свързан с изисквания 199 и 219.

```
DailyPresenceCounter ::= BCDString(SIZE(2))
```

Определяне на стойност: последователно номериране, максималната стойност на което е равна на 9999, като броячът започва от 0. По време на първото влизане в сила на определена карта, съответният брояч показва нула.

2.47. Datef

Дата, изразена в цифров формат, който може да се разпечата веднага.

```
Datef ::= SEQUENCE {
    year      BCDString(SIZE(2)),
    month     BCDString(SIZE(1)),
    day       BCDString(SIZE(1))
}
```

YYYY година

mm месец

dd ден

'00000000'H указва експлицитно липсата на дата.

2.48. Distance

Изминатото разстояние (резултат от изчислението на разликата между две стойности, указани от брояча на километрите на разглежданото превозно средство).

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

Определяне на стойност: Двоична без знак. Стойност, изразена в километри и намираща се в експлоатационен диапазон от 0 до 9999 км.

2.49. DriverCardApplicationIdentification

Информации, записани на карта на водач и отнасящи се до идентифицирането на приложението на картата (изискване 190).

```
DriverCardApplicationIdentification ::= SEQUENCE {
    typeOfTachographCardId                    EquipmentType,
    cardStructureVersion                      CardStructureVersion,
    noOfEventsPerType                         NoOfEventsPerType,
    noOfFaultsPerType                         NoOfFaultsPerType,
    activityStructureLength                    CardActivityLengthRange,
    noOfCardVehicleRecords                   NoOfCardVehicleRecords,
    noOfCardPlaceRecords                     NoOfCardPlaceRecords
}
```

typeOfTachographCardId указва типа на картата, която се използва.

cardStructureVersion указва версията на структурата, приложена в картата.

noOfEventsPerType указва броя на събитията от всеки тип, които картата може да съхрани.

noOfFaultsPerType указва броя на аномалиите от всеки тип, които картата може да съхрани.

activityStructureLength указва броя на байтовете, които могат да се използват за съхраняване на записите на дейността.

noOfCardVehicleRecords указва броя на записите на превозното средство, които картата може да съхрани.

noOfCardPlaceRecords указва броя на местоположенията, които картата може да съхрани.

2.50. DriverCardHolderIdentification

Информации, записани на карта на водач и отнасящи се до идентифицирането на притежателя на картата (изискване 195).

```
DriverCardHolderIdentification ::= SEQUENCE {
    cardHolderName                            HolderName,
    cardHolderBirthDate                      Datef,
    cardHolderPreferredLanguage             Language
}
```

cardHolderName указва фамилията и името(името и презимето) на притежателя на картата на водача.

cardHolderBirthDate указва датата на раждане на притежателя на картата на водача.

cardHolderPreferredLanguage указва предпочитания работен език на притежателя на картата.

2.51. EntryTypeDailyWorkPeriod

Код, позволяващ да се прави разлика между местоположението в началото и в края на един дневен период на работа и условията на въвеждане на тези данни.

EntryTypeDailyWorkPeriod ::= INTEGER

Begin,	related time = card insertion time or time of entry	(0),
End,	related time = card withdrawal time or time of entry	(1),
Begin,	related time manually entered (start time)	(2),
End,	related time manually entered (end of work period)	(3),
Begin,	related time assumed by VU	(4),
End,	related time assumed by VU	(5)

}

Определяне на стойност: съгласно стандарт ISO/CEI 8824-1.

2.52. EquipmentType

Код, позволяващ да се прави разлика между различните типове оборудване, използвани за тахографското приложение.

EquipmentType ::= INTEGER(0..255)

-- Reserved	(0),
-- Driver Card	(1),
-- Workshop Card	(2),
-- Control Card	(3),
-- Company Card	(4),
-- Manufacturing Card	(5),
-- Vehicle Unit	(6),
-- Motion Sensor	(7),
-- RFU	(8..255)

Определяне на стойност: Съгласно стандарт ISO/CEI 8824-1.

Стойността 0 е запазена за указване на определена държава-членка или на Европа в полето СНА на сертификатите.

2.53. EuropeanPublicKey

Европейски публичен ключ.

EuropeanPublicKey ::= PublicKey

2.54. EventFaultType

Код, характеризиращ определено събитие или аномалия.

EventFaultType ::= OCTET STRING (SIZE(1))

Определяне на стойност:

'0x'H	Събития от общ характер,
'00'H	Липса на допълнителна информация,
'01'H	Поставяне на невалидна карта,
'02'H	Конфликт, предизвикан от картата,
'03'H	Припокриване на времеви период,
'04'H	Кормуване без съответната карта,
'05'H	Поставяне на карта по време на кормуване,
'06'H	Неправилно приключена последна сесия,
'07'H	Превъзаване на допустимата скорост,

'08'H	Прекъсване на електрическото захранване,
'09'H	Грешка в данните относно движението,
'0A'H .. '0F'H	RFU,
'1x'H	Опит за нарушаване на сигурността, свързан с блока, монтиран на превозното средство,
'10'H	Липса на допълнителна информация,
'11'H	Липса на удостоверяване на датчика за движение,
'12'H	Липса на удостоверяване на тахографска карта,
'13'H	Замяна без разрешение на датчика за движение,
'14'H	Липса на цялостност относно въвеждането на данни на картата,
'15'H	Липса на цялостност относно запамените данни за ползвателя,
'16'H	Грешка при трансфера на вътрешни данни,
'17'H	Неправомерно отваряне на корпуса,
'18'H	Саботаж на хардуера,
'19'H .. '1F'H	RFU,
'2x'H	Опит за нарушаване на сигурността, свързан с датчика за движение,
'20'H	Липса на допълнителна информация,
'21'H	Неуспешно удостоверяване,
'22'H	Липса на цялостност относно запамените данни,
'23'H	Грешка при трансфера на вътрешни данни,
'24'H	Неправомерно отваряне на корпуса,
'25'H	Саботаж на хардуера,
'26'H .. '2F'H	RFU,
'3x'H	Аномалии, засягащи уредите за регистриране на данните за движението,
'30'H	Липса на допълнителна информация,
'31'H	Вътрешна аномалия, засягаща блока, монтиран на превозното средство,
'32'H	Аномалия, засягаща принтера,
'33'H	Аномалия, засягаща изобразяването на данни,
'34'H	Аномалия, засягаща прехвърлянето на данни,
'35'H	Аномалия, засягаща датчика за движение,
'36'H .. '3F'H	RFU,
'4x'H	Аномалия, засягаща дадена карта,
'40'H	Липса на допълнителна информация,
'41'H .. '4F'H	RFU,
'50'H .. '7F'H	RFU,
'80'H .. 'FF'H	Принадлежи на производителя.

2.55. EventFaultRecordPurpose

Код, указващ причината за записване на определено събитие или аномалия.

EventFaultRecordPurpose ::= OCTET STRING (SIZE (1))

Определяне на стойност:

'00'H	едно от 10-те (последни) най-събития или аномалии,
'01'H	най-дългото събитие, настъпило по време на всеки от 10-те последни дена, в които са отбелязани събития,
'02'H	едно от 5-те най-дълги събития, записани по време на 365-те последни дена,
'03'H	последното събитие, настъпило по време на всеки от 10-те последни дена, в които са отбелязани събития,
'04'H	най-сериозното събитие, записани по време на всеки от 10-те последни дена, в които са отбелязани събития,
'05'H	едно от 5-те най-сериозни събития, записани по време на 365-те последни дена,
'06'H	първото събитие или аномалия, настъпило след последното еталониране,
'07'H	текущо събитие или аномалия,
'08'H до '7F'H	RFU
'80'H до 'FF'H	зависи от производителя.

2.56. ExtendedSerialNumber

Индивидуално идентифициране на определено оборудване. Този номер може също така да изпълнява ролята на идентификатор на публичния ключ на оборудването.

```
ExtendedSerialNumber ::= SEQUENCE {
    serialNumber          INTEGER(0..232-1)
    monthYear            BCDSstring(SIZE(2))
    type OCTET           STRING(SIZE(1))
    manufacturerCode     ManufacturerCode
}
```

serialNumber указва серийния номер на оборудването, даден му от производителя, както и типа на оборудването и месеца по-долу.

monthYear идентифицира месеца и годината на производството (или на даването на серийен номер).

Определяне на стойност: кодиране BCD на месеца (две цифри) и на годината (двете последни цифри).

type е идентификатор на типа използвано оборудване.

Определяне на стойност: зависи от производителя, като стойността „FFh“ е резервирана.

Код на производителя: съответства на цифровия код на производителя на разглежданото оборудване.

2.57. FullCardNumber

Код, позволяващ сигурното идентифициране на тахографска карта.

```
FullCardNumber ::= SEQUENCE {
    cardType              EquipmentType,
    cardIssuingMemberState NationNumeric,
    cardNumber            CardNumber
}
```

cardType указва типа на тахографската карта.

cardIssuingMemberState указва кода на държавата-членка, която е издала разглежданата карта.

cardNumber указва номера на картата.

2.58. HighResOdometer

Стойност, отчитана от брояча на километрите на превозното средство: общо разстояние, изминато от превозното средство по време на експлоатацията му.

```
HighResOdometer ::= INTEGER(0..232-1)
```

Определяне на стойност: Двоична без знак. Стойност, изразена в 1/200 от км и намираща се в експлоатационен диапазон от 0 до 21 055 406 км.

2.59. HighResTripDistance

Разстояние, изминато по време на цяло пътуване или част от него.

```
HighResTripDistance ::= INTEGER(0..232-1)
```

Определяне на стойност: Двоична без знак. Стойност, изразена в 1/200 от км и намираща се в експлоатационен диапазон от 0 до 21 055 406 км.

2.60. HolderName

Фамилия и име(име и презиме) на притежател на карта.

```
HolderName ::= SEQUENCE {
    holderSurname          Name,
    holderFirstNames      Name
}
```


holderSurname указва фамилното име на титуляра. То не се придружава от никаква титла.

Определяне на стойност: ако разглежданата карта не е индивидуална, holderSurname съдържа същите данни, като companyname, workshopName или controlBodyName.

holderFirstNames указва името(имената) и инициала(ите) на титуляра.

2.61. K-ConstantOfRecordingEquipment

Константа на уредите за регистриране на данните за движението [определение м)].

$K\text{-ConstantOfRecordingEquipment} ::= \text{INTEGER}(0..2^{16}-1)$

Определяне на стойност: Импулси на километър и намира се в експлоатационен диапазон от 0 до 64 255 имп/км.

2.62. KeyIdentifier

Уникален идентификатор на публичен ключ, позволяващ неговото указване и селектиране. Този идентификатор идентифицира също така титуляра на ключа.

```
KeyIdentifier ::= CHOICE {
    extendedSerialNumber          ExtendedSerialNumber,
    certificateRequestID          CertificateRequestID,
    certificationAuthorityKID     CertificationAuthorityKID
}
```

Първата опция позволява указването на публичния ключ на блок, монтиран на превозното средство или на тахографска карта.

Втората опция позволява указването на публичния ключ на блок, монтиран на превозното средство (в случай че серийният номер на блока е неизвестен по време на изработването на сертификата).

Третата опция позволява указването на публичния ключ на определена държава-членка.

2.63. L-TyreCircumference

Реална окръжност на търкаляне на гумите [определение ф)].

$L\text{-TyreCircumference} ::= \text{INTEGER}(0..2^{16}-1)$

Определяне на стойност: Двоична без знак. Стойност, изразена в 1/8 от мм и намира се в експлоатационен диапазон от 0 до 8031 мм.

2.64. Language

Код, идентифициращ определен работен език.

$Language ::= \text{IA5String}(\text{SIZE}(2))$

Определяне на стойност: Код, съставен от две малки букви съгласно стандарт ISO 639.

2.65. LastCardDownload

Дата и час, записани на картата на водача, на последното прехвърляне на данните от дадена карта (с цели, различни от извършването на контрол). Тази дата може да бъде актуализирана посредством блок, монтиран на превозното средство, или всяко картово четящо устройство.

$LastCardDownload ::= \text{TimeReal}$

Определяне на стойност: Липса на допълнителна информация.

2.66. ManualInputFlag

Код, позволяващ да се разбере дали притежателят на картата е извършил или не ръчно въвеждане на дейностите на водача по време на поставянето на тази карта (изискване 081).

```
ManualInputFlag ::= INTEGER {
    noEntry                (0)
    manualEntries          (1)
}
```

Определяне на стойност: Липса на допълнителна информация.

2.67. ManufacturerCode

Код, идентифициращ определен производител.

```
ManufacturerCode ::= INTEGER(0..255)
```

Определяне на стойност:

'00'H	Няма никаква информация
'01'H	Запазена стойност
'02'H .. '0F'H	Запазено за по-нататъшна употреба
'10'H	ACTIA
'11'H .. '17'H	Запазено за производители, чието име започва с „А“
'18'H .. '1F'H	Запазено за производители, чието име започва с „В“
'20'H .. '27'H	Запазено за производители, чието име започва с „С“
'28'H .. '2F'H	Запазено за производители, чието име започва с „D“
'30'H .. '37'H	Запазено за производители, чието име започва с „Е“
'38'H .. '3F'H	Запазено за производители, чието име започва с „F“
'40'H	Giesecke & Devrient GmbH
'41'H	GEM plus
'42'H .. '47'H	Запазено за производители, чието име започва с „G“
'48'H .. '4F'H	Запазено за производители, чието име започва с „H“
'50'H .. '57'H	Запазено за производители, чието име започва с „I“
'58'H .. '5F'H	Запазено за производители, чието име започва с „J“
'60'H .. '67'H	Запазено за производители, чието име започва с „K“
'68'H .. '6F'H	Запазено за производители, чието име започва с „L“
'70'H .. '77'H	Запазено за производители, чието име започва с „M“
'78'H .. '7F'H	Запазено за производители, чието име започва с „N“
'80'H	OSCARD
'81'H .. '87'H	Запазено за производители, чието име започва с „O“
'88'H .. '8F'H	Запазено за производители, чието име започва с „P“
'90'H .. '97'H	Запазено за производители, чието име започва с „Q“
'98'H .. '9F'H	Запазено за производители, чието име започва с „R“
'A0'H	SETEC
'A1'H	SIEMENS VDO
'A2'H	STONERIDGE
'A3'H .. 'A7'H	Запазено за производители, чието име започва с „S“
'AA'H	TACHOCONTROL
'AB'H .. 'AF'H	Запазено за производители, чието име започва с „T“
'B0'H .. 'B7'H	Запазено за производители, чието име започва с „U“
'B8'H .. 'BF'H	Запазено за производители, чието име започва с „V“
'C0'H .. 'C7'H	Запазено за производители, чието име започва с „W“
'C8'H .. 'CF'H	Запазено за производители, чието име започва с „X“
'D0'H .. 'D7'H	Запазено за производители, чието име започва с „Y“
'D8'H .. 'DF'H	Запазено за производители, чието име започва със „Z“

2.68. MemberStateCertificate

Сертификат на публичния ключ на определена държава-членка, издаден от европейския удостоверяващ орган.

```
MemberStateCertificate ::= Certificate
```

2.69. MemberStatePublicKey

Публичен ключ на определена държава-членка.

MemberStatePublicKey ::= PublicKey

2.70. Name

Име.

```
Name ::= SEQUENCE {
    codePage                INTEGER (0..255),
    name                    OCTET STRING (SIZE(35))
}
```

codePage специфицира частта от стандарта ISO/CEI 8859, използвана за кодирането на името.

name указва име, кодирането на което се извършва съгласно съответната страница с кодове от стандарта ISO/CEI 8859.

2.71. NationAlpha

Азбучна препратка към определена страна съгласно класическото кодиране на нациите, което се използва при самозалепващите винетки, поставяни на броните и/или хармонизираните документи, издавани от застрахователните компании (зелена карта).

NationAlpha ::= IA5String(SIZE(3))

Определяне на стойност:

' '	Няма никаква информация
'A'	Австрия
'AL'	Албания
'AND'	Андора
'ARM'	Армения
'AZ'	Азербайджан
'B'	Белгия
'BG'	България
'BIN'	Босна и Херцеговина
'BY'	Беларус
'CH'	Швейцария
'CY'	Кипър
'CZ'	Чешка република
'D'	Германия
'DK'	Дания
'E'	Испания
'EST'	Естония
'F'	Франция
'FIN'	Финландия
'FL'	Лихтенщайн
'FR'	Фарьорски острови
'UK'	Обединено кралство, Олдърни, Гърнзи, Джързи, Остров Ман, Гибралтар
'GE'	Грузия
'GR'	Гърция
'H'	Унгария
'HR'	Хърватска
'I'	Италия
'IRL'	Ирландия
'IS'	Исландия
'KZ'	Казахстан
'L'	Люксембург
'LT'	Литва
'LV'	Латвия
'M'	Малта
'MC'	Монако

'MD'	Република Молдова
'MK'	Македония
'N'	Норвегия
'NL'	Нидерландия
'P'	Португалия
'PL'	Полша
'RO'	Румъния
'RSM'	Сан Марино
'RUS'	Руска федерация
'S'	Швеция
'SK'	Словакия
'SLO'	Словения
'TM'	Туркменистан
'TR'	Турция
'UA'	Украйна
'V'	Ватикана
'YU'	Югославия
'UNK'	Неизвестно
'EC'	Европейска общност
'EUR'	Останала част от Европа
'WLD'	Останала част от света.

2.7.2. NationNumeric

Цифров код, указващ определена страна.

`NationNumeric ::= INTEGER(0..255)`

Определяне на стойност:

-- Няма никаква информация	(00)H,
-- Австрия	(01)H,
-- Албания	(02)H,
-- Андора	(03)H,
-- Армения	(04)H,
-- Азербайджан	(05)H,
-- Белгия	(06)H,
-- България	(07)H,
-- Босна и Херцеговина	(08)H,
-- Беларус	(09)H,
-- Швейцария	(0A)H,
-- Кипър	(0B)H,
-- Чешка република	(0C)H,
-- Германия	(0D)H,
-- Дания	(0E)H,
-- Испания	(0F)H,
-- Естония	(10)H,
-- Франция	(11)H,
-- Финландия	(12)H,
-- Лихтенщайн	(13)H,
-- Фарьорски острови	(14)H,
-- Обединено кралство	(15)H,
-- Грузия	(16)H,
-- Гърция	(17)H,
-- Унгария	(18)H,
-- Хърватска	(19)H,
-- Италия	(1A)H,
-- Ирландия	(1B)H,
-- Исландия	(1C)H,

-- Казахстан	(1D)H,
-- Люксембург	(1E)H,
-- Литва	(1F)H,
-- Латвия	(20)H,
-- Малта	(21)H,
-- Монако	(22)H,
-- Република Молдова	(23)H,
-- Македония	(24)H,
-- Норвегия	(25)H,
-- Нидерландия	(26)H,
-- Португалия	(27)H,
-- Полша	(28)H,
-- Румъния	(29)H,
-- Сан Марино	(2A)H,
-- Руска федерация	(2B)H,
-- Швеция	(2C)H,
-- Словакия	(2D)H,
-- Словения	(2E)H,
-- Туркменистан	(2F)H,
-- Турция	(30)H,
-- Украйна	(31)H,
-- Ватикана	(32)H,
-- Югославия	(33)H,
-- RFU	(34..FC)H,
-- Европейска общност	(FD)H,
-- Останала част от Европа	(FE)H,
-- Останала част от света	(FF)H

2.73. NoOfCalibrationRecords

Брой на записите на еталониранията, които една цехова карта може да съхрани.

NoOfCalibrationRecords ::= INTEGER(0..255)

Определяне на стойност: виж параграф 3.

2.74. NoOfCalibrationsSinceDownload

Брояч, указващ броя на еталониранията, извършени с една цехова карта от последното прехвърляне на данни, извършено с нея (изискване 230).

NoOfCalibrationsSinceDownload ::= INTEGER(0..2¹⁶-1),

Определяне на стойност: липса на допълнителна информация.

2.75. NoOfCardPlaceRecords

Брой на записите на местоположенията, които една карта на водач или цехова карта може да съхрани.

NoOfCardPlaceRecords ::= INTEGER(0..255)

Определяне на стойност: виж параграф 3.

2.76. NoOfCardVehicleRecords

Брой на записите на данните относно превозното средство, които една карта на водач или цехова карта може да съхрани.

NoOfCardVehicleRecords ::= INTEGER(0..2¹⁶-1)

Определяне на стойност: виж параграф 3.

2.77. NoOfCompanyActivityRecords

Брой на записите на дейностите, извършвани от предприятие, които една карта на предприятие може да съхрани.

NoOfCompanyActivityRecords ::= INTEGER(0..2¹⁶-1)

Определяне на стойност: виж параграф 3.

2.78. NoOfControlActivityRecords

Брой на записите на дейностите по осъществяване на контрол, които една карта на контролър може да съхрани.

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

Определяне на стойност: виж параграф 3.

2.79. NoOfEventsPerType

Брой на събитията от всеки тип, които една карта може да съхрани.

`NoOfEventsPerType ::= INTEGER(0..255)`

Определяне на стойност: виж параграф 3.

2.80. NoOfFaultsPerType

Брой на аномалиите от всеки тип, които една карта може да съхрани.

`NoOfFaultsPerType ::= INTEGER(0..255)`

Определяне на стойност: виж параграф 3.

2.81. OdometerValueMidnight

Стойност, отчетена от брояча на километрите на превозното средство точно в полунощ на определен ден (изискване 090).

`OdometerValueMidnight ::= OdometerShort`

Определяне на стойност: липса на допълнителна информация.

2.82. OdometerShort

Стойност, отчетена от брояча на километрите на превозното средство в съкратена форма.

`OdometerShort ::= INTEGER(0..224-1)`

Определяне на стойност: Двоична без знак. Стойност, изразена в километри, и намираща се в експлоатационен диапазон от 0 до 9 999 999 км.

2.83. OverspeedNumber

Брой на събитията от типа превишаване на допустимата скорост, настъпили след последния контрол за превишаванията на допустимата скорост.

`OverspeedNumber ::= INTEGER(0..255)`

Определяне на стойност: 0 означава, че никакво събитие от типа превишаване на допустимата скорост не е настъпило след последния контрол за превишаванията на допустимата скорост, 1 означава, че събитие от този тип е настъпило веднъж след последния контрол за превишаванията на допустимата скорост ... 255 означава, че броят на събитията от типа превишаване на допустимата скорост, настъпили след последния контрол за превишаванията на допустимата скорост, е равен на 255 или надвишава тази стойност.

2.84. PlaceRecord

Информации относно местоположението в началото или в края на един дневен период на работа (изисквания 087, 202 и 221).

```
PlaceRecord ::= SEQUENCE {
    entryTime                               TimeReal,
    entryTypeDailyWorkPeriod                EntryTypeDailyWorkPeriod,
    dailyWorkPeriodCountry                  NationNumeric,
    dailyWorkPeriodRegion                   RegionNumeric,
    vehicleOdometerValue                    OdometerShort
}
```

entryTime указва датата и часа на въвеждането на данните.

entryTypeDailyWorkPeriod указва типа на въвеждането.

dailyWorkPeriodCountry указва въведената страна.

dailyWorkPeriodRegion указва въведената област.

vehicleOdometerValue указва стойността, отчетена от брояча на километрите в часа на въвеждането на местоположението.

2.85. PreviousVehicleInfo

Информации относно превозното средство, използвано преди това от определен водач по време на поставянето на неговата карта в четящото устройство на определен блок, монтиран на превозното средство (изискване 081).

```
PreviousVehicleInfo ::= SEQUENCE {
    vehicleRegistrationIdentification      VehicleRegistrationIdentification,
    cardWithdrawalTime                    TimeReal
}
```

vehicleRegistrationIdentification указва регистрационния номер, както и държавата-членка, извършила регистрацията на превозното средство.

cardWithdrawalTime указва датата и часа на изваждането на картата.

2.86. PublicKey

Публичен ключ RSA

```
PublicKey ::= SEQUENCE {
    rsaKeyModulus                        RSAKeyModulus,
    rsaKeyPublicExponent                 RSAKeyPublicExponent
}
```

rsaKeyModulus указва модула на двойката ключове.

rsaKeyPublicExponent указва публичния степенен показател на двойката ключове.

2.87. RegionAlpha

Азбучни съответствия на различните области на определена страна.

```
RSACKeyModulus ::= OCTET STRING (SIZE (128))
```

Определяне на стойност:

' ' Няма никаква информация

Испания:

'AN'	Андалусия
'AR'	Арагон
'AST'	Астурия
'C'	Кантабрия
'CAT'	Каталуния
'CL'	Кастилия и Леон
'CM'	Кастилия-Ла Манча
'CV'	Валенсия
'EXT'	Естремадура
'G'	Галисия
'IB'	Балеарски острови
'IC'	Канарски острови
'LR'	Ла Риоха
'M'	Мадрид
'MU'	Мурсия
'NA'	Навара
'PV'	Баския

2.88. RegionNumeric

Азбучни съответствия на различните области на определена страна.

```
RegionNumeric ::= OCTET STRING (SIZE (1))
```

Определяне на стойност:

'00'Н Няма никаква информация

Испания:

'01'Н Андалусия
 '02'Н Арагон
 '03'Н Астурия
 '04'Н Кантабрия
 '05'Н Каталуния
 '06'Н Кастилия и Леон
 '07'Н Кастилия-Ла Манча
 '08'Н Валенсия
 '09'Н Естремадура
 '0A'Н Галисия
 '0B'Н Балеарски острови
 '0C'Н Канарски острови
 '0D'Н Ла Риоха
 '0E'Н Мадрид
 '0F'Н Мурсия
 '10'Н Навара
 '11'Н Баския

2.89. RSAKeyModulus

Модул на двойка ключове RSA.

`RSAKeyModulus ::= OCTET STRING (SIZE(128))`

Определяне на стойност: не е указана.

2.90. RSAKeyPrivateExponent

Частен степенен показател на двойка ключове RSA.

`RSAKeyPrivateExponent ::= OCTET STRING (SIZE(128))`

Определяне на стойност: не е указана.

2.91. RSAKeyPublicExponent

Публичен степенен показател на двойка ключове RSA.

`RSAKeyPublicExponent ::= OCTET STRING (SIZE(8))`

Определяне на стойност: не е указана.

2.92. SensorApprovalNumber

Номер на типово одобрение на датчика.

`SensorApprovalNumber ::= IA5String(SIZE(8))`

Определяне на стойност: не е указана.

2.93. SensorIdentification

Информации, записани в паметта на датчик за движение и отнасящи се до идентифицирането на този елемент (изискване 077).

```
SensorIdentification ::= SEQUENCE {
    sensorSerialNumber          SensorSerialNumber,
    sensorApprovalNumber       SensorApprovalNumber,
    sensorSCIdentifier          SensorSCIdentifier,
    sensorOSIdentifier         SensorOSIdentifier
}
```


sensorSerialNumber указва разширения сериен номер на датчика за движение (включително фабричния номер и кода на производителя).

sensorApprovalNumber указва номера на одобрение на датчика за движение.

sensorSCIdentifier указва идентификатора на компонента за сигурност на датчика за движение.

sensorOSIdentifier указва идентификатора на операционната система на датчика за движение.

2.94. SensorInstallation

Информации, записани в паметта на датчик за движение и отнасящи се до монтирането на този елемент (изискване 099).

```
SensorInstallation ::= SEQUENCE {
    sensorPairingDateFirst          SensorPairingDate,
    firstVuApprovalNumber          VuApprovalNumber,
    firstVuSerialNumber            VuSerialNumber,
    sensorPairingDateCurrent       SensorPairingDate,
    currentVuApprovalNumber        VuApprovalNumber,
    currentVUSerialNumber          VuSerialNumber
}
```

sensorPairingDateFirst указва датата на първото свързване на датчика за движение с блок, монтиран на превозно средство.

firstVuApprovalNumber указва номера на одобрение на първия блок, монтиран на превозно средство, който е свързан с датчика за движение.

firstVuSerialNumber указва серийния номер на първия блок, монтиран на превозно средство, който е свързан с датчика за движение.

sensorPairingDateCurrent указва датата на сегашното свързване на датчика за движение с блока, монтиран на превозно средство.

currentVuApprovalNumber указва номера на одобрение на блока, монтиран на превозно средство, който е свързан в момента с датчика за движение.

currentVUSerialNumber указва серийния номер на блока, монтиран на превозно средство, който е свързан в момента с датчика за движение.

2.95. SensorInstallationSecData

Информации, записани на цехова карта и отнасящи се до данните относно сигурността, необходими за свързването на датчиците за движение с блоковете, монтирани на превозните средства (изискване 214).

```
SensorInstallationSecData ::= TDesSessionKey
```

Определяне на стойност: съгласно стандарт ISO 16844-3.

2.96. SensorOSIdentifier

Идентификатор на операционната система на датчика за движение.

```
SensorOSIdentifier ::= IA5String(SIZE(2))
```

Определяне на стойност: зависи от производителя.

2.97. SensorPaired

Информации, записани в паметта на блок, монтиран на превозното средство, и отнасящи се до идентифицирането на датчика за движение, свързан с този блок (изискване 079).

```
SensorPaired ::= SEQUENCE {
    sensorSerialNumber          SensorSerialNumber,
    sensorApprovalNumber        SensorApprovalNumber,
    sensorPairingDateFirst      SensorPairingDate
}
```

sensorSerialNumber указва серийния номер на датчика за движение, който е свързан в момента с блока, монтиран на превозното средство.

sensorApprovalNumber указва номера на одобрение на датчика за движение, който е свързан в момента с блока, монтиран на превозното средство.

sensorPairingDateFirst указва датата на първото свързване на блок, монтиран на превозно средство, с датчика за движение, който е свързан в момента с блока, монтиран на разглежданото превозно средство

2.98. **SensorPairingDate**

Дата на свързване на датчика за движение с блок, монтиран на превозно средство.

`SensorPairingDate ::= TimeReal`

Определяне на стойност: не е указана.

2.99. **SensorSerialNumber**

Сериен номер на датчика за движение.

`SensorSerialNumber ::= ExtendedSerialNumber`

2.100. **SensorSCIdentifier**

Идентификатор на компонента за сигурност на датчика за движение.

`SensorSCIdentifier ::= IA5String(SIZE(8))`

Определяне на стойност: зависи от производителя на компонента.

2.101. **Signature**

Цифров подпис.

`Signature ::= OCTET STRING (SIZE(128))`

Определяне на стойност: съгласно допълнение 11 (Общи механизми за сигурност).

2.102. **SimilarEventsNumber**

Брой на сходните събития, възникнали в определен ден (изискване 094).

`SimilarEventsNumber ::= INTEGER(0..255)`

Определяне на стойност: 0 не се използва, 1 означава, че само едно събитие от този тип е настъпило и е било записано през съответния ден, 2 означава, че две събития от този тип са настъпили през съответния ден (и само едно от тях е било записано), ... 255 означава, че през разглеждания ден са настъпили 255 или повече събития от този тип.

2.103. **SpecificConditionType**

Код, идентифициращ особено условие (изисквания 050b, 105a, 212a и 230a).

`SpecificConditionType ::= INTEGER(0..255)`

Определяне на стойност:

'00'H	RFU
'01'H	Извън обсег - Начало
'02'H	Извън обсег - Край
'03'H	Пътуване с ферибот/влак
'04'H .. 'FF'H	RFU

2.104. **SpecificConditionRecord**

Информации, записани на карта на водача, на цехова карта или на блок, монтиран на превозното средство, и отнасящи се до определено особено условие (изисквания 105a, 212a и 230a).

```
SpecificConditionRecord ::= SEQUENCE {
    entryTime                TimeReal,
    specificConditionType    SpecificConditionType
}
```

entryTime указва датата и часа на въвеждането на тези данни.

specificConditionType указва кода, идентифициращ въпросното особено условие.

2.105. Speed

Скорост на превозното средство (км/ч).

```
Speed ::= INTEGER(0..255)
```

Определяне на стойност: Стойност, изразена в км/ч и намираща се в експлоатационен диапазон от 0 до 220 км/ч.

2.106. SpeedAuthorised

Максимална разрешена скорост на превозното средство [определение бб)].

```
SpeedAuthorised ::= Speed
```

2.107. SpeedAverage

Средна скорост, измерена по отношение на предварително определено времетраене (км/ч).

```
SpeedAverage ::= Speed
```

2.108. SpeedMax

Максимална скорост, измерена по време на предварително определено времетраене.

```
SpeedMax ::= Speed
```

2.109. TDesSessionKey

Ключ на сесия Троен DES (Data Encryption Standart).

```
TDesSessionKey ::= SEQUENCE {
    tDesKeyA                OCTET STRING (SIZE(8))
    tDesKeyB                OCTET STRING (SIZE(8))
}
```

Определяне на стойност: липса на допълнителна информация.

2.110. TimeReal

Код, свързан с поле, съчетаващо датата и часа, изразени в секунди, считано от 00ч.00м.00сек. по координираното универсално време на 1 януари 1970 г.

```
TimeReal{INTEGER:TimeRealRange} ::= INTEGER(0..TimeRealRange)
```

Определяне на стойност — Поредов байт: брой секунди, изтекли след полунощ по координираното универсално време на 01 януари 1970 г.

Най-далечната бъдеща дата/час е през 2106 г.

2.111. TyreSize

Обозначение на размерите на гумите.

```
TyreSize ::= IA5String(SIZE(15))
```

Определяне на стойност: съгласно Директива 92/23/ЕИО от 31.3.1992 г. (ОБ L 129 от 14.5.1992 г., стр. 95).

2.112. VehicleIdentificationNumber

Идентификационен номер на превозното средство (NIIDV), отнасящ се до цялото превозно средство; обикновено се отнася до серийния номер на шасито или до номера на рамата.

VehicleIdentificationNumber ::= IA5String(SIZE(17))

Определяне на стойност: съгласно стандарт ISO 3779.

2.113. VehicleRegistrationIdentification

Идентифициране на превозно средство, което е уникално в рамките на Европа (регистрационен номер и държава-членка).

```
VehicleRegistrationIdentification ::= SEQUENCE {
    vehicleRegistrationNation      NationNumeric,
    vehicleRegistrationNumber      VehicleRegistrationNumber
}
```

vehicleRegistrationNation указва страната, в която е извършена регистрацията на превозното средство.

vehicleRegistrationNumber указва регистрационния номер на превозното средство (VIN).

2.114. VehicleRegistrationNumber

Регистрационен номер на превозното средство (VIN). Регистрационният номер на превозното средство се издава от органа, който е компетентен относно регистрацията на превозните средства.

```
VehicleRegistrationNumber ::= SEQUENCE {
    codePage                      INTEGER (0..255),
    vehicleRegNumber              OCTET STRING (SIZE(13))
}
```

codePage (страница с кодове) специфицира частта от стандарта ISO/CEI 8859, използван за кодирането на регистрационния номер на превозното средство.

vehicleRegNumber указва регистрационен номер на превозно средство, кодирането на който се извършва съгласно съответната страница с кодове от стандарта ISO/CEI 8859.

Определяне на стойност: зависи от съответната страна.

2.115. VuActivityDailyData

Информации, записани в паметта на блок, монтиран на превозното средство, и отнасящи се до промените на дейността, както и до промените в положението при кормуване и/или в състоянието на картата за определен календарен ден (изискване 084) и в състоянието на четящите устройства в 00.00 часа на този ден.

```
VuActivityDailyData ::= SEQUENCE {
    noOfActivityChanges           INTEGER SIZE(0..1440),
    activityChangeInfos           SET SIZE(noOfActivityChanges) OF
    ActivityChangeInfo
}
```

noOfActivityChanges указва броя на думите, които съдържа комплектът ActivityChangeInfos.

activityChangeInfo указва комплекта от думи ActivityChangeInfo, записани в блока за разглеждания ден. Той съдържа винаги две думи ActivityChangeInfo, които указват състоянието на двете четящи устройства в 00.00 часа на същия ден.

2.116. VuApprovalNumber

Номер на типово одобрение на блока, монтиран на превозното средство.

VuApprovalNumber ::= IA5String(SIZE(8))

Определяне на стойност: не е указана.

2.117. VuCalibrationData

Информации, записани в паметта на блок, монтиран на превозното средство, и отнасящи се до последователните еталонирания на уредите за регистриране на данните за движението (изискване 098).

```
VuCalibrationData ::= SEQUENCE {
    noOfVuCalibrationRecords      INTEGER(0..255),
    vuCalibrationRecords SET      SIZE(noOfVuCalibrationRecords) OF
    VuCalibrationRecord
}
```

noOfVuCalibrationRecords указва броя на записите, които съдържа комплектът **vuCalibrationRecords**.

vuCalibrationRecords указва комплекта със записите от еталониранията.

2.118. VuCalibrationRecord

Информации, записани в паметта на блок, монтиран на превозното средство, и отнасящи се до еталониране на уредите за регистриране на данните за движението (изискване 098).

```
VuCalibrationRecord ::= SEQUENCE {
    calibrationPurpose           CalibrationPurpose,
    workshopName                 Name,
    workshopAddress              Address,
    workshopCardNumber           FullCardNumber,
    workshopCardExpiryDate      TimeReal,
    vehicleIdentificationNumber  VehicleIdentificationNumber,
    vehicleRegistrationIdentification VehicleRegistrationIdentification,
    wVehicleCharacteristicConstant W-VehicleCharacteristicConstant,
    kConstantOfRecordingEquipment K-ConstantOfRecordingEquipment,
    lTyreCircumference           L-TyreCircumference,
    tyreSize                     TyreSize,
    authorisedSpeed              SpeedAuthorised,
    oldOdometerValue             OdometerShort,
    newOdometerValue             OdometerShort,
    oldTimeValue                 TimeReal,
    newTimeValue                 TimeReal,
    nextCalibrationDate          TimeReal
}
```

calibrationPurpose указва причината за еталонирането.

workshopName, **workshopAddress** указват името и адреса на цеха.

workshopCardNumber идентифицира цеховата карта, използвана по време на еталонирането.

workshopCardExpiryDate указва датата на край на валидността на картата.

vehicleIdentificationNumber указва идентификационния номер на превозното средство.

vehicleRegistrationIdentification съдържа регистрационния номер, както и държавата-членка, извършила регистрацията на превозното средство.

wVehicleCharacteristicConstant указва характеристикния коефициент на превозното средство.

kConstantOfRecordingEquipment указва константата на уредите за регистриране на данните за движението.

lTyreCircumference указва реалната окръжност на търкаляне на гумите.

tyreSize указва обозначаването на размерите на гумите, монтирани на превозното средство.

authorisedSpeed указва разрешената скорост на превозното средство.

oldOdometerValue, **newOdometerValue** указват старата и новата стойност, отчетени от брояча на километрите.

oldTimeValue, **newTimeValue** указват старите и новите стойности на датата и часа.

nextCalibrationDate указва датата на следващото еталониране, съответстващо на типа, указан в полето **CalibrationPurpose**, което лицензирият инспектиращ орган трябва да извърши.

2.119. VuCardIWDData

Информации, записани в паметта на блок, монтиран на превозното средство, и отнасящи се до циклите на поставяне и на изваждане на карти на водач или цехови карти в съответното четящо устройство на този блок (изискване 081).

```
VuCardIWDData ::= SEQUENCE {
    noOfIWRecords                INTEGER(0..216-1),
    vuCardIWRecords              SET SIZE (noOfIWRecords) OF
                                VuCardIWRecord
}
```

noOfIWRRecords указва броя на записите, които съдържа комплектът **vuCardIWRRecords**

vuCardIWRRecords указва комплект от записи относно циклите на поставяне и изваждане на картите.

2.120. VuCardIWRRecord

Информации, записани в паметта на блок, монтиран на превозното средство и отнасящи се до циклите на поставяне и на изваждане на определена карта на водач или цехова карта в съответното четящо устройство на този блок (изискване 081).

```
VuCardIWRRecord ::= SEQUENCE {
    cardHolderName                HolderName,
    fullCardNumber                 FullCardNumber,
    cardExpiryDate                 TimeReal,
    cardInsertionTime              TimeReal,
    vehicleOdometerValueAtInsertion OdometerShort,
    cardSlotNumber                 CardSlotNumber,
    cardWithdrawalTime             TimeReal,
    vehicleOdometerValueAtWithdrawal OdometerShort,
    previousVehicleInfo            PreviousVehicleInfo
    manualInputFlag                ManualInputFlag
}
```

cardHolderName указва фамилията и името(името и презимето) на водача или на притежателя на цеховата карта така, както те са записани на нея.

fullCardNumber указва типа на картата, държавата-членка, която я е издала, и номера ѝ така, както тези данни са записани на нея.

cardExpiryDate указва датата на край на валидността на картата така, както тя е записана на нея.

cardInsertionTime указва датата и часа на поставянето на картата.

vehicleOdometerValueAtInsertion указва стойността, отчетена от брояча на километрите в момента на поставяне на картата.

cardSlotNumber указва четящото устройство, в процеп на което е поставена картата.

cardWithdrawalTime указва датата и часа на изваждането на картата.

vehicleOdometerValueAtWithdrawal указва стойността, отчетена от брояча на километрите в момента на поставяне на картата.

previousVehicleInfo съдържа информация относно последното превозно средство, използвано от водача, така, както тя е записана на картата.

manualInputFlag съответства на флаг, позволяващ да се разбере дали притежателят на картата е извършил или не ръчно въвеждане на дейностите на водача по време на поставянето на тази карта.

2.121. VuCertificate

Сертификат, свързан с публичния ключ на блок, монтиран на превозното средство.

```
VuCertificate ::= Certificate
```

2.122. VuCompanyLocksData

Информации, записани в паметта на блок, монтиран на превозното средство, и отнасящи се до блокировките от страна на предприятието (изискване 104).

```
VuCompanyLocksData ::= SEQUENCE {
    noOfLocks                      INTEGER(0..20),
    vuCompanyLocksRecords          SET SIZE(noOfLocks) OF
                                   VuCompanyLocksRecord
}
```

noOfLocks указва броя на блокировките, записани във **vuCompanyLocksRecords**.

vuCompanyLocksRecords съответства на комплекта от записи на блокировките от страна на предприятието.

2.123. VuCompanyLocksRecord

Информации, записани в паметта на блок, монтиран на превозното средство, и отнасящи се до определена блокировка от страна на предприятието (изискване 104).

```
VuCompanyLocksRecord ::= SEQUENCE {
    lockInTime           TimeReal,
    lockOutTime          TimeReal,
    companyName          Name,
    companyAddress       Address,
    companyCardNumber   FullCardNumber
}
```

lockInTime, **lockOutTime** указват датите и часовете на блокиране и отблокиране.

companyName, **companyAddress** указват името и адреса на предприятието, имащо отношение към блокирането.

companyCardNumber идентифицира картата, използвана по време на блокирането.

2.124. VuControlActivityData

Информации, записани в паметта на блок, монтиран на превозното средство, и отнасящи се до контролиранията, извършени с помощта на този блок (изискване 102).

```
VuControlActivityData ::= SEQUENCE {
    noOfControls          INTEGER(0..20),
    vuControlActivityRecords SET SIZE(noOfControls) OF
                          VuControlActivityRecord
}
```

noOfControls указва броя на контролиранията, записани в **vuControlActivityRecords**.

vuControlActivityRecords указва комплекта от записи относно дейността по извършване на контрол.

2.125. VuControlActivityRecord

Информации, записани в паметта на блок, монтиран на превозното средство, и отнасящи се до точно определен контрол, извършен с помощта на този блок (изискване 102).

```
VuControlActivityRecord ::= SEQUENCE {
    controlType           ControlType,
    controlTime           TimeReal,
    controlCardNumber    FullCardNumber,
    downloadPeriodBeginTime TimeReal,
    downloadPeriodEndTime TimeReal
}
```

controlType указва типа на извършения контрол.

controlTime указва датата и часа на извършения контрол.

ControlCardNumber идентифицира картата на контролор, използвана по време на извършването на контрола.

downloadPeriodBeginTime указва часа на начало на периода, данните за който са били прехвърлени, при положение че има такова прехвърляне.

downloadPeriodEndTime указва часа на край на периода, данните за който са били прехвърлени при положение, че има такова прехвърляне.

2.126. VuDataBlockCounter

Брояч, записан на карта и идентифициращ последователно циклите на поставяне и изваждане на картата в съответното четящо устройство на блоковете, монтирани на превозните средства.

```
VuDataBlockCounter ::= BCDString(SIZE(2))
```

Определяне на стойност: Последователно номериране, максималната стойност на което е равно на 9999, като броенето започва от 0.

2.127. VuDetailedSpeedBlock

Информации, записани в паметта на блок, монтиран на превозното средство, и отнасящи се до промяната на скоростта на превозното средство в продължение на една минута, по време на която превозното средство е било в движение (изискване 093).

```
VuDetailedSpeedBlock ::= SEQUENCE {
    speedBlockBeginDate          TimeReal,
    speedsPerSecond              SEQUENCE SIZE (60) OF Speed
}
```

speedBlockBeginDate указва датата и часа на първата моментна скорост, която блокът данни съдържа.

speedsPerSecond указва хронологичната последователност на скоростите, измерени през всички секунди на минутата, която е започнала в speedBlockBeginDate (включена).

2.128. VuDetailedSpeedData

Информации, записани в паметта на блок, монтиран на превозното средство, и отнасящи се до промяната на скоростта на превозното средство.

```
VuDetailedSpeedData ::= SEQUENCE {
    noOfSpeedBlocks              INTEGER (0..216-1),
    vuDetailedSpeedBlocks        SET SIZE (noOfSpeedBlocks) OF
                                VuDetailedSpeedBlock
}
```

noOfSpeedBlocks указва броя на блоковете с данни за скоростта, които съдържа комплектът на vuDetailedSpeedBlocks.

vuDetailedSpeedBlocks указва комплекта от блокове с данни от измерване на моментната скорост.

2.129. VuDownloadablePeriod

Най-старата и най-скорошната дати, за които определен блок, монтиран на превозното средство, съдържа данни относно дейностите на водача (изисквания 081, 084 или 087).

```
VuDownloadablePeriod ::= SEQUENCE {
    minDownloadableTime          TimeReal
    maxDownloadableTime          TimeReal
}
```

minDownloadableTime указва най-старите дата и час на поставяне на определена карта, на въвеждане на местоположението или на промяната на дейността, записани в паметта на блока, монтиран на превозното средство.

maxDownloadableTime указва най-скорошните дата и час на изваждане на определена карта, на въвеждане на местоположението или на промяната на дейността, записани в паметта на блока, монтиран на превозното средство.

2.130. VuDownloadActivityData

Информации, записани в паметта на блок, монтиран на превозното средство, и отнасящи се до последното прехвърляне на данните от него (изискване 105).

```
VuDownloadActivityData ::= SEQUENCE {
    downloadingTime              TimeReal,
    fullCardNumber                FullCardNumber,
    companyOrWorkshopName        Name
}
```

downloadingTime указва датата и часа на прехвърлянето на данните.

fullCardNumber идентифицира картата, използвана за разрешаване на прехвърлянето на данните.

companyOrWorkshopName указва името на предприятието или на цеха.

2.131. VuEventData

Информации, записани в паметта на блок, монтиран на превозното средство, и отнасящи се до различни събития (изискване 094, с изключение на събитията от типа превишаване на допустимата скорост).

```
VuEventData ::= SEQUENCE {
    noOfVuEvents                  INTEGER (0..255),
    vuEventRecords                SET SIZE (noOfVuEvents) OF VuEventRecord
}
```

noOfVuEvents указва броя на събитията, записани в комплекта от данни vuEventRecords.

vuEventRecords указва определен комплект със записи на събития.

2.132. VuEventRecord

Информации, записани в паметта на блок, монтиран на превозното средство, и отнасящи се до определено събитие (изискване 094 с изключение на всяко събитие от типа превишаване на допустимата скорост).

```
VuEventRecord ::= SEQUENCE {
    eventType                EventFaultType,
    eventRecordPurpose       EventFaultRecordPurpose,
    eventBeginTime           TimeReal,
    eventEndTime             TimeReal,
    cardNumberDriverSlotBegin FullCardNumber,
    cardNumberCodriverSlotBegin FullCardNumber,
    cardNumberDriverSlotEnd  FullCardNumber,
    cardNumberCodriverSlotEnd FullCardNumber,
    similarEventsNumber      SimilarEventsNumber
}
```

eventType указва типа на събитието.

eventRecordPurpose указва причината за записване на разглежданото събитие.

eventBeginTime указва датата и часа на началото на събитието.

eventEndTime указва датата и часа на края на събитието.

cardNumberDriverSlotBegin идентифицира картата, поставена в предназначения за водача четящо устройство в началото на събитието.

cardNumberCodriverSlotBegin идентифицира картата, поставена в предназначения за помощник-водача четящо устройство в началото на събитието.

cardNumberDriverSlotEnd идентифицира картата, поставена в предназначения за водача четящо устройство в края на събитието.

cardNumberCodriverSlotEnd идентифицира картата, поставена в предназначения за помощник-водача четящо устройство в края на събитието.

similarEventsNumber указва броя на сходните събития, настъпили в същия ден.

Тази последователност се използва за всички събития, освен тези от типа превишаване на допустимата скорост.

2.133. VuFaultData

Информации, записани в паметта на блок, монтиран на превозното средство, и отнасящи се до различни аномалии (изискване 096).

```
VuFaultData ::= SEQUENCE {
    noOfVuFaults            INTEGER(0..255),
    vuFaultRecords SET      SIZE(noOfVuFaults) OF VuFaultRecord
}
```

noOfVuFaults указва броя на аномалиите, записани в комплекта от данни vuFaultRecords.

vuFaultRecords указва комплект със записи на аномалии.

2.134. VuFaultRecord

Информации, записани в паметта на блок, монтиран на превозното средство, и отнасящи се до определена аномалия (изискване 096).

```
VuFaultRecord ::= SEQUENCE {
    faultType                EventFaultType,
    faultRecordPurpose       EventFaultRecordPurpose,
    faultBeginTime           TimeReal,
    faultEndTime             TimeReal,
    cardNumberDriverSlotBegin FullCardNumber,
    cardNumberCodriverSlotBegin FullCardNumber,
    cardNumberDriverSlotEnd  FullCardNumber,
    cardNumberCodriverSlotEnd FullCardNumber
}
```

faultType указва типа на аномалията, засягаща уредите за регистриране на данните за движението.

faultRecordPurpose указва причината за записване на разглежданата аномалия.

faultBeginTime указва датата и часа на началото на аномалията.

faultEndTime указва датата и часа на края на аномалията.

cardNumberDriverSlotBegin идентифицира картата, поставена в предназначения за водача четящо устройство в началото на аномалията.

cardNumberCodriverSlotBegin идентифицира картата, поставена в предназначения за помощник-водача четящо устройство в началото на аномалията.

cardNumberDriverSlotEnd идентифицира картата, поставена в предназначения за водача четящо устройство в края на аномалията.

cardNumberCodriverSlotEnd идентифицира картата, поставена в предназначения за помощник-водача четящо устройство в края на аномалията.

2.135. VuIdentification

Информации, записани в паметта на блок, монтиран на превозното средство, и отнасящи се до идентифицирането на този блок (изискване 075).

```
VuIdentification ::= SEQUENCE {
    vuManufacturerName          VuManufacturerName,
    vuManufacturerAddress      VuManufacturerAddress,
    vuPartNumber                VuPartNumber,
    vuSerialNumber              VuSerialNumber,
    vuSoftwareIdentification    VuSoftwareIdentification,
    vuManufacturingDate        VuManufacturingDate,
    vuApprovalNumber           VuApprovalNumber
}
```

vuManufacturerName указва името на производителя на блока, монтиран на превозното средство.

vuManufacturerAddress указва адреса на производителя на блока, монтиран на превозното средство.

vuPartNumber указва фабричния номер на блока, монтиран на превозното средство.

vuSerialNumber указва серийния номер на блока, монтиран на превозното средство.

vuSoftwareIdentification идентифицира софтуера, използван в блока, монтиран на превозното средство.

vuManufacturingDate указва датата на производство на блока, монтиран на превозното средство.

vuApprovalNumber указва номера на одобрение на блока, монтиран на превозното средство.

2.136. VuManufacturerAddress

Адрес на производителя на блока, монтиран на превозното средство.

```
VuManufacturerAddress ::= Address
```

Определяне на стойност: не е указана.

2.137. VuManufacturerName

Име на производителя на блока, монтиран на превозното средство.

```
VuManufacturerName ::= Name
```

Определяне на стойност: не е указана.

2.138. VuManufacturingDate

Дата на производство на блока, монтиран на превозното средство.

```
VuManufacturingDate ::= TimeReal
```

Определяне на стойност: не е указана.

2.139. VuOverSpeedingControlData

Информации, записани в паметта на блок, монтиран на превозното средство, и отнасящи се до събитията от типа превишаване на допустимата скорост, настъпили след извършването на последния контрол за превишаване на допустимата скорост (изискване 095).

```
VuOverSpeedingControlData ::= SEQUENCE {
    lastOverspeedControlTime      TimeReal,
    firstOverspeedSince           TimeReal,
    numberOfOverspeedSince        OverspeedNumber
}
```

lastOverspeedControlTime указва датата и часа на последния контрол на превишаването на допустимата скорост.

firstOverspeedSince указва датата и часа на първото превишаване на допустимата скорост, констатирано след последния контрол на превишаването на допустимата скорост.

numberOfOverspeedSince указва броя на събитията от типа превишаване на допустимата скорост, настъпили след последния контрол на превишаването на допустимата скорост.

2.140. VuOverSpeedingEventData

Информации, записани в паметта на блок, монтиран на превозното средство, и отнасящи се до събитията от типа превишаване на допустимата скорост (изискване 094).

```
VuOverSpeedingEventData ::= SEQUENCE {
    noOfVuOverSpeedingEvents      INTEGER(0..255),
    vuOverSpeedingEventRecords    SET SIZE(noOfVuOverSpeedingEvents) OF
    VuOverSpeedingEventRecord
}
```

noOfVuOverSpeedingEvents указва броя на събитията, записани в комплекта от данни vuOverSpeedingEventRecords.

vuOverSpeedingEventRecords указва комплект със записи на събития от типа превишаване на допустимата скорост.

2.141. VuOverSpeedingEventRecord

Информации, записани в паметта на блок, монтиран на превозното средство, и отнасящи се до събитията от типа превишаване на допустимата скорост (изискване 094).

```
VuOverSpeedingEventRecord ::= SEQUENCE {
    eventType                     EventFaultType,
    eventRecordPurpose            EventFaultRecordPurpose,
    eventBeginTime                TimeReal,
    eventEndTime                  TimeReal,
    maxSpeedValue                 SpeedMax,
    averageSpeedValue             SpeedAverage,
    cardNumberDriverSlotBegin     FullCardNumber,
    similarEventsNumber           SimilarEventsNumber
}
```

eventType указва типа на събитието.

eventRecordPurpose указва причината за записване на разглежданото събитие.

eventBeginTime указва датата и часа на началото на събитието.

eventEndTime указва датата и часа на края на събитието.

maxSpeedValue указва максималната скорост, измерена по време на събитието.

averageSpeedValue указва средната скорост, измерена по време на събитието.

cardNumberDriverSlotBegin идентифицира картата, поставена в предназначения за водача четящо устройство в началото на събитието.

similarEventsNumber указва броя на сходните събития, настъпили в същия ден.

2.142. VuPartNumber

Фабричен номер на блока, монтиран на превозното средство.

```
VuPartNumber ::= IA5String(SIZE(16))
```

Определяне на стойност: зависи от производителя на блока.

2.143. VuPlaceDailyWorkPeriodData

Информации, записани в паметта на блок, монтиран на превозното средство, и отнасящи се до местоположението в началото или в края на дневните периоди на работа (изискване 087).

```
VuPlaceDailyWorkPeriodData ::= SEQUENCE {
    noOfPlaceRecords          INTEGER(0..255),
    vuPlaceDailyWorkPeriodRecords SET SIZE(noOfPlaceRecords) OF
                               VuPlaceDailyWorkPeriodRecord
}
```

noOfPlaceRecords указва броя на записите, които съдържа комплекта **vuPlaceDailyWorkPeriodRecords**.

vuPlaceDailyWorkPeriodRecords указва комплект със записи на местоположения.

2.144. VuPlaceDailyWorkPeriodRecord

Информации, записани в паметта на блок, монтиран на превозното средство, и отнасящи се до местоположението в началото или в края на определен дневен период на работа (изискване 087).

```
VuPlaceDailyWorkPeriodRecord ::= SEQUENCE {
    fullCardNumber            FullCardNumber,
    placeRecord               PlaceRecord
}
```

fullCardNumber указва типа на картата, държавата-членка, която я е издала, и номера ѝ.

placeRecord съдържа данни относно въведеното местоположение.

2.145. VuPrivateKey

Частен ключ на блок, монтиран на превозното средство.

```
VuPrivateKey ::= RSAKeyPrivateExponent
```

2.146. VuPublicKey

Публичен ключ на блок, монтиран на превозното средство.

```
VuPublicKey ::= PublicKey
```

2.147. VuSerialNumber

Сериен номер на блока, монтиран на превозното средство (изискване 075).

```
VuSerialNumber ::= ExtendedSerialNumber
```

2.148. VuSoftInstallationDate

Дата на инсталиране на версията на операционната система на блока, монтиран на превозното средство.

```
VuSoftInstallationDate ::= TimeReal
```

Определяне на стойност: не е указана.

2.149. VuSoftwareIdentification

Информации, записани в паметта на блок, монтиран на превозното средство, и отнасящи се до инсталирания софтуер.

```
VuSoftwareIdentification ::= SEQUENCE {
    vuSoftwareVersion          VuSoftwareVersion,
    vuSoftInstallationDate     VuSoftInstallationDate
}
```

vuSoftwareVersion указва номера на версията на софтуера на блока.

vuSoftInstallationDate указва датата на инсталиране на тази версия на софтуера.

2.150. VuSoftwareVersion

Номер на версията на софтуера на блока, монтиран на превозното средство.

```
VuSoftwareVersion ::= IA5String(SIZE(4))
```

Определяне на стойност: не е указана.

2.151. VuSpecificConditionData

Информации, записани в паметта на блок, монтиран на превозното средство, и отнасящи се до особените условия.

```
VuSpecificConditionData ::= SEQUENCE {
    noOfSpecificConditionRecords      INTEGER(0..216-1)
    specificConditionRecords          SET SIZE (noOfSpecificConditionRecords) OF
                                     SpecificConditionRecord
}
```

noOfSpecificConditionRecords указва броя на записите, които съдържа комплектът specificConditionRecords.

specificConditionRecords указва комплект със записи относно особените условия.

2.152. VuTimeAdjustmentData

Информации, записани в паметта на блок, монтиран на превозното средство, и отнасящи се до сверяванията на часовника, извършени извън рамките на процедура по пълно еталониране (изискване 101).

```
VuTimeAdjustmentData ::= SEQUENCE {
    noOfVuTimeAdjRecords             INTEGER(0..6),
    vuTimeAdjustmentRecords          SET SIZE (noOfVuTimeAdjRecords) OF
                                     VuTimeAdjustmentRecord
}
```

noOfVuTimeAdjRecords указва броя на записите, които съдържа комплектът vuTimeAdjustmentRecords.

vuTimeAdjustmentRecords указва комплект със записи относно сверяването на часовника.

2.153. VuTimeAdjustmentRecord

Информации, записани в паметта на блок, монтиран на превозното средство, и отнасящи се до определено сверяване на часовника, извършено извън рамките на процедура по пълно еталониране (изискване 101).

```
VuTimeAdjustmentRecord ::= SEQUENCE {
    oldTimeValue                     TimeReal,
    oldTimeValue                     TimeReal,
    newTimeValue                     TimeReal,
    workshopName                     Name,
    workshopAddress                  Address,
    workshopCardNumber               FullCardNumber
}
```

oldTimeValue, newTimeValue указват старите и новите стойности, дадени на датата и часа.

workshopName, workshopAddress указват името и адреса на цеха.

workshopCardNumber идентифицира цеховата карта, използвана за извършване на сверяването на часовника.

2.154. Характеристичен коефициент W на превозното средство

Характеристичен коефициент на превозното средство [определение κ].

```
W-VehicleCharacteristicConstant ::= INTEGER(0..216-1)
```

Определяне на стойност: Импулси на километър и намираща се в експлоатационния диапазон от 0 до 64 255 имп/км.

2.155. WorkshopCardApplicationIdentification

Информации, записани на цехова карта и отнасящи се до идентифицирането на приложението на картата (изискване 190).

```
WorkshopCardApplicationIdentification ::= SEQUENCE {
    typeOfTachographCardId           EquipmentType,
    cardStructureVersion              CardStructureVersion,
    noOfEventsPerType                 NoOfEventsPerType,
    noOfFaultsPerType                 NoOfFaultsPerType,
    activityStructureLength            CardActivityLengthRange,
    noOfCardVehicleRecords            NoOfCardVehicleRecords,
    noOfCardPlaceRecords              NoOfCardPlaceRecords,
    noOfCalibrationRecords            NoOfCalibrationRecords
}
```

typeOfTachographCardId указва типа на картата, която се използва.

cardStructureVersion указва версията на структурата, приложена в картата.

noOfEventsPerType указва броя на събитията от всеки тип, които картата може да съхрани.

noOfFaultsPerType указва броя на аномалиите от всеки тип, които картата може да съхрани.

activityStructureLength указва броя на байтовете, които могат да се използват за съхраняване на записите на дейността.

noOfCardVehicleRecords указва броя на записите на превозното средство, които картата може да съхрани.

noOfCardPlaceRecords указва броя на местоположенията, които картата може да съхрани.

noOfCalibrationRecords указва броя на записите на извършените еталонирания, които картата може да съхрани.

2.156. WorkshopCardCalibrationData

Информации, записани на цехова карта и отнасящи се до определена цехова дейност, извършена с картата (изисквания 227 и 229).

```
WorkshopCardCalibrationData ::= SEQUENCE {
    calibrationTotalNumber            INTEGER(0..216-1),
    calibrationPointerNewestRecord    INTEGER(0..NoOfCalibrationRecords-1),
    calibrationRecords                SET SIZE (NoOfCalibrationRecords) OF
                                        WorkshopCardCalibrationRecord
}
```

calibrationTotalNumber указва общия брой на извършените с картата еталонирания.

calibrationPointerNewestRecord указва индекса на последния запис на извършено еталониране, актуализиран от системата.

Определяне на стойност: число, съответстващо на номератора на запис на извършеното еталониране, започващо със серия от „0“ за първия случай на запис на еталониране в разглежданата структура.

calibrationRecords указва комплекта от записи, съдържащи данните относно извършените еталонирания и/или относно регулирането на показанията на часовника.

2.157. WorkshopCardCalibrationRecord

Информации, записани на цехова карта и отнасящи се до определено еталониране, извършено с картата (изискване 227).

```
WorkshopCardCalibrationRecord ::= SEQUENCE {
    calibrationPurpose                CalibrationPurpose,
    vehicleIdentificationNumber        VehicleIdentificationNumber,
    vehicleRegistration                VehicleRegistrationIdentification,
    wVehicleCharacteristicConstant     W-VehicleCharacteristicConstant,
    kConstantOfRecordingEquipment      K-ConstantOfRecordingEquipment,
    lTyreCircumference                 L-TyreCircumference,
    tyreSize                            TyreSize,
}
```

```

    authorisedSpeed           SpeedAuthorised,
    oldOdometerValue         OdometerShort,
    newOdometerValue         OdometerShort,
    oldTimeValue             TimeReal,
    newTimeValue             TimeReal,
    nextCalibrationDate      TimeReal,
    vuPartNumber             VuPartNumber,
    vuSerialNumber           VuSerialNumber,
    sensorSerialNumber       SensorSerialNumber
}

```

calibrationPurpose указва причината за еталонирането.

vehicleIdentificationNumber указва идентификационния номер на превозното средство.

vehicleRegistration съдържа регистрационния номер, както и държавата-членка, извършила регистрацията на превозното средство.

wVehicleCharacteristicConstant указва характеристикния коефициент на превозното средство.

kConstantOfRecordingEquipment указва константата на уредите за регистриране на данните за движението.

ITyreCircumference указва реалната окръжност на търкаляне на гумите.

tyreSize указва обозначаването на размерите на гумите, монтирани на превозното средство.

authorisedSpeed указва разрешената максимална скорост на превозното средство.

oldOdometerValue, newOdometerValue указват старата и новата стойност, отчетени от брояча на километрите.

oldTimeValue, newTimeValue указват старите и новите стойности на датата и часа.

nextCalibrationDate указва датата на следващото еталониране, съответстващо на типа, указан в полето CalibrationPurpose, което лицензиращият инспектиращ орган трябва да извърши.

vuPartNumber, vuSerialNumber и **sensorSerialNumber** съставят елементите от информация, необходими за идентифицирането на уредите за регистриране на данните за движението.

2.158. WorkshopCardHolderIdentification

Информации, записани на цехова карта и отнасящи се до идентифицирането на притежателя на картата (изискване 216).

```

WorkshopCardHolderIdentification ::= SEQUENCE {
    workshopName             Name,
    workshopAddress          Address,
    cardHolderName           HolderName,
    cardHolderPreferredLanguage Language
}

```

workshopName указва името на цеха или на притежателя на картата.

workshopAddress указва адреса на цеха или на притежателя на картата.

cardHolderName указва фамилията и името (името и презимето) на притежателя на картата (например името на механика).

cardHolderPreferredLanguage указва предпочитания работен език на притежателя на картата.

2.159. WorkshopCardPIN

Индивидуален идентификационен номер на цеховата карта (изискване 213).

```

WorkshopCardPIN ::= IA5String(SIZE(8))

```

Определяне на стойност: известният индивидуален идентификационен номер на притежателя на картата, допълнен отгласно със серия от байтове „FF“, която може да съдържа 8 байта.

3. ОПРЕДЕЛЕНИЯ НА ДИАПАЗОНИТЕ ОТ СТОЙНОСТИ И ОТ РАЗМЕРИ

Определяне на променливите, използвани в определенията на параграф 2.

Диапазон от реално време::= $2^{32}-1$

3.1. Определения, отнасящи се до картите на водача:

Име на променливата	Минимум	Максимум
CardActivityLengthRange	5 544 байта (28 дена 93 промени на дейността на ден)	13 776 байта (28 дена 240 промени на дейността на ден)
NoOfCardPlaceRecords	84	112
NoOfCardVehicleRecords	84	200
NoOfEventsPerType	6	12
NoOfFaultsPerType	12	24

3.2. Определения, отнасящи се до цеховите карти:

Име на променливата	Минимум	Максимум
CardActivityLengthRange	198 байта (1 ден 93 промени на дейността)	492 байта (1 ден 240 промени на дейността)
NoOfCardPlaceRecords	6	8
NoOfCardVehicleRecords	4	8
NoOfEventsPerType	3	3
NoOfEventsPerType	6	6
NoOfCalibrationRecords	88	255

3.3. Определения, отнасящи се до картите на контролор:

Име на променливата	Минимум	Максимум
NoOfControlActivityRecords	230	520

3.4. Определения, отнасящи се до картите на предприятие:

Име на променливата	Минимум	Максимум
NoOfCompanyActivityRecords	230	520

4. НАБОР ОТ СИМВОЛИ

Низовете IA5 по дефиниция се състоят от ASCII-символи по смисъла на стандарт ISO/CEI 8824-1. За по-голяма четливост и за да се улесни указването на символите, определянето на техните стойности се дава по-долу. В случай на различие, прилагането на стандарт ISO/CEI 8824-1 има предимство пред настоящата информация.

```
! " # $ % & ' ( ) * + , - . / 0 1 2 3 4 5 6 7 8 9 : ; < = > ?
@ A B C D E F G H I J K L M N O P Q R S T U V W X Y Z [ \ ] ^ _
` a b c d e f g h i j k l m n o p q r s t u v w x y z { | } ~
```

Други символни низове (адрес, име, регистрационен номер на превозното средство) използват, освен това, символи, определени от кодове от 192 до 255, дефинирани според стандарт ISO/CEI 8859-1 (набори от латински символи 1) или ISO/CEI 8859-7 (набор от гръцки символи).

5. КОДИРАНЕ

Ако правилата за кодиране от тип ASN.1 се прилагат към различните дефинирани типове данни, тяхното кодиране трябва да съответства на приведения в съответствие вариант на стандарт ISO/CEI 8825-2.

Допълнение 2

ХАРАКТЕРИСТИКИ НА ТАХОГРАФСКИТЕ КАРТИ

СЪДЪРЖАНИЕ

1.	Въведение	101
1.1.	Съкращения	101
1.2.	Изходна база	102
2.	Електрически и физически характеристики	102
2.1.	Захранващо напрежение и потребление на електрически ток	102
2.2.	Напрежение при програмиране V_{pp}	103
2.3.	Генериране на тактове и тактова честота	103
2.4.	Контакти на E/S	103
2.5.	Състояния на картата	103
3.	Хардуер и предаване на информация	103
3.1.	Въведение	103
3.2.	Протокол за предаване на информация	103
3.2.1.	Протоколи	103
3.2.2.	RAR	104
3.2.3.	STP	105
3.3.	Условия за достъп (CA)	105
3.4.	Криптиране	106
3.5.	Общ преглед на командите и кодовете за грешка	106
3.6.	Описание на командите	107
3.6.1.	Select File (селектиране на файл)	107
3.6.1.1.	Селектиране по име (IDA)	107
3.6.1.2.	Селектиране на елементарен файл с помощта на неговия файлов идентификатор	108
3.6.2.	Read Binary (четене на данни)	108
3.6.2.1.	Команда без защитен от неоторизиран достъп обмен на съобщенията	109
3.6.2.2.	Команда със защитен от неоторизиран достъп обмен на съобщенията	109
3.6.3.	Update Binary (актуализиране на данните)	111
3.6.3.1.	Команда без защитен от неоторизиран достъп обмен на съобщенията	111
3.6.3.2.	Команда със защитен от неоторизиран достъп обмен на съобщенията	112
3.6.4.	Get Challenge (получаване на искане за достъп)	113
3.6.5.	Verify (контрол)	113
3.6.6.	Get Response (получаване на отговор)	114
3.6.7.	PSO: Verify Certificate (контрол на валидността)	114
3.6.8.	Internal Authenticate (вътрешно удостоверяване)	115

3.6.9.	External Authenticate (външно удостоверяване).....	116
3.6.10.	Manage Security Environment (управление на средата, свързана със защитата от неоторизиран достъп)	117
3.6.11.	PSO: Hash (сегментиране)	118
3.6.12.	Perform Hash of File (сегментиране на файл)	118
3.6.13.	PSO: Compute Digital Signature (изчисляване на цифровия подпис)	119
3.6.14.	PSO: Verify Digital Signature (контрол на цифровия подпис)	120
4.	Структура на тахографските карти	120
4.1.	Структура на картите на водача	121
4.2.	Структура на цеховите карти	123
4.3.	Структура на картите на контролъора.....	125
4.4.	Структура на картите на предприятие.....	127

1. ВЪВЕДЕНИЕ

1.1. Съкращения

За целите на настоящото допълнение се използват следните съкращения.

AC	Access conditions (Условия за достъп)
AID	Application Identifier (Идентификатор на приложение)
ALW	Always (Винаги)
APDU	Application Protocol Data Unit (structure of a command) (Единица данни на приложния протокол)
ATR	Answer To Reset (Отговор на реинициализиране)
AUT	Authenticated (Удостоверен)
C6, C7	Contacts No 6 and 7 of the card as described in ISO/IEC 7816-2 (Контакти номера 6 и 7 на картата са описани съгласно разпоредбите на стандарт ISO/CEI 7816-2)
cc	clock cycles (тактова честота)
CHV	Card holder Verification Information (Информация за проверка самоличността на титулярите)
CLA	Class Octet of an ADPU command (Байт за определяне на класа на команда на UDPA)
DF	Dedicated File. A DF can contain other files (EF or DF) (Специализиран файл. Той може да съдържа други файлове (елементарни или специализирани файлове))
EF	Elementary File (Елементарен файл)
ENC	Encrypted: Access is possible only by encoding data. (Криптирано: Достъпът е възможен единствено чрез кодирани данни)
etu	elementary time unit (елементарна времева единица)
IC	Integrated Circuit (Вграден чип)
ICC	Integrated Circuit Card (Карта с вграден чип)
ID	Identifier (Идентификатор)
IFD	Interface Device (Периферно интерфейсно устройство)
IFS	Information Field Size (Дължина на зоната за информация)
IFSC	Information Field Size for the card (Дължина на зоната за информация, запазена за картата)
IFSD	Information Field Size Device (for the Terminal) (Дължина на зоната за информация, запазена за терминалното устройство)
INS	Instruction Octet of an ADPU command (Байт за инструкция на определена команда на UDPA)
Lc	Length of the input data for a APDU command (Дължина на входните данни, отнасящи се до определена команда на UDPA)
Le	Length of the expected data (output data for a command) (Дължина на очакваните данни (изходни данни, отнасящи се до определена команда))
MF	Master File (root DF) (Главен файл (специализиран файл, намиращ се в кореновата директория))
P1-P2	Parameter bytes (Байтове за определяне на параметри)
NAD	Node Address used in T = 1 protocol (Възлов адрес, използван в протокол T = 1)
NEV	Never (Никога)
PIN	Personal Identification Number (Персонален идентификационен номер)
PRO SM	Protected with secure messaging (Предпазен посредством защитен от неотризиран достъп обмен на съобщения)
PTS	Protocol Transmission Selection (Избор на протокола за предаване на информацията)
RFU	Reserved for Future Use (Запазен за понататъшно използване)

RST	Reset (of the card) (Реинициализиране (на картата))
SM	Secure Messaging (Защитен от неоторизиран достъп обмен на съобщения)
SW1-SW2	Status bytes (Думи (байтове) за състояние)
TS	Initial ATR character (Начален символ на отговор за реинициализиране)
VPP	Programming Voltage (Напрежение при програмиране)
XXh	Value XX in hexadecimal notation (Стойност XX при записване в шестнадесетичен вид)
	Concatenation symbol 03 04=0304 (Символ за конкатенация 03 04=0304)

1.2. Изходна база

В настоящото допълнение се използва следната изходна база:

EN 726-3	Системи от идентификационни карти — Карти и телекомуникационни терминали с интегрална/и схема/и — Част 3: Изисквания, независещи от приложенията, на които картите трябва да отговарят. Декември 1994 г.
ISO/CEI 7816-2	Информационна технология — Идентификационни карти — Карти с вградена/и интегрална/и схема/и с контакти — Част 2: Размери и местоположение на контактите. Първо издание: 1999 г.
ISO/CEI 7816-3	Информационна технология — Идентификационни карти — Карти с вградена/и интегрална/и схема/и с контакти — Част 3: Електрически сигнали и протоколи за предаване на информация. Второ издание: 1997 г.
ISO/CEI 7816-4	Информационна технология — Идентификационни карти — Карти с вградена/и интегрална/и схема/и с контакти — Част 4: Междоиндустриални команди за вътрешна връзка. Първо издание: 1995 г. + Изменение 1: 1997 г.
ISO/CEI 7816-6	Информационна технология — Идентификационни карти — Карти с вградена/и интегрална/и схема/и с контакти — Част 6: Елементи на междоиндустриалните данни. Първо издание: 1996 г. + Cor 1: 1998 г.
ISO/CEI 7816-8	Информационна технология — Идентификационни карти — Карти с вградена/и интегрална/и схема/и с контакти — Част 8: Междоиндустриални команди, свързани със сигурността. Първо издание: 1999 г.
ISO/CEI 9797	Информационна технология — Техники на предпазване от неоторизиран достъп — Механизми на предпазване на целостта на данните, основаващи се на прилагането на функция за криптографски контрол, използваща алгоритъм за блоково шифроване на данни. Второ издание: 1994 г.

2. ЕЛЕКТРИЧЕСКИ И ФИЗИЧЕСКИ ХАРАКТЕРИСТИКИ

- TCS_200 Всички електронни сигнали трябва да отговарят на стандарт ISO/CEI 7816-3, освен ако не е указано друго.
- TCS_201 Местоположението и размерите на контактите на разглежданата карта трябва да отговарят на стандарта ISO/CEI 7816-2.

2.1. Захранващо напрежение и потребление на електрически ток

- TCS_202 Функционирането на разглежданата карта трябва да отговаря на спецификациите и да бъде в рамките на потреблението, предвидено в стандарт ISO/CEI 7816-3.
- TCS_203 Функционирането на картата трябва да се осигурява от захранващо напрежение $V_{cc} = 3 \text{ V} (\pm 0,3 \text{ V})$ или $V_{cc} = 5 \text{ V} (\pm 0,5 \text{ V})$.

Изборът на съответното напрежение трябва да се извършва съгласно стандарт ISO/CEI 7816-3.

2.2. Напрежение при програмиране V_{pp}

TCS_204 Картата не трябва да изисква прилагането на каквото и да било напрежение при програмиране в краче С6 на чипа. Предвижда се крачето С6 на каквото и да е периферно устройство за четене на карти (PIF) да се свързва. Ако контакт С6 има възможност да бъде свързан към напрежението при програмиране V_{cc} на картата, той не може да се свързва на маса. Това напрежение не подлежи на никакво тълкуване.

2.3. Генериране на тактове и тактова честота

TCS_205 Картата трябва да функционира в диапазон от честоти от 1 до 5 MHz. По време на една и съща сесия, тактовата честота на картата може да варира в рамките на $\pm 2\%$. Тактовата честота се генерира от блока, монтиран на превозното средство, а не от разглежданата карта. Коефициентът на употреба може да варира от 40 до 60 %.

TCS_206 Възможно е спирането на външния тактов генератор при условията, записани във файла на картата FECCI. Първият байт на тялото на файла FECCI програмира условията за приложение на режима „Спиране на тактовия генератор“ (виж EN 726-3 за повече подробности):

Долно	Горно		
Бит 3	Бит 2	Бит 1	
0	0	1	Разрешено спиране на тактовия генератор, няма предпочитаност
0	1	1	Разрешено спиране на тактовия генератор, с предпочитаност към горното равнище
1	0	1	Разрешено спиране на тактовия генератор, с предпочитаност към долното равнище
0	0	0	Забранено спирането на тактовия генератор
0	1	0	Разрешено спиране на тактовия генератор единствено на горното равнище
1	0	0	Разрешено спиране на тактовия генератор единствено на долното равнище

Битове от 4 до 8 не се използват.

2.4. Контакти на E/S

TCS_207 Контактът на E/S C7 позволява приемането и предаването на данни, идващи от или предназначени за съответното PIF. По време на експлоатацията картата и PIF не могат да работят заедно в режим на предаване. Ако се предположи, че тези два компонента биха могли да бъдат използвани в режим на предаване, за картата не би трябвало да има каквото и да е риск от повреда. Когато картата не извършва никакво предаване, тя преминава систематично в режим на приемане.

2.5. Състояния на картата

TCS_208 Картата функционира в две състояния, когато изискваното захранващо напрежение се прилага към контактите ѝ:

- състояние на експлоатация по време на изпълнение на команди или при създаване на връзка с цифрово устройство,
- състояние на покой при всички други случаи; в това състояние картата трябва да запаметява всички необходими данни.

3. ХАРДУЕР И ПРЕДАВАНЕ НА ИНФОРМАЦИЯ

3.1. Въведение

Функциите на тахографските карти и блоковете, монтирани на превозни средства, минимално необходими за гарантиране на задоволителни условия на експлоатация и възможност за взаимна работа, са предмет на подробно описание в настоящия параграф.

Тахографските карти трябва също така да отговарят възможно най-точно на действащите стандарти ISO/CEI (и по-специално на стандарт ISO/CEI 7816). Въпреки това командите и протоколите са предмет на подробно описание, с цел да се дадат при необходимост известни уточнения относно някои ограничени употреби или евентуални различия. Освен ако не е указано противното, всички описани команди отговарят на въпросните стандарти.

3.2. Протокол за предаване на информация

TCS_300 Протоколът за предаване на информация трябва да отговаря на стандарт ISO/CEI 7816-3. По-специално блокът трябва да бъде в състояние да разпознава разширенията на времето на изчакване, които му изпраща картата.

3.2.1. Протоколи

TCS_301 Картата трябва да може да предоставя протоколите $T = 0$ и $T = 1$.

TCS_302 Протоколът $T = 0$ е избран по подразбиране; вследствие на това подаването на команда STP е необходимо за преминаване към протокол $T = 1$.

TCS_303 Периферните устройства трябва да могат да използват прякото условие за връзка, което съдържат тези два протокола. Следователно прякото условие за връзка е задължително за картата.

TCS_304 RAR трябва да представя байта Дължина на зоната за информация, запазена за картата на нивото на символа TA3. Минимална стойност: 'F0h' (= 240 байта).

Следните ограничения се прилагат към протоколите:

TCS_305 $T = 0$

- периферното интерфейсно устройство трябва да може да възприема отговор на нивото на E/S след възходящия фронт на сигнала на RINIT от 400 ch,
- периферното интерфейсно устройство трябва да бъде в състояние да чете символите, разделени с 12 ute,
- периферното интерфейсно устройство трябва да бъде в състояние да разпознава грешен символ и неговото повторение, дори и ако те са разделени с 13 ute. В случай на откриване на грешен символ, сигналът за грешка може да се прояви в E/S в отрязък от време от 1 до 2 ute. Периферното устройство трябва да бъде в състояние да понася закъснение от 1 ute,
- периферното интерфейсно устройство трябва да бъде в състояние да приема RAR от 33 байта (TS+32),
- ако RAR представя символа TC1, предвиденото допълнително време за изчакване трябва да бъде съобразено със символите, предадени чрез периферното интерфейсно устройство, въпреки че символите, предадени чрез картата, могат да бъдат разделени от още 12 ute. Тази разпоредба се прилага също така за символа за удостоверяване на приемане, предаден от картата след предаване на символ P3 от периферното интерфейсно устройство,
- периферното интерфейсно устройство трябва да приеме символ NUL, предаден от картата,
- периферното интерфейсно устройство трябва да приеме режима на допълване за удостоверяване на приемането на информация,
- командата GET RESPONSE (получаване на отговор) не може да се използва в режим на сплъбяване на данните за получаване на блокове с данни, чиято дължина би могла да надвиши 255 байта.

TCS_306 $T = 1$

- байт ADN: не се използва (байтът ADN трябва да бъде поставен на '00'),
- ИЗОСТАВЯНЕ на блок S: не се използва,
- грешка в състоянието VPP, засягаща блок S: не се използва,
- общата дължина на свързването, отнасящо се до определена зона с данни, не трябва да надвишава 255 байта (за да бъде гарантирана от PIF),
- PIF трябва да указва дължината на зоната за информация, запазена за периферното устройство (LZIP) непосредствено след RAR. PIF трябва да предаде запитването за дължина на зоната за информация на блока S след RAR и картата трябва да ѝ върне отново LZI на блок S. Препоръчва се на LZID да се дава следната стойност: 254 байта,
- картата не трябва да прави искане за промяна на LZI.

3.2.2. RAR (Отговор на реинициализиране)

TCS_307 Периферното устройство извършва контрол на байтовете RAR съгласно стандарта ISO/CEI 7816-3. Символите, отбелязващи историята на RAR, не трябва да бъдат подложени на никаква проверка.

Пример за базов двупротоколен RAR съгласно стандарта ISO/CEI 7816-3.

Символ	Стойност	Забележки
TS	'3Bh'	Указва пряко условие за връзка
T0	'85h'	TD1 е налично; наличие на 5 байта, отбелязващи историята
TD1	'80h'	TD2 е налично; Използва се $T = 0$
TD2	'11h'	TA3 е налично; Използва се $T = 1$
TA3	'XXh' (най-малко 'F0h')	Дължина на зоната за информация, запазена за картата (LZIC)
TH1 до TH5	'XXh'	Символи, използвани за отбелязване на историята
TCK	'XXh'	Проверка на символ (ексклузивно OU)

TCS_308 След отговора на реинициализиране (RAR), главният файл (FM) се избира по подразбиране. Той става текуща директория.

3.2.3. STP (Избор на протокола за предаване на информация)

TCS_309 Използва се следният протокол по подразбиране: T = 0. За да се избере протоколът T = 1, периферното устройство трябва да изпрати на картата съобщение за STP (който също така се указва от съкращението PPS).

TCS_310 Също както протоколи T = 0 и T = 1, базовият STP, който позволява промяната на протоколите, е също така задължителен за картата.

STP се използва, съгласно разпоредбите на стандарт ISO/CEI 7816-3, за преминаване към скорост на предаване в битове, която е по-висока от предложената по подразбиране, което при необходимост става посредством картата на нивото на RAR [байт TA(1)].

Използването на по-висока скорост на предаване в битове не е задължително за картата.

TCS_311 Ако картата е съвместима само със скоростта на предаване в битове по подразбиране (или ако избраната скорост на предаване в битове е несъвместима), картата трябва да изпрати правилен отговор на STP, като изпусне байта PPS1, съгласно стандарта ISO/CEI 7816-3.

По-долу фигурира серия от примери за базов STP, предназначени за избирането на протоколи:

Символ	Стойност	Забележки
PPSS	'FFh'	Символ за започване
PPSO	'00h' или '01h'	от PPS1 до PPS3 не са налични; '00h' за избиране на T0, '01h' за избиране на T1
PK	'XXh'	Контролен символ: 'XXh' = 'FFh' ако PPS0 = 00h' 'XXh' = 'FEh' ако PPS0 = '01h'

3.3. Условия за достъп (CA)

Условията за достъп (CA) до командите UPDATE_BINARY и READ_BINARY са определени за всеки елементарен файл.

TCS_312 Условията за достъп до текущия файл трябва да бъдат удовлетворени, преди той да стане достъпен посредством тези команди.

Предвидимите условия за достъп се определят, както следва:

- TJR: винаги предвидимото действие може да се изпълнява без ограничение,
- JAM: действието никога не е предвидимо,
- AUT: правата, съответстващи на успешно външно удостоверяване, трябва да бъдат отворени (чрез командата EXTERNAL_AUTHENTICATION),
- PRO MS: командата трябва да бъде предадена със сума за криптографски контрол, като се използва защитен от неоторизиран достъп обмен на съобщения (виж допълнение 11),
- AUT и PRO MS (комбинирани).

Що се отнася до командите за обработка (UPDATE_BINARY и READ_BINARY), е възможно да се конфигурират следните условия за достъп на нивото на картата:

	UPDATE_BINARY	READ_BINARY
TJR	Да	Да
JAM	Да	Да
AUT	Да	Да
PRO MS	Да	Не
AUT и PRO MS	Да	Не

Условието за достъп PRO MS не е достъпно за командата READ_BINARY. Това означава, че наличието на сума за криптографски контрол за команда READ никога не е задължително. Въпреки това определянето на стойност '0C' на класа позволява да се използва командата READ_BINARY, като се използва защитен от неоторизиран достъп обмен на съобщения, съгласно описанието, дадено в параграф 3.6.2.

3.4. Криптиране

Когато е необходимо да се предпази конфиденциалността на данните, които трябва да бъдат извлечени от определен файл, той се маркира като „Криптиран“. Криптирането се извършва с помощта на защитен от неотризиран достъп обмен на съобщения (виж допълнение 11).

3.5. Общ преглед на командите и кодовете за грешка

Командите и структурата на файловете се определят от стандарт ISO/CEI 7816-4 и отговарят на неговите разпоредби.

TCS_313 Двойките команда/отговор UDPA, които следват по-долу, са описани подробно в този параграф:

Команда	INS
SELECT FILE	A4
READ BINARY	B0
UPDATE BINARY	D6
GET CHALLENGE	84
VERIFY	20
GET RESPONSE	C0
PERFORM SECURITY OPERATION: VERIFY CERTIFICATE COMPUTE DIGITAL SIGNATURE VERIFY DIGITAL SIGNATURE HASH	2A
INTERNAL AUTHENTICATE	88
EXTERNAL AUTHENTICATE	82
MANAGE SECURITY ENVIRONMENT: SETTING A KEY	22
PERFORM HASH OF FILE	2A

TCS_314 Думите за състояние ME1 и ME2 придружават всяко съобщение, съдържащо отговор. Те указват състоянието на обработване на съответната команда.

ME1	ME2	Значение
90	00	Нормална обработка
61	XX	Нормална обработка. XX = брой на наличните байтове на отговора
62	81	Обработка на предупреждение. XX = брой на наличните байтове на отговора
63	CX	Грешни IVT (NIP). Брояч на оставашите опити, осигуряван от 'X'
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 в сигурността: Грешна криптографска контролна сума (по време на обмен на защитени от неотризиран достъп съобщения) Грешен сертификат (по време на проверката на сертификата) Грешна криптограма (по време на външното удостоверяване) Грешен цифров подпис (по време на проверката на подписа)
67	00	Грешна дължина (грешни Lc или Le)
69	00	Забранена команда (няма възможност за отговор при T = 0)
69	82	Незадоволително състояние 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 информативни обекти при защитения от неотризиран достъп обмен на съобщения
69	88	Неправилни информативни обекти при защитения от неотризиран достъп обмен на съобщения
6A	82	Неоткриваем файл
6A	86	Грешни параметри P1-P2
6A	88	Неоткриваеми указани данни
6B	00	Грешни параметри (преместване извън елементарния файл)

ME1	ME2	Значение
6C	XX	Грешна дължина, ME2 указва точната дължина. Не се връща като отговор никаква зона за данни
6D	00	Несъвместим или неправилен код на команда
6E	00	Несъвместим клас
6F	00	Други грешки, свързани с контрола

3.6. Описание на командите

За дължителните команди, на които трябва да реагират тахографските карти, са описани подробно в този раздел.

Допълнение 11 (Общи механизми за сигурност) представлява източник на важна информация относно въпросните криптографски операции.

Всички команди са описани независимо от използвания протокол ($T = 0$ или $T = 1$). Байтовете UDPA CLA, INS, P1, P2, Lc и Le винаги са указани. Ако описаната команда може да не използва байт Lc или Le, свързаните с него клетки за дължина, стойност и описание остават празни.

TCS_315 Ако се изисква наличието на двата байта за дължина (Lc и Le), описаната команда трябва да бъде сегментирана на две части, ако PIF използва протокола $T = 0$: PIF изпраща описаната команда с $P3 = Lc + \text{данни}$, после изпраща команда GET_RESPONSE (виж точка 3.6.6) с $P3 = Le$.

TCS_316 Ако се изисква наличието на двата байта за дължина и ако $Le = 0$ (защитен от неотризиран достъп обмен на съобщения):

- при използване на протокола $T = 1$, картата трябва да отговори на $Le = 0$ като изпрати всички налични изходни данни,
- при използване на протокола $T = 0$, PIF трябва да изпрати първата команда с $P3 = Lc + \text{данни}$, картата трябва да отговори (на тази имплицитна $Le = 0$), като изпрати байтовете за състояние '61La', където La съответства на броя на наличните байтове за отговор. След това PIF трябва да генерира команда GET_RESPONSE с $P3 = La$, за да премине към четене на данните.

3.6.1. Select file (селектиране на файл)

Тази команда отговаря на стандарта ISO/CEI 7816-4, но се характеризира с ограничена употреба в сравнение с аналогичната команда, описана в този стандарт.

Използване на командата SELECT FILE:

- селектиране на специализиран файл на приложение (императивно селектиране по име),
- селектиране на елементарен файл, съответстващ на идентификатора на представения файл.

3.6.1.1. Селектиране по име (IDA)

Тази команда позволява селектирането на специализиран файл на приложение, записан на картата.

TCS_317 Тази команда се изпълнява от коя да е точка на структурата на файловете (след RAR или във всеки един момент).

TCS_318 Селектирането на определено приложение инициализира отново активната среда, свързана със защитата от неотризиран достъп. След като се е извършило селектирането на приложението, повече не се селектира никакъв активен публичен ключ и ключът на предишната сесия престава да бъде достъпен за защитения от неотризиран достъп обмен на съобщения. Условието за достъп AUT също така се деактивира.

TCS_319 Командно съобщение

Байт	Дължина	Стойност	Описание
CLA	1	'00h'	
INS	1	'A4h'	
P1	1	'04h'	Селектиране по име (IDA)
P2	1	'0Ch'	Не е предвиден никакъв отговор
Lc	1	'NNh'	Брой байтове, изпратени на картата (дължина на IDA): '06h' за тахографското приложение
#6-#(5+NN)	NN	'XX..XXh'	IDA 'FF 54 41 43 48 4F' за тахографското приложение

Системата не очаква отговор на командата SELECT FILE (липсвашо Le при T = 1 или не се изисква отговор при T = 0).

TCS_320 Отвѣтно съобщение (не се изисква отговор)

Байт	Дължина	Стойност	Описание
ME	2	'XXXXh'	Думи за състояние (ME1, ME2)

- ако командата се извърши успешно, картата връща състоянието '9000',
- ако софтуерът не успее да намери приложението, съответстващо на IDA, той връща следното състояние на обработка: '6A82',
- при T = 1 наличието на байта Le предизвиква връщането на състоянието '6700',
- при T = 0 изискването за отговор след получаването на командата SELECT FILE води до връщането на състоянието '6900',
- ако селектираното приложение се смята за повредено (открита е грешка в целостта на атрибутите на файла), софтуерът връща състояние на обработка '6400' или '6581'.

3.6.1.2. Селектиране на елементарен файл с помощта на неговия файлов идентификатор

TCS_321 Командно съобщение

Байт	Дължина	Стойност	Описание
CLA	1	'00h'	
INS	1	'A4h'	
P1	1	'02h'	Селектиране на елементарен файл, който зависи от активния специализиран файл
P2	1	'0Ch'	Не е предвиден никакъв отговор
Lc	1	'02h'	Брой байтове, изпратени на картата
#6-#7	2	'XXXXh'	Файлов идентификатор

Системата не очаква отговор на командата SELECT FILE (липсвашо Le при T = 1 или не се изисква отговор при T = 0).

TCS_322 Отвѣтно съобщение (не се изисква отговор)

Байт	Дължина	Стойност	Описание
ME 2	2	'XXXXh'	Думи за състояние (ME1, ME2)

- ако командата се извърши успешно, картата връща състоянието '9000',
- ако софтуерът не успее да намери файла, съответстващ на файловия идентификатор, той връща следното състояние на обработка: '6A82',
- при T = 1 наличието на байта Le предизвиква връщането на състоянието '6700',
- при T = 0 изискването за отговор след получаването на командата SELECT FILE води до връщането на състоянието '6900',
- ако селектираният файл се смята за повреден (открита е грешка в целостта на атрибутите на файла), софтуерът връща състояние на обработка '6400' или '6581'.

3.6.2. Read Binary (четене на данни)

Тази команда отговаря на стандарта ISO/CEI 7816-4, но се характеризира с ограничена употреба в сравнение с аналогичната команда, описана в този стандарт.

Командата READ BINARY позволява извличането на данните, записани във файл, който не зависи от използвания код.

Отговорът на картата се състои във връщането на извлечените данни, като те се включват при необходимост в структура на защитен от неотризиран достъп обмен на съобщения.

TCS_323 Тази команда може да бъде изпълнена единствено при условие, че нивото на сигурността удовлетворява изискванията за сигурността на елементарния файл и за функцията READ (четене, извличане на данни).

3.6.2.1. Команда без защитен от неоторизиран достъп обмен на съобщенията

Тази команда позволява на PIF извличането на данните от селектирания елементарен файл, без да използва защитен от неоторизиран достъп обмен на съобщенията.

TCS_324 Тази команда не позволява извличането на данни от файл, който има статут на „Кодиран“.

TCS_325 Командно съобщение

Байт	Дължина	Стойност	Описание
CLA	1	'00h'	Не се използва никакъв защитен от неоторизиран достъп обмен на съобщения
INS	1	'B0h'	
P1	1	'XXh'	Отместване в байтове, считано от началото на файла: най-значещият байт (най-левият байт)
P2	1	'XXh'	Отместване в байтове, считано от началото на файла: байтът с най-малко значение (най-десният байт)
Le	1	'XXh'	Очаквана дължина на данните. Брой на байтовете, които трябва да се извлекат.

Забележка: бит 8 на байт P1 трябва да бъде равен на нула.

TCS_326 Отвечно съобщение

Байт	Дължина	Стойност	Описание
#1-#X	X	'XX..XXh'	Извлечени данни
SW	2	'XXXXh'	Думи за състояние (ME1, ME2)

- ако командата се извърши успешно, картата връща състоянието '9000',
- ако софтуерът не успее да селектира никакъв елементарен файл, той връща следното състояние на обработка: '6986',
- ако условията за достъп до селектирания файл не са изпълнени, изпълнението на командата се прекъсва от състоянието '6982',
- ако отместването не е съвместимо с размера на елементарния файл (отместване > размера на елементарния файл), софтуерът връща следното състояние на обработка: '6B00',
- ако обемът на данните, които ще се извличат, не е съвместим с размера на елементарния файл (отместване + Le > размера на елементарния файл), софтуерът връща следното състояние на обработка: '6700' или '6Cxx', където 'xx' указва точната дължина,
- ако е открита грешка в целостта на атрибутите на файла, картата счита файла за повреден и невъзстановим и софтуерът връща състояние на обработка '6400' или '6581',
- ако е открита грешка в целостта на записаните данни, картата връща поисканите данни и софтуерът връща състояние на обработка '6281'.

3.6.2.2. Команда със защитен от неоторизиран достъп обмен на съобщенията

Тази команда позволява на периферното устройство за четене на карти да извлече данни от селектирания елементарен файл, като използва защитен от неоторизиран достъп обмен на съобщенията, за да се увери в целостта на получените данни и да предпази тяхната конфиденциалност, при положение че разглежданият елементарен файл има статут на „Криптиран“.

TCS_327 Командно съобщение

Байт	Дължина	Стойност	Описание
CLA	1	'0Ch'	Изисква се защитен от неоторизиран достъп обмен на съобщения
INS	1	'B0h'	INS
P1	1	'XXh'	P1 (отместване в офсет-байтове, считано от началото на файла): най-значещият байт (най-левият байт)
P2	1	'XXh'	P2 (отместване в офсет-байтове, считано от началото на файла): байтът с най-малко значение (най-десният байт)
Lc	1	'09h'	Дължина на входящите данни за защитения от неоторизиран достъп обмен на съобщения
#6	1	'97h'	T _{LE} : таг, указващ спецификацията на очакваната дължина
#7	1	'01h'	L _{LE} : дължина на очакваната дължина
#8	1	'NNh'	Специфициране на очакваната дължина (първоначална Le): брой на байтовете, които трябва да се извлекат.

Байт	Дължина	Стойност	Описание
#9	1	'8Eh'	T _{CC} : таг, указващ сумата за криптографски контрол
#10	1	'04h'	L _{CC} : дължина на следващата сума за криптографски контрол
#11-#14	4	'XX..XXh'	Сума за криптографски контрол (4-те най-значещи байта)
Le	1	'00h'	Съгласно разпоредбите на стандарт ISO/CEI 7816-4

TCS_328 Отвечно съобщение, ако елементарният файл няма статут на „кодиран“ и ако входящият формат на защитения от неототоризиран достъп обмен на съобщения е коректен:

Байт	Дължина	Стойност	Описание
#1	1	'81h'	T _{PV} : таг, указващ стойността на обикновените данни
#2	L	'NNh' или '81 NNh'	L _{PV} : дължина на върнатите данни (първоначална Le) L съответства на 2 байта ако L _{PV} > 127 байта
#(2+L)-#(1+L+NN)	NN	'XX..XXh'	Стойност на обикновените данни
#(2+L+NN)	1	'8Eh'	T _{CC} : таг, указващ сума за криптографски контрол
#(3+L+NN)	1	'04h'	L _{CC} : дължина на следващата сума за криптографски контрол
#(4+L+NN)-#(7+L+NN)	4	'XX..XXh'	Сума за криптографски контрол (4-те най-значещи байта)
ME	2	'XXXXh'	Думи за състояние (ME1, ME2)

TCS_329 Отвечно съобщение, ако елементарният файл има статут на „криптиран“ и ако входящият формат на защитения от неототоризиран достъп обмен на съобщения е коректен:

Байт	Дължина	Стойност	Описание
#1	1	'87h'	T _{PI CG} : таг, указващ кодираните данни (криптограма)
#2	L	'MMh' или '81 MMh'	L _{PI CG} : дължина на върнатите кодирани данни (различни от първоначалната Le на командата поради запълване) L съответства на 2 байта ако L _{PI CG} > 127 байта
#(2+L)-#(1+L+MM)	MM	01XX..XXh'	Кодирани данни: криптограма и индикатор за запълване
#(2+L+MM)	1	'8Eh'	T _{CC} : таг, указващ сума за криптографски контрол
#(3+L+MM)	1	'04h'	L _{CC} : дължина на следващата сума за криптографски контрол
#(4+L+MM)-#(7+L+MM)	4	'XX..XXh'	Сума за криптографски контрол (4-те най-значещи байта)
ME	2	'XXXXh'	Думи за състояние (ME1, ME2)

Върнатите кодирани данни съдържат първи байт, който указва използвания начин на запълване. За тахографското приложение индикаторът на запълване приема винаги стойност '01h', която указва, че използваният начин на запълване е този, който е уточнен в стандарт ISO/CEI 7816-4 (един байт, имащ стойност '80h', последван от серия от нулеви байтове: стандарт ISO/CEI 9797 метод 1).

Описаните по-горе структури на отвечно съобщение позволяват връщането на „нормални“ състояния на обработка, уточнени за командата READ BINARY без използване на защитен от неототоризиран достъп обмен на съобщения (виж параграф 3.6.2.1).

От друга страна, могат да се проявят някои грешки, свързани със защитения от неототоризиран достъп обмен на съобщения. В този случай софтуерът само връща съответното състояние на обработка, без да въвежда някаква структура на защитен от неототоризиран достъп обмен на съобщения:

TCS_330 Отвечно съобщение, ако входящият формат на защитения от неототоризиран достъп обмен на съобщения е некоректен:

Байт	Дължина	Стойност	Описание
ME	2	'XXXXh'	Думи за състояние (ME1, ME2)

— ако не е достъпен никакъв ключ на активна сесия, софтуерът връща състоянието на обработка '6A88'. Това събитие се извършва, ако ключът на сесията все още не е генериран или ако валидността му е изтекла (в този случай PIF трябва да извърши отново съответния процес на взаимно удостоверяване за определяне на нов ключ на сесия),

— ако някои очаквани информативни обекти (както бе уточнено по-горе) липсват в структурата на защитения от неототоризиран достъп обмен на съобщения, софтуерът връща състояние на обработка '6987': тази грешка се проявява, ако липсва някой очакван таг или ако тялото на командата не е конструирано правилно,

- ако някои информативни обекти са некоректни, софтуерът връща състоянието на обработка '6988': тази грешка се проявява, ако всички необходими тагове са налични, но някои дължини се различават от очакваните,
- ако проверката на сумата за криптографски контрол е неуспешна, софтуерът връща състоянието на обработка '6688'.

3.6.3. Update Binary (актуализиране на данните)

Тази команда отговаря на стандарта ISO/CEI 7816-4, но се характеризира с ограничена употреба в сравнение с аналогичната команда, описана в този стандарт.

Командното съобщение UPDATE BINARY започва актуализирането (изтриване + записване) на битовете, които вече присъстват в определен елементарен файл, с битовете, които съдържа командата UDPA.

TCS_331 Тази команда може да бъде изпълнена единствено при условие, че нивото на сигурността удовлетворява изискванията за сигурността на елементарния файл и за функцията UPDATE (ако контролът на достъпа на функцията UPDATE съдържа PRO MS, е необходимо към тази команда да се добави структура на защитен от неототоризиран достъп обмен на съобщения).

3.6.3.1. Команда без защитен от неототоризиран достъп обмен на съобщения

Тази команда позволява на PIF да запише данните в селектирания елементарен файл, без картата да проверява целостта на получените данни. Този директен режим е разрешен единствено при условие че съответният файл не е маркиран като „криптиран“.

TCS_332 Командно съобщение

Байт	Дължина	Стойност	Описание
CLA	1	'00h'	Не се изисква защитен от неототоризиран достъп обмен на съобщения
INS	1	'D6h'	Отместване в байтове, считано от началото на файла: най-значещият байт (най-левият байт)
P1	1	'XXh'	
P2	1	'XXh'	Отместване в байтове, считано от началото на файла: байтът с най-малко значение (най-десният байт)
Lc	1	'NNh'	Дължина Lc на данните, която трябва да се актуализира. Брой на байтовете, които трябва да се запишат
#6-#(5+NN)	NN	'XX..XXh'	Данни, които трябва да се запишат

Забележка: бит 8 на байт P1 трябва да бъде равен на нула.

TCS_333 Отвечно съобщение

Байт	Дължина	Стойност	Описание
ME	2	'XXXXh'	Думи за състояние (ME1, ME2)

- ако командата се извърши успешно, картата връща състоянието на обработка '9000',
- ако софтуерът не успее да селектира никакъв елементарен файл, той връща следното състояние на обработка: '6986',
- ако условията за достъп до селектирания файл не са изпълнени, изпълнението на командата се прекъсва от състоянието '6982',
- ако отместването не е съвместимо с размера на елементарния файл (отместване > размера на елементарния файл), софтуерът връща следното състояние на обработка: '6B00',
- ако обемът на данните, които ще се записват, не е съвместим с размера на елементарния файл (отместване + Le > размера на елементарния файл), софтуерът връща следното състояние на обработка: '6700',
- ако е открита грешка в целостта на атрибутите на файла, картата счита файла за повреден и невъзстановим и софтуерът връща състояние на обработка '6400' или '6500',
- ако записването е невъзможно, софтуерът връща състояние на обработка '6581'.

3.6.3.2. Команда със защитен от неотризиран достъп обмен на съобщенията

Тази команда позволява на PIF да запише данните в селектирания елементарен файл, без картата да проверява целостта на получените данни. Тъй като няма изискване за конфиденциалност, данните не са кодирани.

TCS_334 Командно съобщение

Байт	Дължина	Стойност	Описание
CLA	1	'0Ch'	Изисква се защитен от неотризиран достъп обмен на съобщения
INS	1	'D6h'	INS
P1	1	'XXh'	Отместване в байтове, считано от началото на файла: най-значещият байт (най-левият байт)
P2	1	'XXh'	Отместване в байтове, считано от началото на файла: байтът с най-малко значение (най-десният байт)
Lc	1	'XXh'	Дължина на зоната за данни, защитена от неотризиран достъп
#6	1	'81h'	T _{PV} : таг, указващ стойността на обикновените данни
#7	L	'NNh' или '81 NNh'	L _{PV} : дължина на предадените данни L съответства на 2 байта ако L _{PV} > 127 байта
#(7+L)-#(6+L+NN)	NN	'XX..XXh'	Дължина на обикновените данни (данни, които трябва да се запишат)
#(7+L+NN)	1	'8Eh'	T _{CC} : таг, указващ сума за криптографски контрол
#(8+L+NN)	1	'04h'	L _{CC} : дължина на следващата сума за криптографски контрол
#(9+L+NN)-#(12+L+NN)	4	'XX..XXh'	Сума за криптографски контрол (4-те най-значещи байта)
Le	1	'00h'	Съгласно разпоредбите на стандарт ISO/CEI 7816-4

TCS_335 Отвечно съобщение, ако входящият формат на защитения от неотризиран достъп обмен на съобщения е коректен

Байт	Дължина	Стойност	Описание
#1	1	'99h'	T _{SW} : таг, указващ думите за състояние (които трябва да се предпазват от криптографския контрол)
#2	1	'02h'	L _{SW} : дължина на върнатите думи за състояние
#3-#4	2	'XXXXh'	Думи за състояние (ME1, ME2)
#5	1	'8Eh'	T _{CC} : таг, указващ сума за криптографски контрол
#6	1	'04h'	L _{CC} : дължина на следващата сума за криптографски контрол
#7-#10	4	'XX..XXh'	Сума за криптографски контрол (4-те най-значещи байта)
ME	2	'XXXXh'	Думи за състояние (ME1, ME2)

Описаната по-горе структура на отвечно съобщение позволява връщането на „нормални“ състояния на обработка, уточнени за командата UPDATE BINARY без използване на защитен от неотризиран достъп обмен на съобщения (виж параграф 3.6.3.1).

От друга страна, могат да се проявят някои грешки, свързани със защитения от неотризиран достъп обмен на съобщения. В този случай софтуерът само връща съответното състояние на обработка, без да въвежда никаква структура на защитен от неотризиран достъп обмен на съобщения:

TCS_336 Отвечно съобщение в случай на грешка, засягаща защитения от неотризиран достъп обмен на съобщения

Байт	Дължина	Стойност	Описание
ME	2	'XXXXh'	Думи за състояние (ME1, ME2)

- ако не е достъпен никакъв ключ на активна сесия, софтуерът връща състоянието на обработка '6A88',
- ако някои очаквани информативни обекти (както бе уточнено по-горе) липсват в структурата на защитения от неотризиран достъп обмен на съобщения, софтуерът връща състояние на обработка '6987': тази грешка се проявява, ако липсва някой очакван таг или ако тялото на командата не е конструирано правилно,
- ако някои информативни обекти са некоректни, софтуерът връща състояние на обработка '6988': тази грешка се проявява, ако всички необходими тагове са налични, но някои дължини се различават от очакваните,
- ако проверката на сумата за криптографски контрол е неуспешна, софтуерът връща състоянието на обработка '6688'.

3.6.4. *Get Challenge (получаване на искане за достъп)*

Тази команда отговаря на стандарта ISO/CEI 7816-4, но се характеризира с ограничена употреба в сравнение с аналогичната команда, описана в този стандарт.

Командата GET CHALLENGE иска от картата да изпрати искане за достъп, за да го използва в рамките на процедура, свързана със сигурността и съдържаща изпращането на криптограма или на кодирани данни на картата.

TCS_337 Искането за достъп, изпратено от картата, важи единствено за следващата команда (която прибегва до използването на искане за достъп), изпратена на картата.

TCS_338 Командно съобщение

Байт	Дължина	Стойност	Описание
CLA	1	'00h'	CLA
INS	1	'84h'	INS
P1	1	'00h'	P1
P2	1	'00h'	P2
Le	1	'08h'	Le (дължина на очакваното искане за достъп)

TCS_339 Ответно съобщение

Байт	Дължина	Стойност	Описание
#1-#8	8	'XX..XXh'	Искане за достъп
ME	2	'XXXXh'	Думи за състояние (ME1, ME2)

- ако командата се извърши успешно, картата връща състоянието '9000',
- ако байтът Le се различава от '08h', софтуерът връща следното състояние на обработка: '6700',
- ако параметрите P1-P2 са некоректни, софтуерът връща следното състояние на обработка: '6A86'.

3.6.5. *Verify (контрол)*

Тази команда отговаря на стандарта ISO/CEI 7816-4, но се характеризира с ограничена употреба в сравнение с аналогичната команда, описана в този стандарт.

Командата VERIFY стартира на нивото на картата сравняването между изпратените данни IVT (NIP) и референтните данни IVT, записани в паметта на картата.

Забележка: Периферното устройство за четене на карти трябва да допълва отлясно със серия от байтове 'FFh' въведения от потребителя PIN, докато този номер достигне дължина от 8 байта.

TCS_340 Ако командата се извърши успешно, правата относно представянето на данните IVT се отварят и броячът на оставащите опити за IVT се реинициализира.

TCS_341 Всеки неуспех при предприетото сравняване води до записването на данните на картата с цел да се ограничи броят на по-късните опити за използване на референтните данни IVT.

TCS_342 Командно съобщение

Байт	Дължина	Стойност	Описание
CLA	1	'00h'	CLA
INS	1	'20h'	INS
P1	1	'00h'	P1
P2	1	'00h'	P2 (проверените IVT са познати по подразбиране)
Lc	1	'08h'	Дължина на предадения код IVT
#6-#13	8	'XX..XXh'	IVT

TCS_343 Отвечно съобщение

Байт	Дължина	Стойност	Описание
ME	2	'XXXXh'	Думи за състояние (ME1, ME2)

- ако командата се извърши успешно, картата връща състоянието '9000',
- ако референтните IVT са неоткриваеми, софтуерът връща състоянието на обработка '6A88',
- ако IVT са блокирани (броячът на оставащите опити за IVT показва нула), софтуерът връща състоянието на обработка '6983'. След като веднъж се окажат в това състояние, IVT никога повече няма да могат да бъдат представени успешно,
- ако сравняването не завърши успешно, броячът на оставащите опити се намалява с една единица и софтуерът връща състоянието '63CX' (X > 0 и X съответства на брояча на оставащите опити за IVT. Ако X = 'F', броячът на опитите за IVT показва число, по-голямо от 'F'),
- ако референтните IVT са приети за повредени, софтуерът връща състоянието на обработка '6400' или '6581'.

3.6.6. **Get Response (получаване на отговор)**

Тази команда отговаря на стандарт ISO/CEI 7816-4.

Тази команда (достъпна и необходима изключително за протокола T = 0) позволява осигуряването на предаването между картата и периферното интерфейсно устройство на приготвените данни (случай, при който двата байта Lc и Le са включени в определена команда).

Командата GET_RESPONSE трябва да бъде изпратена непосредствено след командата за приготвяне на данните, в противен случай загубата на тази данни е неизбежна. След изпълнението на командата GET_RESPONSE (освен ако се прояви грешката '61xx' или '6Cxx', виж по-долу), предварително приготвените данни престават да бъдат достъпни.

TCS_344 Командно съобщение

Байт	Дължина	Стойност	Описание
CLA	1	'00h'	
INS	1	'C0h'	
P1	1	'00h'	
P2	1	'00h'	
Le	1	'XXh'	Брой на очакваните байтове

TCS_345 Отвечно съобщение

Байт	Дължина	Стойност	Описание
#1-#X	X	'XX..XXh'	Данни
ME	2	'XXXXh'	Думи за състояние (ME1, ME2)

- ако командата се извърши успешно, картата връща състояние на обработка '9000',
- ако картата не е приготвила никакви данни, тя връща състояние на обработка '6900' или '6F00',
- ако байтът Le надвишава броя на достъпните байтове или ако този байт е нулев, софтуерът връща следното състояние на обработка — '6Cxx', като символите 'xx' указват точния брой на достъпните байтове. В този случай приготвените данни остават достъпни за изпълнението по-късно на команда GET_RESPONSE,
- ако байтът Le представлява ненулева стойност, която е по-ниска от броя на достъпните байтове, картата изпраща нормално исканите данни и връща състояние на обработка '61xx', в което 'xx' указва броя на допълнителните байтове, които все още са достъпни за изпълнението по-късно на команда GET_RESPONSE,
- ако командата не се поддържа (протокол T = 1), картата връща състояние на обработка '6D00'.

3.6.7. **PSO (Protocol Supporting Organization): Verify Certificate (контрол на валидността)**

Тази команда отговаря на стандарта ISO/CEI 7816-8, но се характеризира с ограничена употреба в сравнение с аналогичната команда, описана в този стандарт.

Картата използва командата VERIFY CERTIFICATE, за да получи публичен ключ, идващ от публичното пространство, и за проверка на неговата валидност.

TCS_346 Когато командата VERIFY CERTIFICATE завърши успешно, съответният публичен ключ се запазва в средата, свързана със защитата от неототоризиран достъп, с цел по-късното му използване. Този ключ трябва да бъде специално конфигуриран, за да бъде използван в рамките на командите, имащи отношение към сигурността (INTERNAL AUTHENTICATE, EXTERNAL AUTHENTICATE или VERIFY CERTIFICATE), чрез командата MSE (виж точка 3.6.10), като се използва неговият идентификатор на ключа.

TCS_347 При всички положения командата VERIFY CERTIFICATE използва предварително избрания чрез командата MSE публичен ключ, за да отвори определен сертификат. Това трябва да бъде публичен ключ на определена държава-членка или на Европа.

TCS_348 Командно съобщение

Байт	Дължина	Стойност	Описание
CLA	1	'00h'	CLA
INS	1	'2Ah'	Извършване на операция, свързана със защитата от неототоризиран достъп
P1	1	'00h'	P1
P2	1	'AEh'	P2: кодирани данни, които не са BER-TLV (конкатенация на елементи на информация)
Lc	1	'CEh'	Lc: Дължина на сертификата, 194 байта
#6-#199	194	'XX..XXh'	Сертификат: конкатенация на елементи на информация (съгласно описанието, дадено в допълнение 11)

TCS_349 Ответно съобщение

Байт	Дължина	Стойност	Описание
ME	2	'XXXXh'	Думи за състояние (ME1, ME2)

- ако командата се извърши успешно, картата връща състоянието '9000',
- ако проверката на сертификата е неуспешна, софтуерът връща състоянието на обработка '6688'. Процесът на проверка и на отваряне на сертификата е описан подробно в допълнение 11,
- ако не е достъпен никакъв ключ в средата, свързана със защитата от неототоризиран достъп, софтуерът връща състоянието на обработка '6A88',
- ако избраният публичен ключ (който също така се използва за отваряне на сертификата) се приема за повреден, софтуерът връща състоянието на обработка '6400' или '6581',
- ако избраният публичен ключ (който също така се използва за отваряне на сертификата) притежава CHA.LSB (CertificateHolderAuthorisation.equipmentType), различен от '00' (тоест, който не принадлежи на държава-членка или на Европа), софтуерът връща състоянието на обработка '6985'.

3.6.8. *Internal Authenticate (вътрешно удостоверяване)*

Тази команда отговаря на стандарт ISO/CEI 7816-4.

Командата INTERNAL AUTHENTICATE позволява на периферното устройство за четене на карти (PIF) да удостовери картата.

Процесът на удостоверяване е описан подробно в допълнение 11. Той обхваща следните инструкции:

TCS_350 Командата INTERNAL AUTHENTICATE си служи с частния ключ на картата (избран по подразбиране), за да подпише данните от удостоверяването, K1 (първият елемент, указващ съставянето на ключовете на сесията) и RND1 включително, и също така използва избрания публичен ключ (посредством последната команда MSE), за да кодира подписа и да състави управляващия удостоверяването маркер (за повече подробности виж допълнение 11).

TCS_351 Командно съобщение

Байт	Дължина	Стойност	Описание
CLA	1	'00h'	CLA
INS	1	'88h'	INS
P1	1	'00h'	P1
P2	1	'00h'	P2
Lc	1	'10h'	Дължина на данните, изпратени на картата
#6-#13	8	'XX..XXh'	Искане за достъп, използвано за удостоверяване на картата
#14-#21	8	'XX..XXh'	UV.CTC (виж допълнение 11)
Le	1	'80h'	Дължина на очакваните данни, идващи от картата

TCS_352 Отвечно съобщение

Байт	Дължина	Стойност	Описание
#1-#128	128	'XX..XXh'	Маркер, управляващ удостоверяването на картата (виж допълнение 11)
ME	2	'XXXXh'	Думи за състояние (ME1, ME2)

- ако командата се извърши успешно, картата връща състоянието на обработка '9000',
- ако не е достъпен никакъв ключ в средата, свързана със защитата от неоторизиран достъп, софтуерът връща състоянието на обработка '6A88',
- ако не е достъпен никакъв частен ключ в средата, свързана със защитата от неоторизиран достъп, софтуерът връща състоянието на обработка '6A88',
- ако UV.CTC не съответства на идентификатора на активния публичен ключ, софтуерът връща състоянието на обработка '6A88',
- ако избраният частен ключ се приема за повреден, софтуерът връща състоянието на обработка '6400' или '6581'.

TCS_353 Ако командата INTERNAL_AUTHENTICATE завърши успешно, активният ключ на сесията при положение, че той съществува, се изтрива и престава да бъде достъпен. За да се разполага с нов ключ на сесия, е необходимо да се изпълни успешно командата EXTERNAL_AUTHENTICATE.

3.6.9. External Authenticate (външно удостоверяване)

Тази команда отговаря на стандарт ISO/CEI 7816-4.

Командата EXTERNAL AUTHENTICATE позволява на картата да удостовери периферното устройство за четене на карти.

Процесът на удостоверяване е описан подробно в допълнение 11. Той обхваща следните инструкции:

TCS_354 Необходимо е командата GET CHALLENGE да предшества непосредствено командата EXTERNAL_AUTHENTICATE. Картата изпраща искане за достъп към публичното пространство (RND3).

TCS_355 Функцията за проверка на криптограмата използва искането за достъп RND3 (изпратено от картата), частния ключ на картата (избран по подразбиране) и предварително избрания чрез командата MSE публичен ключ.

TCS_356 Картата проверява криптограмата и ако тя е правилна, условието за достъп AUT се отваря.

TCS_357 Входящата криптограма въвежда втория елемент K2, указващ съставянето на ключовете на сесията.

TCS_358 Командно съобщение

Байт	Дължина	Стойност	Описание
CLA	1	'00h'	CLA
INS	1	'82h'	INS
P1	1	'00h'	P1
P2	1	'00h'	P2 (публичният ключ, който трябва да се използва, е познат по подразбиране; той е избран предварително чрез командата MSE)
Lc	1	'80h'	Lc (дължина на данните, изпратени на картата)
#6-#133	128	'XX..XXh'	Криптограма (виж допълнение 11)

TCS_359 Отвечно съобщение

Байт	Дължина	Стойност	Описание
ME	2	'XXXXh'	Думи за състояние (ME1, ME2)

- ако командата се извърши успешно, картата връща състоянието на обработка '9000',
- ако не е достъпен никакъв ключ в средата, свързана със защитата от неоторизиран достъп, софтуерът връща състоянието на обработка '6A88',
- ако АТС на избрания публичен С12 не съответства на конкатенацията на IDA на тахографското приложение и на определен тип блок, софтуерът връща състоянието на обработка '6F00' (виж допълнение 11),
- ако не е достъпен никакъв частен ключ в средата, свързана със защитата от неоторизиран достъп, софтуерът връща състоянието на обработка '6A88',
- ако проверката на криптограмата е неуспешна, софтуерът връща състоянието на обработка '6688',
- ако командата не е непосредствено предшествана от командата GET CHALLENGE, софтуерът връща състоянието на обработка '6985',
- ако избраният частен ключ се приема за повреден, софтуерът връща състоянието на обработка '6400' или '6581'.

TCS_360 Ако командата EXTERNAL AUTHENTICATE завърши успешно и ако първата част на ключа на сесията е достъпна след успешното завършване на наскоро изпълнената команда INTERNAL AUTHENTICATE, ключът на сесията е готов за изпълняването на бъдещи команди, използващи защитения от неоторизиран достъп обмен на съобщения.

TCS_361 Ако първата част на ключа на сесията не е достъпна въпреки изпълнението на командата INTERNAL AUTHENTICATE, втората част на този ключ на сесия, изпратена от PIF, няма да бъде записана в паметта на картата. Този механизъм позволява да се гарантира, че протичането на процеса по взаимно удостоверяване спазва реда, уточнен в допълнение 11.

3.6.10. *Manage Security Environment (управление на средата, свързана със защитата от неоторизиран достъп)*

Тази команда позволява определянето на публичен ключ за целите на удостоверяването.

Тази команда отговаря на стандарт ISO/CEI 7816-8. Нейната употреба е ограничена съгласно въпросния стандарт.

TCS_362 Ключът, указан в зоната за данни MSE, се прилага към всички файлове от главния файл на тахографското приложение.

TCS_363 Ключът, указан в зоната за данни MSE, остава активен публичен ключ до следващата правилна команда MSE.

TCS_364 Ако упоменатият ключ не е (все още) достъпен в паметта на картата, средата, свързана със защитата от неоторизиран достъп, остава непроменена.

TCS_365 Командно съобщение

Байт	Дължина	Стойност	Описание
CLA	1	'00h'	CLA
INS	1	'22h'	INS
P1	1	'C1h'	P1: упоменат ключ, който е валиден за всички криптографски операции
P2	1	'B6h'	P2 (упоменати данни, отнасящи се до цифровия подпис)
Lc	1	'0Ah'	Lc дължина на последващата зона за данни
#6	1	'83h'	Tag, указващ публичен ключ в случай на асиметрия
#7	1	'08h'	Дължина на препратката (идентификатор на ключа)
#8-#15	08h	'XX..XXh'	Идентификатор на ключ съгласно разпоредбите на допълнение 11

TCS_366 Отвѣтно съобщение

Байт	Дължина	Стойност	Описание
ME	2	'XXXXh'	Думи за състояние (ME1, ME2)

- ако командата се извърши успешно, картата връща състоянието на обработка '9000',
- ако упоменатият ключ не е достъпен в паметта на картата, софтуерът връща състоянието на обработка '6A88',
- ако някои очаквани информативни обекти липсват в структурата на защитения от неотризиран достъп обмен на съобщения, софтуерът връща състояние на обработка '6987'. Това събитие може да се прояви, ако липсва тагът '83h',
- ако някои информативни обекти са некоректни, софтуерът връща състояние на обработка '6988': Това събитие може да се прояви, ако дължината на идентификатора на ключа не съответства на '08h',
- ако избраният ключ се приема за повреден, софтуерът връща състоянието на обработка '6400' или '6581'.

3.6.11. *PSO: Hash (сегментиране)*

Тази команда позволява прехвърлянето към картата на резултата от изчислението на сегментирането, на което някои данни могат да бъдат подложени. Тази команда се използва по време на проверката на цифровите подписи. Стойността на сегментирането се записва в програмируема електронно постоянна памет (EEPROM) с цел използването ѝ от следващата команда за проверка на цифровите подписи.

Тази команда отговаря на стандарт ISO/CEI 7816-8. Нейната употреба е ограничена съгласно въпросния стандарт.

TCS_367 Командно съобщение

Байт	Дължина	Стойност	Описание
CLA	1	'00h'	CLA
INS	1	'2Ah'	Извършване на операция, свързана със сигурността
P1	1	'90h'	Връщане на код за сегментиране
P2	1	'A0h'	Таг: зона за данни, съдържаща съответните DO за сегментиране
Lc	1	'16h'	Дължина Lc на последващата зона за данни
#6	1	'90h'	Таг, указващ кода за сегментиране
#7	1	'14h'	Дължина на кода за сегментиране
#8-#27	20	'XX.XXh'	Код за сегментиране

TCS_368 Отвѣтно съобщение

Байт	Дължина	Стойност	Описание
ME	2	'XXXXh'	Думи за състояние (ME1, ME2)

- ако командата се извърши успешно, картата връща състоянието на обработка '9000',
- ако някои очаквани информативни обекти липсват, софтуерът връща състояние на обработка '6987'. Това събитие може да се прояви, ако един от таговете '90h' липсва,
- ако някои информативни обекти са некоректни, софтуерът връща състояние на обработка '6988'. Тази грешка може да се прояви, ако необходимият таг е наличен, но неговата дължина се различава от '14h'.

3.6.12. *Perform Hash of File (сегментиране на файл)*

Тази команда не отговаря на стандарт ISO/CEI 7816-8. Вследствие на това байтът CLA на тази команда указва изключителната употреба на командата PERFORM SECURITY OPERATION/HASH.

TCS_369 Командата PERFORM HASH OF FILE се използва за сегментиране на зоната за данни на селектирания елементарен файл, който не зависи от използвания код.

TCS_370 Резултатът от операцията по сегментиране се записва в паметта на картата. След това нейната употреба ще позволи да се получи цифров подпис за файла, като се използва командата PSO: COMPUTE_DIGITAL_SIGNATURE. Този резултат остава достъпен за командата COMPUTE DIGITAL SIGNATURE до успешното изпълнение на следваща команда PERFORM HASH OF FILE.

TCS_371 Командно съобщение

Байт	Дължина	Стойност	Описание
CLA	1	'80h'	CLA
INS	1	'2Ah'	Извършване на операция, свързана със сигурността
P1	1	'90h'	Таг: сегментиране
P2	1	'00h'	P2: сегментиране на данните, записани в селектирания независим от използвания код файл

TCS_372 Ответно съобщение

Байт	Дължина	Стойност	Описание
ME	2	'XXXXh'	Думи за състояние (ME1, ME2)

- ако командата се извърши успешно, картата връща състоянието на обработка '9000',
- ако не е селектирано никакво приложение, софтуерът връща състоянието на обработка '6985',
- ако селектираният елементарен файл се смята за повреден (открита е грешка в целостта на атрибутите на файла или в съхранените в него данни), софтуерът връща състояние на обработка '6400' или '6581',
- ако селектираният файл не е файл, който не зависи от използвания код, софтуерът връща състоянието на обработка '6986'.

3.6.13. PSO: Compute Digital Signature (изчисляване на цифровия подпис)

Тази команда позволява да се изчисли цифровия подпис на предварително изчисления код за сегментиране (виж командата PERFORM HASH OF FILE, точка 3.6.12).

Тази команда отговаря на стандарт ISO/CEI 7816-8. Нейната употреба е ограничена съгласно въпросния стандарт.

TCS_373 Частният ключ на картата позволява изчисляването на цифровия подпис. На картата този ключ ѝ е известен по подразбиране.

TCS_374 Картата изпълнява цифров подпис, като прибегва до метода на запълване съгласно стандарт PKCS1 (за повече подробности може да се направи справка в допълнение 11).

TCS_375 Командно съобщение

Байт	Дължина	Стойност	Описание
CLA	1	'00h'	CLA
INS	1	'2Ah'	Извършване на операция, свързана със сигурността
P1	1	'9Eh'	Цифров подпис, който трябва да се върне
P2	1	'9Ah'	Таг: зона за данни, съдържаща данните, които трябва да се подпишат. Тъй като не е включена никаква зона за данни, се приема, че данните вече са налични в картата (сегментиране на файла)
Le	1	'80h'	Дължина на очаквания подпис

TCS_376 Ответно съобщение

Байт	Дължина	Стойност	Описание
#1-#128	128	'XX..XXh'	Подпис на предварително изчисленото сегментиране
ME	2	'XXXXh'	Думи за състояние (ME1, ME2)

- Ако командата се извърши успешно, картата връща състоянието на обработка '9000',
- ако избраният по подразбиране частен ключ се приема за повреден, софтуерът връща състоянието на обработка '6400' или '6581'.

3.6.14. *Verify Digital Signature (контрол на цифровия подпис)*

Тази команда позволява да се провери цифровият подпис, въведен като входни данни съгласно PKCS1, на съобщение, чието сегментиране е известно на картата. Алгоритъмът на подписа е известен по подразбиране на картата.

Тази команда отговаря на стандарт ISO/CEI 7816-8. Нейната употреба е ограничена съгласно въпросния стандарт.

TCS_377 Командата VERIFY DIGITAL SIGNATURE си служи винаги с публичния ключ, избран посредством предишната команда MANAGE SECURITY ENVIRONMENT и с предишния коп за сегментиране, въведен чрез командата PSO: HASH.

TCS_378 Командно съобщение

Байт	Дължина	Стойност	Описание
CLA	1	'00h'	CLA
INS	1	'2Ah'	Извършване на операция, свързана със защитата от неотризиран достъп
P1	1	'00h'	Таг: зона за данни, съдържаща съответните DO за проверката
P2	1	'A8h'	
Lc	1	'83h'	Дължина Lc на последващата зона за данни
#28	1	'9Eh'	Таг, указващ цифров подпис
#29-#30	2	'8180h'	Дължина на цифровия подпис (128 байта, кодирани съгласно стандарт ISO/CEI 7816-6)
#31-#158	128	'XX..XXh'	Съдържание на цифровия подпис

TCS_379 Ответно съобщение

Байт	Дължина	Стойност	Описание
ME	2	'XXXXh'	Думи за състояние (ME1, ME2)

- ако командата се извърши успешно, картата връща състоянието на обработка '9000',
- ако проверката на подписа е неуспешна, софтуерът връща състоянието на обработка '6688'. Процесът на проверка е описан подробно в допълнение 11,
- ако не е избран никакъв публичен ключ, софтуерът връща състоянието на обработка '6A88',
- ако някои очаквани информативни обекти липсват, софтуерът връща състояние на обработка '6987'. Това събитие може да се прояви, ако липсва някой от необходимите тагове,
- ако не е достъпен никакъв код за сегментиране за извършване на командата (поради обработването на команда PSO: предишно HASH), софтуерът връща състоянието на обработка '6985',
- ако някои информативни обекти са некоректни, софтуерът връща състояние на обработка '6988'. Тази грешка може да се прояви, ако дължината на някой от изискваните информативни обекти е неправилна,
- ако избраният публичен ключ се приема за повреден, софтуерът връща състоянието на обработка '6400' или '6581'.

4. СТРУКТУРА НА ТАХОГРАФСКИТЕ КАРТИ

Този параграф третира логическата структура на файловете, които тахографските карти определят за запаметяването на достъпните данни.

Той не внася никакви уточнения относно тяхната вътрешна структура, която зависи от производителя (например заглавна част на файла). Той не засяга също така архивирането и обработването на елементите на информацията с вътрешна употреба, като например EuropeanPublicKey, CardPrivateKey, TDesSessionKey или WorkshopCardPin.

Капацитетът на полезната памет на тахографските карти трябва да бъде най-малко равен на 11 kB. Няма пречки за използване на памет с по-голям капацитет. В такъв случай структурата на картата остава непроменена, но броят на записите на някои от структурните елементи се увеличава. Минималните и максималните стойности, които броят на тези записи може да достигне, се уточняват в този параграф.

4.1. Структура на картите на водача

TCS_400 След нейното персонализиране, всяка карта на водач трябва да има следната постоянна логическа структура и условия за достъп до файловете:

Файл	Идентификатор на файла	Условия за достъп		
		Четене	Актуализиране	Криптиране
MF	3F00			
EF ICC	0002	ALW	NEV	No
EF IC	0005	ALW	NEV	No
DF Tachograph	0500			
EF Application_Identification	0501	ALW	NEV	No
EF Card_Certificate	C100	ALW	NEV	No
EF CA_Certificate	C108	ALW	NEV	No
EF Identification	0520	ALW	NEV	No
EF Card_Download	050E	ALW	ALW	No
EF Driving_Licence_Info	0521	ALW	NEV	No
EF Events_Data	0502	ALW	PRO SM / AUT	No
EF Faults_Data	0503	ALW	PRO SM / AUT	No
EF Driver_Activity_Data	0504	ALW	PRO SM / AUT	No
EF Vehicles_Used	0505	ALW	PRO SM / AUT	No
EF Places	0506	ALW	PRO SM / AUT	No
EF Current_Usage	0507	ALW	PRO SM / AUT	No
EF Control_Activity_Data	0508	ALW	PRO SM / AUT	No
EF Specific_Conditions	0522	ALW	PRO SM / AUT	No

TCS_401 Структурата на всички елементарни файлове трябва да бъде такава, че да не зависи от използвания код.

TCS_402 Четенето с използване на защитен от неоторизиран достъп обмен на съобщения трябва да бъде възможно за реализиране за всички файлове, включени в специализирания файл Tachograph.

TCS_403 Всяка карта на водач трябва да има следната структура на данните:

Файл / Елемент на информация	Брой на записите	Размер (байтове)		Стойност по подразбиране
		Мин.	Макс.	
MF		11411	24959	
EF ICC		25	25	
CardIccIdentification		25	25	
clockStop		1	1	{00}
cardExtendedSerialNumber		8	8	{00..00}
cardApprovalNumber		8	8	{20..20}
cardPersonaliserID		1	1	{00}
embedderIcAssemblerId		5	5	{00..00}
icIdentifier		2	2	{00..00}
EF IC		8	8	
CardChipIdentification		8	8	
icSerialNumber		4	4	{00..00}
icManufacturingReferences		4	4	{00..00}
DF Tachograph		11378	24926	
EF Application_Identification		10	10	
DriverCardApplicationIdentification		10	10	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00..00}
noOfEventsPerType		1	1	{00}
noOfFaultsPerType		1	1	{00}
activityStructureLength		2	2	{00..00}
noOfCardVehicleRecords		2	2	{00..00}
noOfCardPlaceRecords		1	1	{00}
EF Card_Certificate		194	194	
CardCertificate		194	194	{00..00}
EF CA_Certificate		194	194	
MemberStateCertificate		194	194	{00..00}
EF Identification		143	143	
CardIdentification		65	65	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
DriverCardHolderIdentification		78	78	
cardHolderName		72	72	
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00, 20..20}
cardHolderBirthDate		4	4	{00..00}
cardHolderPreferredLanguage		2	2	{20 20}

EF Card_Download		4	4	
└─LastCardDownload		4	4	
EF Driving_Licence_Info		53	53	
└─CardDrivingLicenceInformation		53	53	
└─drivingLicenceIssuingAuthority		36	36	{00, 20..20}
└─drivingLicenceIssuingNation		1	1	{00}
└─drivingLicenceNumber		16	16	{20..20}
EF Events_Data		864	1728	
└─CardEventData		864	1728	
└─cardEventRecords	6	144	288	
└─CardEventRecord	n ₁	24	24	
└─eventType		1	1	{00}
└─eventBeginTime		4	4	{00..00}
└─eventEndTime		4	4	{00..00}
└─eventVehicleRegistration				
└─vehicleRegistrationNation		1	1	{00}
└─vehicleRegistrationNumber		14	14	{00, 20..20}
EF Faults_Data		576	1152	
└─CardFaultData		576	1152	
└─cardFaultRecords	2	288	576	
└─CardFaultRecord	n ₂	24	24	
└─faultType		1	1	{00}
└─faultBeginTime		4	4	{00..00}
└─faultEndTime		4	4	{00..00}
└─faultVehicleRegistration				
└─vehicleRegistrationNation		1	1	{00}
└─vehicleRegistrationNumber		14	14	{00, 20..20}
EF Driver_Activity_Data		5548	13780	
└─CardDriverActivity		5548	13780	
└─activityPointerOldestDayRecord		2	2	{00 00}
└─activityPointerNewestRecord		2	2	{00 00}
└─activityDailyRecords	n ₆	5544	13776	{00..00}
EF Vehicles_Used		2606	6202	
└─CardVehiclesUsed		2606	6202	
└─vehiclePointerNewestRecord		2	2	{00 00}
└─cardVehicleRecords		2604	6200	
└─CardVehicleRecord	n ₃	31	31	
└─vehicleOdometerBegin		3	3	{00..00}
└─vehicleOdometerEnd		3	3	{00..00}
└─vehicleFirstUse		4	4	{00..00}
└─vehicleLastUse		4	4	{00..00}
└─vehicleRegistration				
└─vehicleRegistrationNation		1	1	{00}
└─vehicleRegistrationNumber		14	14	{00, 20..20}
└─vuDataBlockCounter		2	2	{00 00}
EF Places		841	1121	
└─CardPlaceDailyWorkPeriod		841	1121	
└─placePointerNewestRecord		1	1	{00}
└─placeRecords		840	1120	
└─PlaceRecord	n ₄	10	10	
└─entryTime		4	4	{00..00}
└─entryTypeDailyWorkPeriod		1	1	{00}
└─dailyWorkPeriodCountry		1	1	{00}
└─dailyWorkPeriodRegion		1	1	{00}
└─vehicleOdometerValue		3	3	{00..00}
EF Current_Usage		19	19	
└─CardCurrentUse		19	19	
└─sessionOpenTime		4	4	{00..00}
└─sessionOpenVehicle				
└─vehicleRegistrationNation		1	1	{00}
└─vehicleRegistrationNumber		14	14	{00, 20..20}
EF Control_Activity_Data		46	46	
└─CardControlActivityDataRecord		46	46	
└─controlType		1	1	{00}
└─controlTime		4	4	{00..00}
└─controlCardNumber				
└─cardType		1	1	{00}
└─cardIssuingMemberState		1	1	{00}
└─cardNumber		16	16	{20..20}
└─controlVehicleRegistration				
└─vehicleRegistrationNation		1	1	{00}
└─vehicleRegistrationNumber		14	14	{00, 20..20}
└─controlDownloadPeriodBegin		4	4	{00..00}
└─controlDownloadPeriodEnd		4	4	{00..00}
EF Specific_Conditions		280	280	
└─SpecificConditionRecord	56	5	5	
└─entryTime		4	4	{00..00}
└─SpecificConditionType		1	1	{00}

TCS_404 Използвани за указване на размери в предишната таблица, стойностите, които следват, съответстват на минималния и максималния брой на записи, които структурата на данните на определена карта на водач трябва да осигурява:

		Мин.	Макс.
n ₁	NoOfEventsPerType	6	12
n ₂	NoOfFaultsPerType	12	24
n ₃	NoOfCardVehicleRecords	84	200
n ₄	NoOfCardPlaceRecords	84	112
n ₆	CardActivityLengthRange	5 544 байта (28 дена * 93 промени на дейността)	13 776 байта (28 дена * 240 про- мени на дейността)

4.2. Структура на цеховите карти

TCS_405 След нейното персонализиране, всяка цехова карта трябва да има следната постоянна логическа структура и условия за достъп до файловете:

Файл	Идентификатор на файла	Условия за достъп		
		Чегене	Актуализиране	Криптиране
MF	3F00	ALW		
EF ICC	0002	ALW	NEV	No
EF IC	0005	ALW	NEV	No
DF Tachograph	0500			
EF Application_Identification	0501	ALW	NEV	No
EF Card_Certificate	C100	ALW	NEV	No
EF CA_Certificate	C108	ALW	NEV	No
EF Identification	0520	ALW	NEV	No
EF Card_Download	0509	ALW	ALW	No
EF Calibration	050A	ALW	PRO SM / AUT	No
EF Sensor_Installation_Data	050B	ALW	NEV	\$\$\$11
EF Events_Data	0502	ALW	PRO SM / AUT	No
EF Faults_Data	0503	ALW	PRO SM / AUT	No
EF Driver_Activity_Data	0504	ALW	PRO SM / AUT	No
EF Vehicles_Used	0505	ALW	PRO SM / AUT	No
EF Places	0506	ALW	PRO SM / AUT	No
EF Current_Usage	0507	ALW	PRO SM / AUT	No
EF Control_Activity_Data	0508	ALW	PRO SM / AUT	No
EF Specific_Conditions	0522	ALW	PRO SM / AUT	No

TCS_406 Структурата на всички елементарни файлове трябва да бъде такава, че да не зависи от използвания код.

TCS_407 Четенето с използване на защитен от неотризиран достъп обмен на съобщения трябва да бъде възможно за реализиране за всички файлове, включени в специализирания файл Tachograph.

TCS_408 Всяка цехова карта трябва да има следната структура на данните:

Файл / Елемент на информация	Брой на записите	Размер (байтове)		Стойност по подразбиране
		Мин.	Макс.	
MF		11088	29061	
EF ICC		25	25	
CardIccIdentification		25	25	
clockStop	1	1	1	{00}
cardExtendedSerialNumber	8	8	8	{00..00}
cardApprovalNumber	8	8	8	{20..20}
cardPersonaliserID	1	1	1	{00}
embedderIcAssemblerId	5	5	5	{00..00}
icIdentifier	2	2	2	{00..00}
EF IC	8	8	8	
CardChipIdentification	8	8	8	
icSerialNumber	4	4	4	{00..00}
icManufacturingReferences	4	4	4	{00..00}
DF Tachograph	11055	29028		
EF Application_Identification	11	11		
WorkshopCardApplicationIdentification	11	11		
typeOfTachographCardId	1	1	1	{00}
cardStructureVersion	2	2	2	{00 00}
noOfEventsPerType	1	1	1	{00}
noOfFaultsPerType	1	1	1	{00}
activityStructureLength	2	2	2	{00 00}
noOfCardVehicleRecords	2	2	2	{00 00}
noOfCardPlaceRecords	1	1	1	{00}
noOfCalibrationRecords	1	1	1	{00}

EF Card_Certificate		194	194	
└CardCertificate		194	194	{00..00}
EF CA_Certificate		194	194	
└MemberStateCertificate		194	194	{00..00}
EF Identification		211	211	
└CardIdentification		65	65	
└└cardIssuingMemberState		1	1	{00}
└└cardNumber		16	16	{20..20}
└└cardIssuingAuthorityName		36	36	{00, 20..20}
└└cardIssueDate		4	4	{00..00}
└└cardValidityBegin		4	4	{00..00}
└└cardExpiryDate		4	4	{00..00}
└WorkshopCardHolderIdentification		146	146	
└└workshopName		36	36	{00, 20..20}
└└workshopAddress		36	36	{00, 20..20}
└└cardHolderName				
└└└holderSurname		36	36	{00, 20..20}
└└└holderFirstNames		36	36	{00, 20..20}
└└cardHolderPreferredLanguage		2	2	{20 20}
EF Card_Download		2	2	
└NoOfCalibrationsSinceDownload		2	2	{00 00}
EF Calibration		9243	26778	
└WorkshopCardCalibrationData		9243	26778	
└└calibrationTotalNumber		2	2	{00 00}
└└calibrationPointerNewestRecord		1	1	{00}
└└calibrationRecords		9240	26775	
└└└WorkshopCardCalibrationRecord	n ₅	105	105	
└└└└calibrationPurpose		1	1	{00}
└└└└vehicleIdentificationNumber		17	17	{20..20}
└└└└vehicleRegistration				
└└└└└vehicleRegistrationNation		1	1	{00}
└└└└└vehicleRegistrationNumber		14	14	{00, 20..20}
└└└└wVehicleCharacteristicConstant		2	2	{00 00}
└└└└kConstantOfRecordingEquipment		2	2	{00 00}
└└└└lTyreCircumference		2	2	{00 00}
└└└└tyreSize		15	15	{20..20}
└└└└authorisedSpeed		1	1	{00}
└└└└oldOdometerValue		3	3	{00..00}
└└└└newOdometerValue		3	3	{00..00}
└└└└oldTimeValue		4	4	{00..00}
└└└└newTimeValue		4	4	{00..00}
└└└└nextCalibrationDate		4	4	{00..00}
└└└└vuPartNumber		16	16	{20..20}
└└└└vuSerialNumber		8	8	{00..00}
└└└└sensorSerialNumber		8	8	{00..00}
EF Sensor_Installation_Data		16	16	
└SensorInstallationSecData		16	16	{00..00}
EF Events_Data		432	432	
└CardEventData		432	432	
└└cardEventRecords	6	72	72	
└└└CardEventRecord	n ₁	24	24	
└└└└eventType		1	1	{00}
└└└└eventBeginTime		4	4	{00..00}
└└└└eventEndTime		4	4	{00..00}
└└└└eventVehicleRegistration				
└└└└└vehicleRegistrationNation		1	1	{00}
└└└└└vehicleRegistrationNumber		14	14	{00, 20..20}
EF Faults_Data		288	288	
└CardFaultData		288	288	
└└cardFaultRecords	2	144	144	
└└└CardFaultRecord	n ₂	24	24	
└└└└faultType		1	1	{00}
└└└└faultBeginTime		4	4	{00..00}
└└└└faultEndTime		4	4	{00..00}
└└└└faultVehicleRegistration				
└└└└└vehicleRegistrationNation		1	1	{00}
└└└└└vehicleRegistrationNumber		14	14	{00, 20..20}
EF Driver_Activity_Data		202	496	
└CardDriverActivity		202	496	
└└activityPointerOldestDayRecord		2	2	{00 00}
└└activityPointerNewestRecord		2	2	{00 00}
└└activityDailyRecords	n ₆	198	492	{00..00}
EF Vehicles_Used		126	250	
└CardVehiclesUsed		126	250	
└└vehiclePointerNewestRecord		2	2	{00 00}
└└cardVehicleRecords		124	248	
└└└CardVehicleRecord	n ₃	31	31	
└└└└vehicleOdometerBegin		3	3	{00..00}

vehicleOdometerEnd		3	3	{00..00}
vehicleFirstUse		4	4	{00..00}
vehicleLastUse		4	4	{00..00}
vehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
vuDataBlockCounter		2	2	{00 00}
EF Places		61	81	
CardPlaceDailyWorkPeriod		61	81	
placePointerNewestRecord		1	1	{00}
placeRecords		60	80	
PlaceRecord	n ₄	10	10	
entryTime		4	4	{00..00}
entryTypeDailyWorkPeriod		1	1	{00}
dailyWorkPeriodCountry		1	1	{00}
dailyWorkPeriodRegion		1	1	{00}
vehicleOdometerValue		3	3	{00..00}
EF Current_Usage		19	19	
CardCurrentUse		19	19	
sessionOpenTime		4	4	{00..00}
sessionOpenVehicle				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Control_Activity_Data		46	46	
CardControlActivityDataRecord		46	46	
controlType		1	1	{00}
controlTime		4	4	{00..00}
controlCardNumber				
cardType		1	1	{00}
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
controlVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
controlDownloadPeriodBegin		4	4	{00..00}
controlDownloadPeriodEnd		4	4	{00..00}
EF Specific_Conditions		10	10	
SpecificConditionRecord	2	5	5	
entryTime		4	4	{00..00}
SpecificConditionType		1	1	{00}

TCS_409 Използвани за указване на размери в предишната таблица, стойностите, които следват, съответстват на минималния и максималния брой записи, които структурата на данните на определена цехова карта трябва да осигурява:

		Мин.	Макс.
n ₁	NoOfEventsPerType	3	3
n ₂	NoOfFaultsPerType	6	6
n ₃	NoOfCardVehicleRecords	4	8
n ₄	NoOfCardPlaceRecords	6	8
n ₆	CardActivityLengthRange	88	255
n ₅	NoOfCalibrationRecords	198 байта (1 ден * 93 промени на дейността)	492 байта (1 ден * 240 промени на дейността)

4.3. Структура на картите на контролър

TCS_410 След нейното персонализиране, всяка карта на контролър трябва да има следната постоянна логическа структура и условия за достъп до файловете:

Файл	Идентификатор на файла	Условия за достъп		
		Четене	Актуализиране	Криптиране
MF	3F00			
EF ICC	0002	ALW	NEV	No
EF IC	0005	ALW	NEV	No
DF Tachograph	0500			
EF Application_Identification	0501	ALW	NEV	No
EF Card_Certificate	C100	ALW	NEV	No
EF CA_Certificate	C108	ALW	NEV	No
EF Identification	0520	AUT	NEV	No
EF Controller_Activity_Data	050C	ALW	PRO SM / AUT	No

- TCS_411 Структурата на всички елементарни файлове трябва да бъде такава, че да не зависи от използвания код.
- TCS_412 Четенето с използване на защитен от неотризиран достъп обмен на съобщения трябва да бъде възможно за реализиране за всички файлове, включени в специализирания файл Tachograph.
- TCS_413 Всяка карта на контролор трябва да има следната структура на данните:

Файл / Елемент на информация	Брой на записите	Размер (байтове)		Брой на записите
		Мин.	Макс.	
MF		11219	24559	
EF ICC		25	25	
CardIccIdentification		25	25	
clockStop		1	1	{00}
cardExtendedSerialNumber		8	8	{00..00}
cardApprovalNumber		8	8	{20..20}
cardPersonaliserID		1	1	{00}
embedderIcAssemblerId		5	5	{00..00}
icIdentifier		2	2	{00..00}
EF IC		8	8	
CardChipIdentification		8	8	
icSerialNumber		4	4	{00..00}
icManufacturingReferences		4	4	{00 00}
DF Tachograph		11186	24526	
EF Application_Identification		5	5	
ControlCardApplicationIdentification		5	5	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfControlActivityRecords		2	2	{00 00}
EF Card_Certificate		194	194	
CardCertificate		194	194	{00..00}
EF CA_Certificate		194	194	
MemberStateCertificate		194	194	{00..00}
EF Identification		211	211	
CardIdentification		65	65	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{00, 20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
ControlCardHolderIdentification		146	146	
controlBodyName		36	36	{00, 20..20}
controlBodyAddress		36	36	{00, 20..20}
cardHolderName				
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00, 20..20}
cardHolderPreferredLanguage		2	2	{20 20}
EF Controller_Activity_Data		10582	23922	
ControlCardControlActivityData		10582	23922	
controlPointerNewestRecord		2	2	{00 00}
controlActivityRecords		10580	23920	
controlActivityRecord	n7	46	46	
controlType		1	1	{00}
controlTime		4	4	{00..00}
controlledCardNumber				
cardType		1	1	{00}
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
controlledVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
controlDownloadPeriodBegin		4	4	{00..00}
controlDownloadPeriodEnd		4	4	{00..00}

TCS_414 Използвани за указване на размери в предишната таблица, стойностите, които следват, съответстват на минималния и максималния брой на записи, които структурата на данните на определена карта на контролор трябва да осигурява:

	Мин.	Макс.
n7 NoOfControlActivityRecords	230	520

4.4. Структура на картите на предприятие

TCS_415 След нейното персонализиране, всяка карта на предприятие трябва да има следната постоянна логическа структура и условия за достъп до файловете:

Файл	Идентификатор на файла	Условия за достъп		
		Четене	Актуализиране	Криптиране
MF	3F00			
EF ICC	0002	ALW	NEV	No
EF IC	0005	ALW	NEV	No
DF Tachograph	0500			
EF Application_Identification	0501	ALW	NEV	No
EF Card_Certificate	C100	ALW	NEV	No
EF CA_Certificate	C108	ALW	NEV	No
EF Identification	0520	AUT	NEV	No
EF Company_Activity_Data	050D	ALW	PRO SM / AUT	No

TCS_416 Структурата на всички елементарни файлове трябва да бъде такава, че да не зависи от използвания код.

TCS_417 Четенето с използване на защитен от неотризиран достъп обмен на съобщения трябва да бъде възможно за реализиране за всички файлове, включени в специализирания файл Tachograph.

TCS_418 Всяка карта на предприятие трябва да има следната структура на данните:

Файл / Елемент на информация	Брой на записите	Размер (байтове)		Стойност по подразбиране
		Мин.	Макс.	
MF		11147	24487	
EF ICC		25	25	
CardIccIdentification		25	25	
clockStop		1	1	{00}
cardExtendedSerialNumber		8	8	{00..00}
cardApprovalNumber		8	8	{20..20}
cardPersonaliserID		1	1	{00}
embedderIcAssemblerId		5	5	{00..00}
icIdentifier		2	2	{00..00}
EF IC		8	8	
CardChipIdentification		8	8	
icSerialNumber		4	4	{00..00}
icManufacturingReferences		4	4	{00..00}
DF Tachograph		11114	24454	
EF Application_Identification		5	5	
CompanyCardApplicationIdentification		5	5	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfCompanyActivityRecords		2	2	{00 00}
EF Card_Certificate		194	194	
CardCertificate		194	194	{00..00}
EF CA_Certificate		194	194	
MemberStateCertificate		194	194	{00..00}
EF Identification		139	139	
CardIdentification		65	65	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{00, 20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
CompanyCardHolderIdentification		74	74	
companyName		36	36	{00, 20..20}
companyAddress		36	36	{00, 20..20}
cardHolderPreferredLanguage		2	2	{20 20}
EF Company_Activity_Data		10582	23922	
CompanyActivityData		10582	23922	
companyPointerNewestRecord		2	2	{00 00}
companyActivityRecords		10580	23920	
companyActivityRecord	n ₈	46	46	
companyActivityType		1	1	{00}
companyActivityTime		4	4	{00..00}
cardNumberInformation				
cardType		1	1	{00}
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
vehicleRegistrationInformation				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}

cardNumberInformation			
cardType	1	1	{00}
cardIssuingMemberState	1	1	{00}
cardNumber	16	16	{20..20}
downloadPeriodBegin	4	4	{00..00}
downloadPeriodEnd	4	4	{00..00}

TCS_419 Използвани за указване на размери в предишната таблица, стойностите, които следват, съответстват на минималния и максималния брой записи, които структурата на данните на определена карта на предприятие трябва да осигурява:

		Мин.	Макс.
№	NoOfCompanyActivityRecords	230	520

Допълнение 3

ПИКТОГРАМИ

PIC_001 Апаратурата за контрол е в състояние да използва следните пиктограми и комбинации от пиктограми:

1. ОСНОВНИ ПИКТОГРАМИ

	Лица	Работни операции	Режими на функциониране
	Предприятие	Контрол	Режим предприятие
	Контрольор	Контрол	Режим на контрол
	Водач	Кормуване	Оперативен режим
	Цех/Изпитателен пункт	Инспекция/Еталониране	Режим на еталониране
	Производител		
	Дейности	Времетраене	
	На разположение	Текущ период на разположение	
	Кормуване	Време на непрекъснато кормуване	
	Почивка	Текущ период на почивка	
	Работа	Текущ период на работа	
	Прекъсване	Общо време на прекъсване	
	Неизвестна дейност		
	Оборудване	Функции	
	Четящо устройство за карта на водача		
	Четящо устройство за карта на помощник-водача		
	Карта	Изобразяване на данните	
	Часовник	Прехвърляне на данни	
	Изобразяване на данните		
	Външна памет		
	Електрическо захранване		
	Принтер/Тиражиране	Отпечатване	
	Датчик		
	Размери на гумите		
	Превозно средство/Блок, монтиран на превозното средство (UEV)		
	Особени условия		
	Извън пределни стойности		
	Преминаване с ферибот/влак		
	Други		
	Събития		Аномалии
	Начало на дневен период на работа		Край на дневен период на работа
	Местонахождение		Ръчно въвеждане на дейностите, извършвани от водача
	Сигурност		Скорост
	Час		Обща сума/Синтез
	Качествени определения		
	За деня		
	За седмица		
	Двуседмично		
	От или към		

2. КОМБИНАЦИИ ОТ ПИКТОГРАМИ

	Други		Други
	Контролен пункт		Крайно място на дневния период на работа
	Начално място на дневния период на работа		До ... часа
	От ... часа		Извън пределните стойности, край
	От превозното средство		
	Извън пределните стойности, начало		

Карти

		Карта на водача
		Карта на предприятие
		Карта на контролор
		Цехова карта
		Без карта

Кормуване

		Кормуване в екип
		Време на седмично кормуване
		Време на двуседмично кормуване

Разпечатване

24			Ежедневна разпечатка на дейностите, извършвани от водача, извлечени от картата		
24			Ежедневна разпечатка на дейностите, извършвани от водача, извлечени от блока, монтиран на превозното средство		
!				Разпечатка на събитията и евентуалните аномалии, извлечени от картата	
!					Разпечатка на събитията и евентуалните аномалии, извлечени от блока, монтиран на превозното средство
T			Разпечатка на техническите данни		
>	>		Разпечатка на превишаванията на допустимата скорост		

Събития

!		Поставяне на нередовна карта	
!			Конфликт, предизвикан от картата
!			Надвишаване на определеното време
!			Кормуване без съответната карта
!			Поставяне на карта по време на кормуване
!			Неправилно приключване на последната сесия
>	>	Надвишаване на допустимата скорост	
!		Прекъсване на електрическото захранване	
!		Грешка на нивото на данните за движение	
!		Нарушаване на сигурността	
!		Сверяване на часовника (в цех)	
>		Контрол на превишаването на допустимата скорост	

Аномалии

X		1	Дефектна карта (Гнездо на картата на водача)
X		2	Дефектна карта (Гнездо на карта на помощник-водача)
X			Дефект при изобразяване на данните
X			Грешка при прехвърляне
X			Дефектен принтер
X			Дефектен датчик
X			Неизправност вътре в блока, монтиран на превозното средство

Процедура по ръчно въвеждане

▶	?	▶	Същия период на дневна работа?
▶	?		Край на предишен период на работа?
▶	•	?	Потвърждение или записване на местонахождението в края на дневния период на работа
⊙	▶	?	Въвеждане часа на тръгване
•	▶	?	Записване на местонахождението в началото на работния период.

Забележка: различни комбинации от допълнителни пиктограми, свързани със същия брой идентификатори за записване или с блокове за отпечатване, се дефинират в допълнение 4.

Допълнение 4

ОТПЕЧАТВАНЕ НА КНИЖЕН НОСИТЕЛ

СЪДЪРЖАНИЕ

1.	Общи положения	133
2	Характеристики на блоковете за данни	133
3.	Характеристики на отпечатките върху хартиен носител	139
3.1.	Ежедневна разпечатка на дейностите, извършвани от водача, извлечени от дадена карта	140
3.2.	Ежедневна разпечатка на дейностите, извършвани от водача, извлечени от блока, монтиран на превозното средство	140
3.3.	Разпечатка на аномалиите и събитията, извлечени от дадена карта	141
3.4.	Разпечатка на аномалиите и събитията, извлечени от блока, монтиран на превозното средство (VU)...	141
3.5.	Разпечатка на техническите данни	142
3.6.	Разпечатка на превишаванията на допустимата скорост	142

2. **Тип на изходящото отпечатване**
Идентификатор на блок
Комбинация от пиктограми за отпечатване (виж Допълнение 3); настройка на устройството за ограничение на скоростта (отпечатване само в случай, когато е надвишена допустимата скорост).
3. **Идентифициране на титуляра на картата**
Идентификатор на блок P = индивидуална пиктограма
Фамилно име на титуляра на картата
Име и презиме на титуляра на картата (при необходимост)
Идентифициране на картата
Краен срок на валидност на картата (при необходимост)
Ако дадена карта не е индивидуална и не съдържа никакво име на титуляр, името на предприятието, на цеха или на съответния контролен орган се отпечатва на неговото място.
4. **Идентификация на превозното средство**
Идентификатор на блок
Идентификационен номер на превозното средство
Държава-членка, в която е регистрирано превозното средство и регистрационен номер на превозното средство.
5. **Идентификация на блока, монтиран на превозното средство**
Идентификатор на блок
Име на производителя на блока
Референтен номер на блока.
6. **Последно еталониране на оборудването за записване**
Идентификатор на блок
Название на цеха
Идентифициране на цеховата карта
Дата на еталониране.
7. **Последна проверка (контрольор)**
Идентификатор на блок
Идентифициране на картата на контрольора
Дата, час и тип на контрола
Тип контрол комбинация, съставена от най-много четири пиктограми. Възможно е типът на контрол да съответства на една от следните пиктограми (или на комбинация от тях):
 : Прехвърляне на данни от карта,; Прехвърляне на данни от блока, монтиран на превозното средство
Отпечатване,; Изобразяване на данните
8. **Дейности, извършвани от водача, записани в хронологичен ред върху картата**
Идентификатор на блок
Дата на консултиране (календарен ден, за който се отнасят отпечатаните данни) + картов брояч за ежедневие присъствие.
- 8.1. *Период, през който картата не се е намирала в четящото устройство*
- 8.1а. Идентификатор на записване (начало на периода)
- 8.1б. *Период с неизвестна дейност* Час на начало и час на край, времетраене
- 8.1в. *Дейност, въведена ръчно*
Пиктограма за дейност, час за начало и за край (включително), продължителност; периодите на почивка с продължителност минимум от един час се отбелязат със звездичка.

Picto xxx km/h

-----P-----
P Last_Name _____
First_Name _____
Card_Identification _____
dd/mm/yyyy

-----D-----
D VIN _____
Nat/VRN _____

-----M-----
M VU_Manufacturer _____
VU_Part_Number _____

-----T-----
T Last_Name _____
Card_Identification _____
T dd/mm/yyyy

-----C-----
Card_Identification _____
C dd/mm/yyyy hh:mm pppp

-----D-----
dd/mm/yyyy xxx

? hh:mm hh:mm hh:mm
A hh:mm hh:mm hh:mm *

- 8.2. **Вкарване на картата в четящото устройство S**
 Държава-членка, в която е регистрирано превозното средство, и регистрационен номер на превозното средство
 Показание на километража на превозното средство при поставянето на картата
- 8.3. **Дейност (по време на поставянето на картата)**
 Пиктограма за дейност, включително часът за начало и за край, продължителност, положение на екипа водачи (пиктограма за екип, ако той се състои от няколко водача, интервал, ако има само един водач); периодите на почивка с продължителност минимум от един час, се отбелязват със звездичка.
- 8.3а. **Особени условия** Час на поставяне, пиктограма (или комбинация от пиктограми), свързана с особените условия.
- 8.4. **Изваждане на карта**
 Показание на километража на превозното средство и изминатото разстояние от последното вкарване на картата, като се има предвид показанието на километража в този момент.
9. **Дейности, извършвани от водача, записани върху блока, монтиран на превозното средство, по хронологичен ред и за всяко четящо устройство**
 Идентификатор на блок
 Дата на консултиране (календарен ден, за който се отнасят отпечатаните данни)
 Показание на километража на превозното средство в 00:00 часа и в 24:00 часа.
10. **Дейности, извършвани в четящото устройство S**
 Идентификатор на блок
- 10.1. **Период, през който не е имало никаква карта в четящото устройство S**
 Идентификатор на запис
 Четящо устройство без карта
 Показание на километража на превозното средство в началото на разглеждания период.
- 10.2. **Поставяне на карта**
 Идентификатор за запис на вкарване на карта
 Фамилно име на водача
 Лично име на водача:
 Идентифициране на картата на водача
 Краен срок на валидност на картата на водача
 Държава-членка, в която е регистрирано предишното използвано превозно средство, и регистрационен номер на това превозно средство
 Дата и час на изваждане на поставената в предишното превозно средство карта
 Празен ред
 Показание на километража при поставянето на картата, ръчно въвеждане на флага за дейност на водача (M при положителен отговор, празно при отрицателен отговор).
- 10.3. **Дейност**
 Пиктограма за дейност, час за начало и за край (включително), продължителност, положение на екипа водачи (пиктограма за екип, ако той се състои от няколко водача, интервал, ако има само един водач); периодите на почивка с продължителност минимум от един час се отбелязват със звездичка.

-----S-----
 Nat/VRN _____
 x xxx xxx km

A hh:mm hh:mm hh:mm ☐☐ *

hh:mm ----- pppp -----

x xxx xxx km; x xxx km

-----☐-----
 dd/mm/yyyy
 x xxx xxx - x xxx xxx km

----- S -----

 ☐☐ ---
 x xxx xxx km

 ☐ Last_Name _____
 First_Name _____
 Card_Identification _____
 dd/mm/yyyy
 Nat/VRN _____
 dd/mm/yyyy hh:mm
 x xxx xxx km M

A hh:mm hh:mm hh:mm ☐☐ *

- 10.3а. *Особени условия* Час на поставяне, пиктограма (или комбинация от пиктограми), свързана с особените условия.

hh:mm - - - - - pppp - - - - -
- 10.4. *Изваждане на карта или край на период „без карта“*
Показание на километража на превозното средство при изваждане на картата или в края на период „без карта“ и изминатото разстояние от поставянето на картата, или от началото на периода „без карта“.

x xxx xxx km; x xxx km
- 11. **Ежедневна справка**
Идентификатор на блок.

----- Σ -----
- 11.1. *Справка на блока, монтиран на превозното средство, за периодите без поставена карта в четящото устройство на водача*
Идентификатор на блок.

1 0 - - -
- 11.2. *Справка на блока, монтиран на превозното средство, за периодите без карта в четящото устройство на помощник-водача*
Идентификатор на блок.

2 0 - - -
- 11.3. *Ежедневна справка на блока, монтиран на превозното средство, за всеки водач*
Идентификатор за запис
Фамилно име на водача
Лично(и) име(на) на водача
Идентифициране на картата на водача

☐ Last_Name _____

First_Name _____

Card_Identification _____
- 11.4. *Въвеждане на местоположението, в което започва и/или завършва един дневен работен период*
pī = пиктограма за местоположението на тръгване/пристигане, час, страна, област,
Показание на километража.

pihh:mm Cou Reg

x xxx xxx km
- 11.5. *Общо времетраене за всяка дейност (извлечено от определена карта)*
Обща продължителност на времето на кормуване, изминатото разстояние
Обща продължителност на периода на работа и на периода на ефективно разположение
Обща продължителност на периода на почивка и на непосочена дейност
Обща продължителност на дейностите на екипа.

☐ hhhmm x xxx km

✱ hhhmm ☐ hhhmm

↳ hhhmm ? hhhmm

☐☐ hhhmm
- 11.6. *Общо времетраене за всяка дейност (периоди, през които не е имало карта в четящото устройство на водача)*
Обща продължителност на времето на кормуване, изминатото разстояние
Обща продължителност на периода на работа и на периода на ефективно разположение
Обща продължителност на периода на почивка.

☐ hhhmm x xxx km

✱ hhhmm ☐ hhhmm

↳ hhhmm
- 11.7. *Общо времетраене за всяка дейност (периоди, през които не е имало карта в четящото устройство на помощник-водача)*
Обща продължителност на периода на работа и на периода на ефективно разположение
Обща продължителност на периода на почивка.

✱ hhhmm ☐ hhhmm

↳ hhhmm

- 11.8. *Общо времетраене за всяка дейност (и за всеки водач, като двете четящи устройства се включват при изчисляването му)*

Обща продължителност на времето на кормуване, изминатото разстояние

Обща продължителност на периода на работа и на периода на ефективно разположение

Обща продължителност на периода на почивка

Обща продължителност на дейностите на екипа

Ако се налага ежедневно отпечатване, установяването на данните, включени в справката, се извършва въз основа на наличните данни към часа на отпечатването.

```

Ⓜ hhhmm x xxx km
Ⓜ hhhmm Ⓜ hhhmm
Ⓜ hhhmm
Ⓜ hhhmm

```

12. Събития и/или аномалии, записани в карта

- 12.1. Идентификатор на блок; 5 последни „Събития и аномалии“, извлечени от дадена карта

```

----- ! x Ⓜ -----

```

- 12.2. Идентификатор на блок; всички „Събития и аномалии“, записани на карта

```

----- ! Ⓜ -----

```

- 12.3. Идентификатор на блок; всички „Аномалии“, записани на карта

```

----- x Ⓜ -----

```

- 12.4. *Записване на събитие и/или на аномалия*

Идентификатор за запис

Пиктограма за събитие/аномалия, мотив за записване, дата и час на начало

Допълнителен код за събитие/аномалия (при необходимост), продължителност

Държава-членка, в която е регистрирано превозното средство, и регистрационен номер на превозното средство, в което се е случило събитието или аномалията.

```

-----
Pic          dd/mm/yyyy hh:mm
| xxx                hhhmm
Ⓜ Nat/VRN _____

```

13. Събития и/или аномалии, които са записани или са в процес на извършване в блок, монтиран на превозното средство

- 13.1. Идентификатор на блок; 5 последни „Събития и аномалии“, извлечени от блока

```

----- ! x Ⓜ -----

```

- 13.2. Идентификатор на блок; всички „Събития“, които са записани или са в процес на извършване в определен блок, монтиран на превозното средство

```

----- ! Ⓜ -----

```

- 13.3. Идентификатор на блок; всички „Аномалии“, които са записани или са в процес на извършване в определен блок, монтиран на превозното средство

```

----- x Ⓜ -----

```

- 13.4. *Записване на събитие и/или на аномалия*

Идентификатор за запис

Пиктограма за събитие/аномалия, причина за записване, дата и час на начало

Допълнителен код за събитие/аномалия (при необходимост), Брой аналогични събития през същия ден, продължителност

Идентифициране на картите, поставени в началото или в края на разглежданото събитие или аномалия (до 4 реда, без повтаряне на номерата на картите)

Случай, когато четящите устройства не приемат никаква карта

Причината за записване (p) приема формата на цифров код, който посочва причината, поради която констатираното събитие или аномалия са записани и кодирани в съответствие с елемента на информация ПричинаЗаписванеСъбитиеАномалия.

```

-----
Pic (p)      dd/mm/yyyy hh:mm
| xxx        (xxx)      hhhmm

Card_Identification _____
Card_Identification _____
Card_Identification _____
Card_Identification _____
Ⓜ ---

```

14. **Идентификация на блока, монтиран на превозното средство**

Идентификатор на блок
 Име на производителя на блока, монтиран на превозното средство
 Адрес на производителя на блока, монтиран на превозното средство
 Референтен номер на блока, монтиран на превозното средство
 Сертификационен номер на блока, монтиран на превозното средство
 Сериен номер на блока, монтиран на превозното средство
 Година на производство на блока, монтиран на превозното средство
 Версия на операционната система на блока и дата на инсталирането му.

```

-----B-----
B Name _____
  Address _____
  PartNumber _____
  Apprv _____
  S/N _____
  yyyy
  v  xx.xx.xx  dd/mm/yyyy
    
```

15. **Идентификация на датчик**

Идентификатор на блок
 Сериен номер на датчика
 Сертификационен номер на датчика
 Дата на първоначално инсталиране на датчика.

```

-----L-----
L S/N _____
  Apprv _____
  dd/mm/yyyy
    
```

16. **Данни за еталониране**

Идентификатор на блок

```

-----T-----
    
```

16.1. *Записване на еталониране*

Идентификатор за запис
 Цех, отговарящ за еталонирането
 Адрес на цеха
 Идентифициране на цехова карта
 Краен срок на валидност на цеховата карта
 Празен ред
 Датата на извършване на еталонирането + причина за еталониране
 Идентификационен номер на превозното средство
 Държава-членка, в която е регистрирано превозното средство и регистрационния номер на превозното средство
 Характеристичен коефициент на превозното средство
 Константа на оборудването за запис
 Действителна окръжност на търкаляне на гумите
 Размери на монтираните гуми
 Регулировка на устройството за ограничаване на скоростта
 Старо и ново показание на километража
 Причината за записване (p) приема формата на цифров код, който посочва причината, поради която тези параметри на еталониране са записани и кодирани в съответствие с елемента на информация ПричинаЕталониране.

```

-----
T Workshop_name _____
  Workshop_address _____
Card-Identification _____
  dd/mm/yyyy

T dd/mm/yyyy (p)
D VIN _____
  Nat/VRN _____
w xx xxx Imp/km
k xx xxx Imp/km
l xx xxx mm
e TyreSize _____
> xxx km/h
x xxx xxx - x xxx xxx km
    
```

17. **Сверяване на часовника**

Идентификатор на блок

```

-----G-----
    
```

17.1. *Записване на сверяването на часовника*

Идентификатор за запис
 Стара дата и час
 Нова дата и час
 Цех, извършил сверяването на часовника
 Адрес на цеха
 Идентифициране на цеховата карта
 Краен срок на валидност на цеховата карта.

```

-----
! G dd/mm/yyyy hh:mm
  G dd/mm/yyyy hh:mm
T Workshop_name _____
  Workshop_address _____
Card_Identification _____
  dd/mm/yyyy
    
```


18. **Най-скорошни събития и аномалии, записани в блока, монтиран на превозното средство**
Идентификатор на блок
Дата и час на „най-скорошното събитие“
Дата и час на най-скорошната аномалия.
19. **Информация относно контрола за превишаване на допустимата скорост**
Идентификатор на блок
Дата и час на последния КОНТРОЛ ЗА ПРЕВИШАВАНЕ НА ДОПУСТИМАТА СКОРОСТ
Дата и час на първото превишаване на допустимата скорост и брой на събитията от такъв характер, записани оттогава.
20. **Записване на превишаванията на допустимата скорост**
- 20.1. Идентификатор на блок „Първо превишаване на допустимата скорост след последното еталониране“
- 20.2. Идентификатор на блок „5 най-сериозни превишавания, записани през последните изминали 365 дни“
- 20.3. Идентификатор на блок „Най-сериозното превишаване за всеки един от периодите, които съвпадат с последните 10 дни на проявяване на това събитие“
- 20.4. Идентификатор за запис
Дата, час и продължителност
Максимална и средна скорост, брой на сходните събития за същия ден
Фамилно име на водача
Лично/и име/на на водача
Идентифициране на картата на водача
- 20.5. Ако в даден блок няма никакъв запис на превишаване на допустимата скорост.
21. **Информация, въведена с клавиатура**
Идентификатор на блок
- 21.1. Контролен пункт
21.2. Подпис на контрольора
21.3. От час
21.4. До час
21.5. Подпис на водача
„Информация, въведена ръчно“: въведете достатъчно празни редове преди всяка рубрика, която е въведена ръчно, за да можете да впишете необходимата информация или да поставите подписа си.

```

----- ! x Д -----
! jj/mm/aaaa hh:mm
x jj/mm/aaaa hh:mm

```

```

----- >> -----
> dd/mm/yyyy hh:mm
>> dd/mm/yyyy hh:mm (nnn)

```

```

----- >>↑ -----

```

```

----- >>(365) -----

```

```

----- >>(10) -----

```

```

-----
>> dd/mm/yyyy hh:mm hh:mm
xxx km/h xxx km/h (xxx)
☐ Last_Name _____
First_Name _____
Card_Identification _____

```

```

>> - - -

```

```

-----
☐ * .....
☐ .....
☐ + .....
+ ☐ .....
☐ .....

```

3. ХАРАКТЕРИСТИКИ НА РАЗПЕЧАТКИТЕ ВЪРХУ ХАРТИЯ

В този раздел се прилагат следните начини за отбелязване:

N
N
X/Y

Отпечатване на блока или на запис номер N

Отпечатване на блока или на запис номер N, повторен толкова пъти, колкото изисква ситуацията

Отпечатване на блоковете или на записите X и/или Y, според нуждите, и повторение на операцията толкова пъти, колкото изисква ситуацията

3.1. Ежедневна разпечатка на дейностите, извършвани от водача, извлечени от дадена карта

PRT_007 Ежедневната разпечатка на дейностите, извършвани от водача, извлечени от дадена карта, трябва да спазва следния формат:

1	Дата и час на отпечатване на документа
2	Тип на отпечатания документ
3	Идентифициране на контрольора (при поставяне на карта за контрол в блока, монтиран на превозното средство)
3	Идентифициране на водача (извлечено от картата, която е обект на отпечатване)
4	Идентифициране на превозното средство (от което е направена разпечатката)
5	Идентифициране на блока, монтиран на превозното средство (от който е направена разпечатката)
6	Последно еталониране на този блок, монтиран на превозното средство
7	Последна проверка, която инспектираният водач е преминал
8	Разграничител на дейностите, извършвани от водача
8.1a / 8.1b / 8.1c / 8.2 / 8.3 / 8.3a / 8.4	Дейности, извършвани от водача, по хронологичен ред
11	Разграничител на ежедневната справка
11.4	Въведени местоположения по хронологичен ред
11.5	Общо времетраене за всяка дейност
12.1	Разграничител на събития и аномалии, извлечени от картата
12.4	Записване на събитие/аномалия (5 последни събития или аномалии, записани върху картата)
13.1	Разпечатка на събития и аномалии, извлечени от блока, монтиран на превозното средство
13.4	Записване на събитие/аномалия (5 последни събития или аномалии, записани или в процес на извършване в блока, монтиран на превозното средство)
21.1	Контролен пункт
21.2	Подпис на контрольора
21.5	Подпис на водача

3.2. Ежедневна разпечатка на дейностите, извършвани от водача, извлечени от блока, монтиран на превозното средство

PRT_008 Ежедневната разпечатка на дейностите, извършвани от водача, извлечени от блока, монтиран на превозното средство, трябва да спазва следния формат:

1	Дата и час на разпечатване на документа
2	Тип на разпечатания документ
3	Идентифициране на титуляра на картата (за всички карти, поставени в блока, монтиран на превозното средство)
4	Идентифициране на превозното средство (от което е направена разпечатката)
5	Идентифициране на блока, монтиран на превозното средство (от който е направена разпечатката)
6	Последно еталониране на този блок
7	Последна проверка, която това оборудване за запис е преминало
9	Разграничител на дейностите, извършвани от водача
10	Разграничител на четящо устройство за карта на водача (четящо устройство 1)
10.1 / 10.2 / 10.3 / 10.3a / 10.4	Дейности, извършвани по хронологичен ред (четящо устройство на водача)
10	Разграничител на четящо устройство за карта на помощник-водач (четящо устройство 2)
10.1 / 10.2 / 10.3 / 10.3a / 10.4	Дейности, извършвани по хронологичен ред (четящо устройство на водача)
11	Разграничител на ежедневната справка
11.1	Справка за периодите без карта в четящото устройство на водача
11.4	Местоположенията, въведени по хронологичен ред
11.6	Общо времетраене за всяка дейност

11.2	Справка за периодите без карта в четящото устройство на помощник-водача
11.4	Местоположенията, въведени по хронологичен ред
11.7	Общо времетраене за всяка дейност
11.3	Справка за дейностите, извършени от водача, като се вземат под внимание и двете четящи устройства
11.4	Местоположенията, въведени от този водач по хронологичен ред
11.7	Общо времетраене за всяка дейност за този водач
13.1	Разграничител на събития и на аномалии
13.4	Записване на събитие/аномалия (5 последни събития или аномалии, записани или в процес на извършване в блока, монтиран на превозното средство)
21.1	Контролен пункт
21.2	Подпис на контрольора
21.3	От час (място, определено за водач без карта, което му позволява да посочи
21.4	периодите, които отговарят на неговите дейности) До час
21.5	Подпис на водача

3.3. Разпечатка на аномалиите и събитията, извлечени от дадена карта

PRT_009 Ежедневната разпечатка на дейностите, извършвани от водача, извлечени от блока, монтиран на превозното средство, трябва да спазва следния формат:

1	Дата и час на отпечатване на документа
2	Тип на отпечатания документ
3	Идентифициране на контрольора (при поставяне на карта за контрол в блока, монтиран на превозното средство)
3	Идентифициране на водача (извлечено от картата, която е обект на разпечатване)
4	Идентифициране на превозното средство (от което е направена разпечатката)
12.2	Разграничител на събитията
12.4	Записване на събития (всички събития, записани върху картата)
12.3	Разграничител на аномалиите
12.4	Записване на аномалии (всички аномалии, записани върху картата)
21.1	Контролен пункт
21.2	Подпис на контрольора
21.5	Подпис на водача

3.4. Разпечатка на аномалиите и събитията, извлечени от блока, монтиран на превозното средство

PRT_010 Разпечатката на аномалиите и събитията, извлечени от блока, монтиран на превозното средство, трябва да спазва следния формат:

1	Дата и час на отпечатване на документа
2	Тип на отпечатвания документ
3	Идентифициране на титуляра на картата (за всички карти, поставени в блока, монтиран на превозното средство)
4	Идентифициране на превозното средство (от което е направена разпечатката)
13.2	Разграничител на събитията
13.4	Записване на събития (всички записани събития или в процес на извършване в блока, монтиран на превозното средство)
13.3	Разграничител на аномалиите
13.4	Записване на аномалии (всички записани аномалии или в процес на извършване в блока, монтиран на превозното средство)
21.1	Контролен пункт
21.2	Подпис на контрольора
21.5	Подпис на водача

3.5. Разпечатка на техническите данни

PRT_011 Разпечатката на техническите данни трябва да спазва следния формат:

1	Дата и час на отпечатване на документа
2	Тип на отпечатвания документ
3	Идентифициране на титуляра на картата (за всички карти, поставени в блока, монтиран на превозното средство)
4	Идентифициране на превозното средство (от което е направена разпечатката)
14	Идентифициране на блока, монтиран на превозното средство
15	Идентифициране на датчиците
16	Разграничител на данните от еталониране
16.1	Записване на еталониране (всички записи, които са на разположение по хронологичен ред)
17	Разграничител на сверяването на часовника
17.1	Записване на сверяването на часовника (всички записи на разположение, извлечени от записите на сверяването на часовника и от записите на данните от еталонирането)
18	Най-скорошни събития и аномалии, записани в блока, монтиран на превозното средство

3.6. Разпечатка на превишенията на допустимата скорост

PRT_012 Разпечатката на превишенията на допустимата скорост трябва да спазва следния формат:

1	Дата и час на отпечатване на документа
2	Тип на отпечатания документ
3	Идентифициране на титуляра на картата (за всички карти, поставени в блока, монтиран на превозното средство)
4	Идентифициране на превозното средство (от което е направена разпечатката)
19	Информация относно контрола за превишаване на допустимата скорост
20.1	Идентификатор на данните за превишаване на допустимата скорост
20.4 / 20.5	Първо превишаване на допустимата скорост след последното еталониране
20.2	Идентификатор на данните за превишаване на допустимата скорост
20.4 / 20.5	5 най-сериозни превишавания, отбелязани в продължение на последните изминали 365 дни
20.3	Идентификатор на данните за превишаване на допустимата скорост
20.4 / 20.5	Най-сериозното превишаване за всеки един от периодите, които съвпадат с последните 10 дни на проявяване на това събитие
21.1	Контролен пункт
21.2	Подпис на контрольора
21.5	Подпис на водача

Допълнение 5

ИЗОБРАЖАВАНЕ НА ДАННИТЕ

В настоящото допълнение се прилагат следните условни начини за обозначаване:

- символите, които се изписват **удебелено**, указват текста, който трябва да се изобрази (при самото изобразяване символите са нормални),
- нормалните символи показват променливите (пиктограми или данни), които се заместват при изобразяването от техните респективни стойности:
 - дд мм ггг: ден, месец, година,
 - чч: часове
 - мм: минути
 - D: пиктограма за времетраене
 - EF: комбинация от пиктограми за събитие или за аномалия
 - O: пиктограма за режим на работа.

DIS_001 Приема се, че оборудването за запис е в състояние да работи със следните формати за изобразяване на данни:

Данни	Format
Изображение по подразбиране	
Местно време	Hh:mm
Режим на работа	O
Информация относно водача	1 Dh <h>h hh<h>h </h></h>
Информация относно помощник-водача	2 Dh <h>h </h>
Условие извън тези граници	OUT
Изобразяване на предупреждения	
Надвишаване на времето за непрекъснато кормуване	1 ⊙ hh <h>h hh<h>h </h></h>
Събитие или аномалия	EF
Изобразяване на други данни	
Дата по координираното универсално време	UTC ⊙ gg/mm/aaaa o UTC ⊙ gg.mm.aaaa
Час	Hh:mm
Време на непрекъснато кормуване и общо време на прекъсване на водача	1 ⊙ hh <h>h hh<h>h </h></h>
Време на непрекъснато кормуване и общо време на прекъсване на помощник-водача	2 ⊙ hh <h>h hh<h>h </h></h>
Общо време на кормуване на водача, записано през текущата и предходната седмица	1 ⊙ hh <h>h </h>
Общо време на кормуване на помощник-водача, записано през текущата и предходната седмица	2 ⊙ hh <h>h </h>

Допълнение 6

ВЪНШНИ ИНТЕРФЕЙСИ

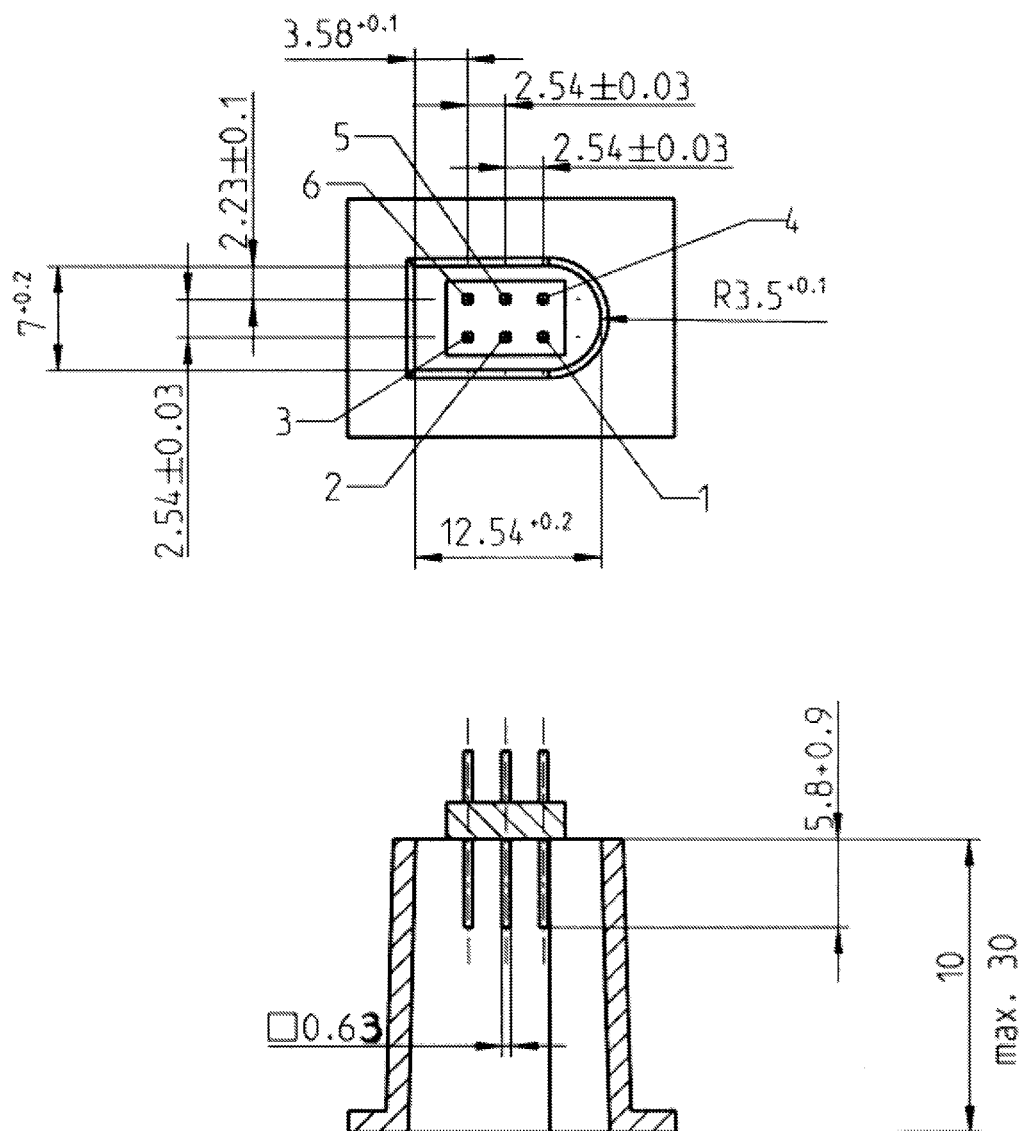
СЪДЪРЖАНИЕ

1.	Техническо оборудване	146
1.1.	Конектор	146
1.2.	Предназначение на контактите	148
1.3.	Схема на работа	148
2.	Интерфейс за прехвърляне на данни	148
3.	Интерфейс за еталониране	149

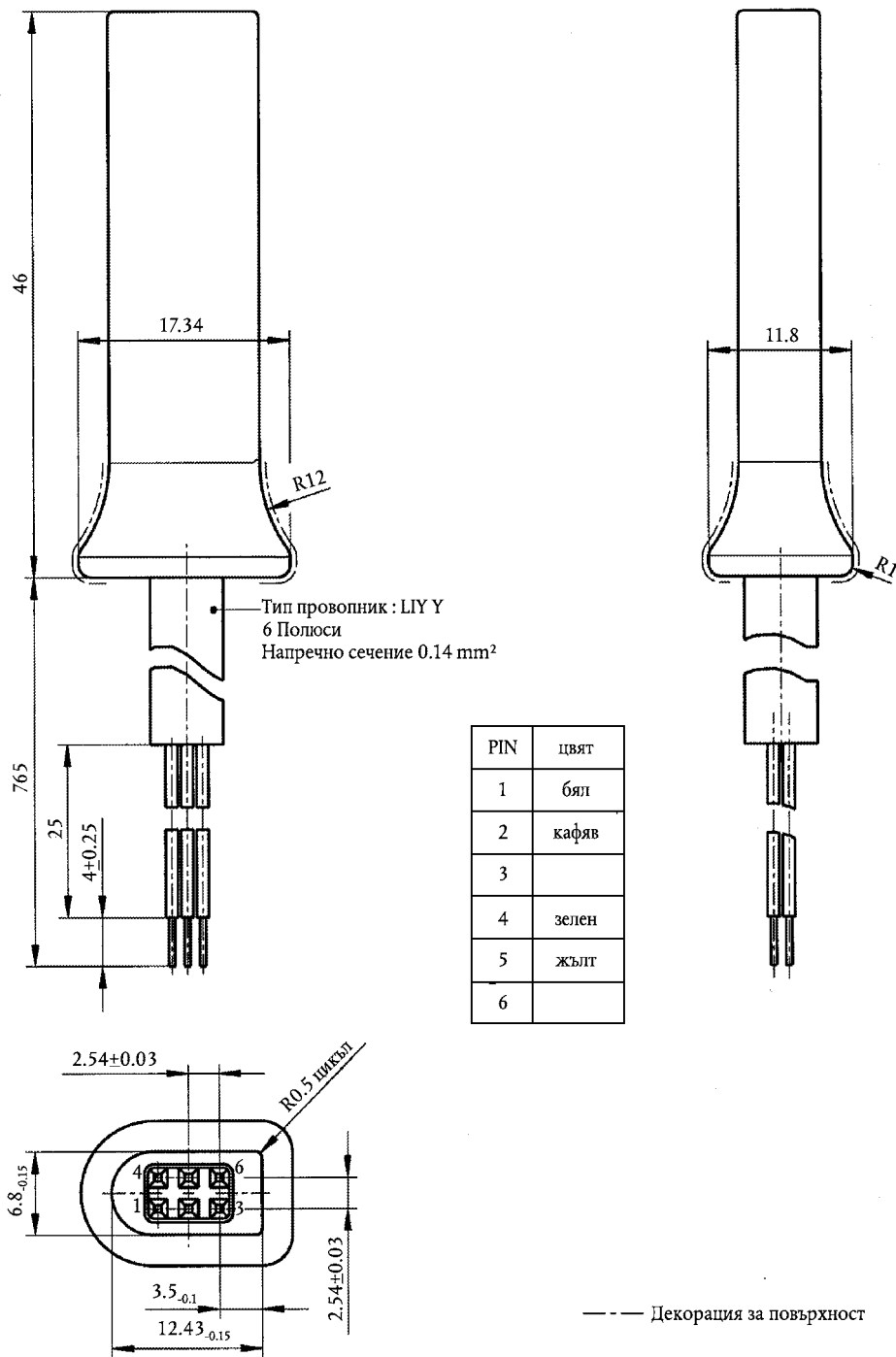
1. ТЕХНИЧЕСКО ОБОРУДВАНЕ

1.1. Конектор

INT_001 Конекторът за прехвърляне/еталониране трябва да представлява съединителен шепсел с шест крачета, достъпен от лицевата страна, без да се налага разкачване на какъвто и да е компонент от оборудването за контрол. Той трябва да отговаря на следния план (всички размери са дадени в милиметри):



Следната схема показва обичайно използвания конектор за свързване с 6 крачета:



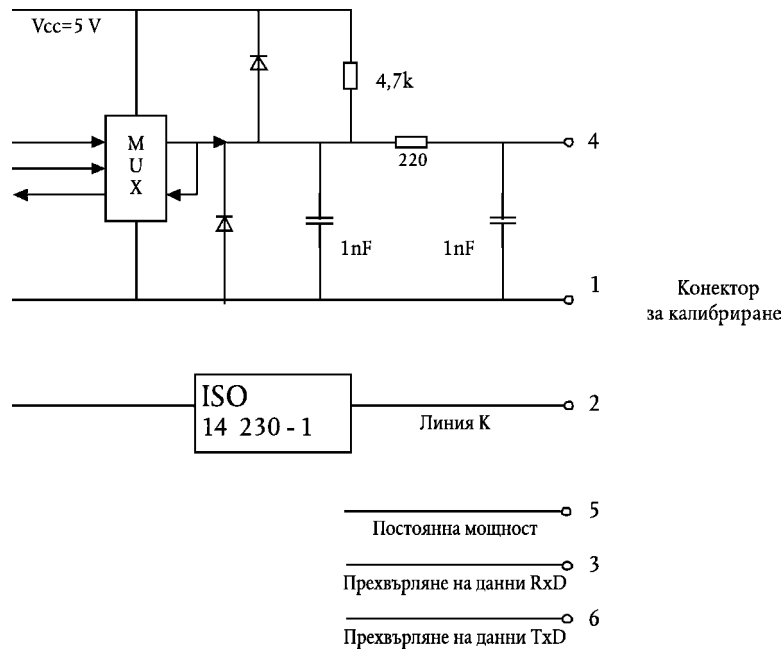
1.2. Предназначение на контактите

INT_002 Предназначението на контактите трябва да отговаря на следната таблица:

Краче	Описание	Забелжка
1	Отрицателен полюс на акумулатора	Свързване с отрицателната клемма на акумулатора на превозното средство
2	Предаване на данни	Линия К (ISO 14 230-1)
3	RxD — Прехвърляне на данни	Вход за данни, предназначени за оборудването за контрол
4	Сигнал вход/изход	Еталониране
5	Постоянна изходяща мощност	Диапазонът на напрежение трябва да бъде идентичен на диапазона на електрическото захранване на превозното средство, намалено с 3 V, за да взема под внимание падането на напрежението, което е неминуемо свързано с преминаването на тока през защитите вериги Изход 40 mA
6	TxD — Прехвърляне на данни	Изход за данни, идващи от оборудването за запис

1.3. Схема на действие

INT_003 Схемата на действие трябва да отговаря на следните указания:



2. ИНТЕРФЕЙС ЗА ПРЕХВЪРЛЯНЕ НА ДАННИ

INT_004 Интерфейсът за прехвърляне на данни трябва да отговаря на спецификациите на стандарт RS232.

INT_005 Интерфейсът за прехвърляне на данни трябва да използва един стартов бит, осем информационни бита (в началото е най-незначещият бит), един бит за контрол на четността и един стопов бит.



Структура на един байт информация

Стартов бит: бит от логическо ниво 0;

Информационни битовете: предават се, като в началото е най-незначещият бит;

бит за контрол на четността: проверка на четността

Стопов бит: бит от логическо ниво 1

При предаването на цифрови данни, съставени от повече от един байт, най-значимият байт се предава на първо място, а най-незначимият байт — последен.

INT_006 Скоростите на предаването на данни трябва да могат да се настройват в диапазон от 9600 и 115 200 бита в секунда. Всяко предаване на данни трябва да се извършва с възможно най-високата скорост на предаване, като стартовата скорост е равна на 9600 бита в секунда непосредствено след началото на връзката.

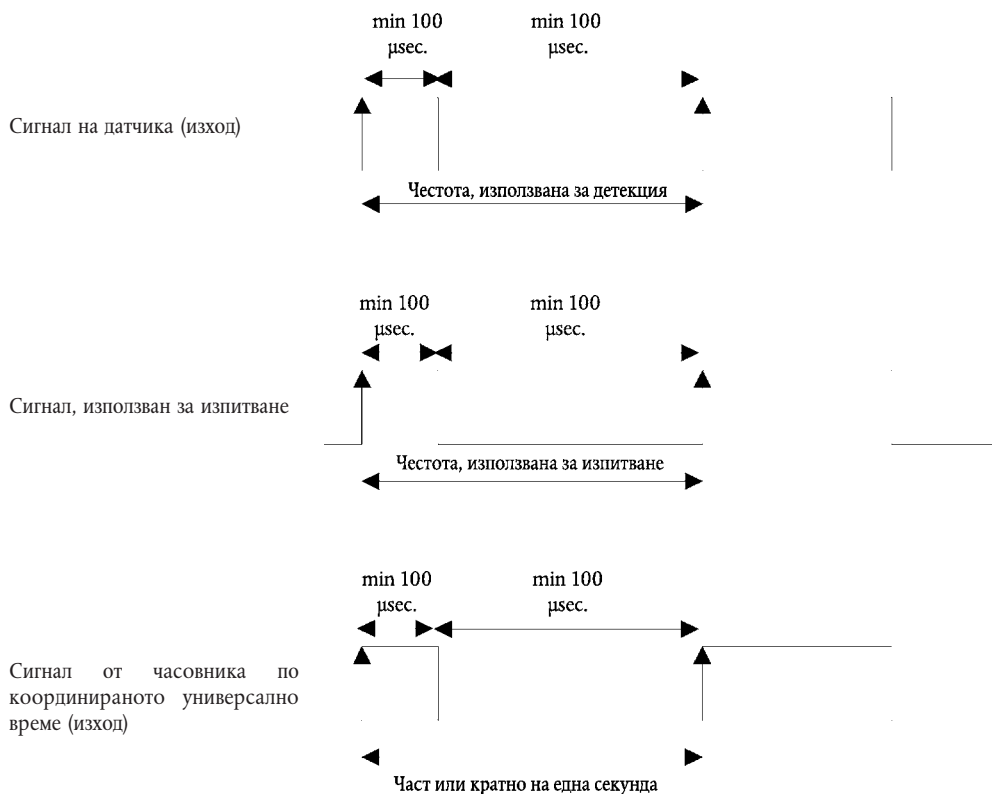
3. ИНТЕРФЕЙС ЗА ЕТАЛОНИРАНЕ

INT_007 Предаването на данните трябва да отговаря на спецификациите на стандарт ISO 14 230-1 Пътни превозни средства — Системи за диагностика — Протокол с ключови думи 2000 — Част I: Физически слой. Първо издание: 1999 г.

INT_008 Входно/изходният сигнал трябва да отговаря на следните електрически спецификации:

Параметър	Минимум	Характеристика	Максимум	Забележка
U_{low} (вход)			1,0 V	$I = 750 \mu A$
U_{high} (вход)	4 V			$I = 200 \mu A$
Честота			4 kHz	
U_{low} (изход)			1,0 V	$I = 1 mA$
U_{high} (изход)	4 V			$I = 1 mA$

INT_009 Входно/изходният сигнал трябва да отговаря на следните хронограми:



Допълнение 7

ПРОТОКОЛИ ЗА ПРЕДАВАНЕ НА ДАННИТЕ

СЪДЪРЖАНИЕ

1.	Въведение	152
1.1.	Обхват	152
1.2.	Съкращения и начин на записване	152
2.	Прехвърляне на данни в блока, монтиран на превозното средство.....	153
2.1.	Процедура по прехвърляне на данни	153
2.2.	Протоколи за прехвърляне на данни	153
2.2.1.	Структура на съобщенията	153
2.2.2.	Типове съобщения	154
2.2.2.1.	Искане за установяване на връзка (IDS 81)	156
2.2.2.2.	Положителен отговор на искане за установяване на връзка (IDS C1).....	156
2.2.2.3.	Искане за започване на сесия за диагностика (IDS 10)	156
2.2.2.4.	Положителен отговор на искане за започване на сесия за диагностика (IDS 50)	156
2.2.2.5.	Услуга за контрол на връзка (IDS 87)	156
2.2.2.6.	Положителен отговор на контрол на връзка (IDS C7).....	156
2.2.2.7.	Искане за прехвърляне на данни (IDS 35)	156
2.2.2.8.	Положителен отговор на искане за прехвърляне на данни (IDS 75)	156
2.2.2.9.	Искане за предаване на данни (IDS 36)	156
2.2.2.10.	Положителен отговор на искане за предаване на данни (IDS 76)	157
2.2.2.11.	Искане за край на предаване на данни (IDS 37)	157
2.2.2.12.	Положителен отговор на искане за край на предаване на данни (IDS 77).....	157
2.2.2.13.	Искане за прекратяване на връзка (IDS 82)	157
2.2.2.14.	Положителен отговор на искане за прекратяване на връзка (IDS C2)	157
2.2.2.15.	Потвърждаване получаването на подсъобщение (IDS 83)	157
2.2.2.16.	Отрицателен отговор (IDS 7F)	157
2.2.3.	Маршрутизация на съобщенията	158
2.2.4.	Синхронизация	159
2.2.5.	Обработка на грешките	159
2.2.5.1.	Фаза за установяване на връзка.....	159
2.2.5.2.	Фаза на връзка	159
2.2.6.	Съдържание на ответните съобщения	162
2.2.6.1.	Положителен отговор на искане за рекапитулация на трансфер на данни.....	162
2.2.6.2.	Положителен отговор на искане за трансфер на данни относно извършените дейности	163
2.2.6.3.	Положителен отговор на искане за трансфер на данни относно събитията и аномалиите	164

2.2.6.4.	Положителен отговор на искане за трансфер на данни относно скоростта на превозното средство.....	165
2.2.6.5.	Положителен отговор на искане за трансфер на технически данни	165
2.3.	Архивиране на файлове върху външно запамятаващо устройство	166
3.	Протокол за прехвърляне на данни от тахографски карти	166
3.1.	Обхват	166
3.2.	Определения	166
3.3.	Прехвърляне на данни от карта	166
3.3.1.	Последователност на инициализиране	167
3.3.2.	Последователност за прехвърляне на файлове с неподписани данни	167
3.3.3.	Последователност за прехвърляне на файлове с подписани данни	167
3.3.4.	Последователност за реинициализиране на брояч на еталониране	168
3.4.	Формат на архивиране на данните	168
3.4.1.	Въведение	168
3.4.2.	Формат на файловете.....	168
4.	Прехвърляне на данни от тахографска карта с помощта на блок, монтиран на превозно средство.....	169

1. ВЪВЕДЕНИЕ

Това допълнение разглежда процедурите, които е необходимо да се прилагат за осъществяването на различните типове прехвърляния на данни към външно запамятащо устройство. То разглежда също и протоколите, които трябва да се прилагат, за да се осигури правилният трансфер на данни и да се гарантира отличната съвместимост на прехвърлените данни с цел всеки контролор да може да инспектира тези данни, като преди да пристъпи към техния евентуален анализ, той се увери в тяхната автентичност и цялост.

1.1. Обхват

Някои данни могат да бъдат прехвърлени към външно запамятащо устройство:

- от блока, монтиран на превозно средство, посредством специализирано логическо устройство (ESI), свързано към този блок,
- от тахографска карта посредством специализирано логическо устройство (ESI), оборудвано с периферно устройство за четене на карти (PIF),
- от тахографска карта посредством блок, монтиран на превозно средство, и посредством специализирано логическо устройство (ESI), свързано към блока, монтиран на превозното средство.

С цел да се даде възможност на контролорите да проверят достоверността и целостта на прехвърлените данни, които са записани върху външно запамятащо устройство, тези данни се придружават от подпис според изискванията на допълнение 11 (Общи механизми за сигурност). Идентифицирането на изходното оборудване (блокът, монтиран на превозното средство, или картата) и неговите сертификати за сигурност (държава-членка и оборудване) също се прехвърлят. Проверителят трябва да притежава европейски публичен ключ, защитен срещу неотризиран достъп.

DDP_001 Данните, които са прехвърлени по време на сесия за прехвърляне, трябва да бъдат записани в един и същ файл върху външното запамятащо устройство.

1.2. Съкращения и начин на записване

Съкращенията, които следват, се използват в настоящото допълнение:

CCI	карта с вграден/и чип/ове
CIB	набелязан байт
EOpS	изпълнение на операция, свързана със сигурността
ESI	специализирано логическо устройство [оборудване, което се използва за прехвърляне на данни към външно запамятащо устройство]
FE	елементарен файл
FMT	байт за структура (първи байт на заглавната част на съобщение)
FE	специализиран файл
IDA	идентификатор на приложение
IDF	идентификатор на файл
IDS	идентификатор на услуга
LON	байт за дължина (последен байт на заглавната част на съобщение)
PIF	периферно устройство за четене на карти
PMC	протокол с ключови думи 2000
PDT	параметър на искане за трансфер
PRT	параметър на отговор за трансфер
RAR	отговор на реинициализиране
SD	сесия за диагностика
SME	външно запамятащо устройство
SPP	избор на параметрите на протокол
SRC	изходен байт
TC	байт за контролна сума
UEV	блок, монтиран на превозното средство
VLB	стойност на дължина на таг

2. ПРЕХВЪРЛЯНЕ НА ДАННИ ВЪРХУ БЛОКА, МОНТИРАН НА ПРЕВОЗНОТО СРЕДСТВО

2.1. Процедура по прехвърляне на данни

За да се извърши прехвърляне на данни върху блока, монтиран на превозното средство, операторът трябва да изпълни следните операции:

- поставя се тахографската карта в отвора на едно от четящите устройства на блока, монтиран върху превозното средство ⁽¹⁾,
- свързва се специализирано логическо устройство към конектора за прехвърляне на данни на блока, монтиран на превозното средство,
- установява се връзка между специализирано логическо устройство и блока, монтиран на превозното средство,
- от специализираното логическо устройство се избират данните, които ще се прехвърлят, и се изпраща необходимото искане към блока, монтиран на превозното средство,
- прекратява се сесията по прехвърляне на данни.

2.2. Протокол за прехвърляне на данни

Структурата на протокола се основава на отношението главно-подчинено устройство, специализираното логическо устройство играе роля на главно устройство, а блокът, монтиран на превозното средство — на подчинено устройство.

Структурата на съобщенията, техният тип и тяхната маршрутизация се основават главно на протокола с ключови думи 2000 (РМС) (ISO 14230-2 Пътни превозни средства — Системи за диагностика — Протокол с ключови думи 2000 — Част II: Слой връзка между данните).

Приложният слой се основава главно върху настоящия проект за стандарт ISO 14229-1 (Пътни превозни средства — системи за диагностика — Част I: услуги за диагностика, версия 6 от 22 февруари 2001 г.).

2.2.1. Структура на съобщенията

DDP_002 Всички разменени съобщения между специализираното логическо устройство и блока, монтиран на превозното средство, се характеризират със структура от три елемента:

- заглавна част, съставена от следните байтове: байт за структура (FMT), набелязан байт (CIB), изходен байт (SRC) и, при необходимост, байт за дължина (LON),
- поле от данни, съдържащо един байт за идентифициране на услуга (IDS) и променлив брой байтове за информация, които могат да включат един опционален байт за сесия по диагностиране (SD) или един опционален байт за параметър за трансфер (PDT или PRT),
- контролна сума, съставена от байт за контролна сума (TC).

Заглавна част на съобщение				Поле с данни					Контролна сума
FMT	CIB	SRC	LON	IDS	ДАННИ	TC
4 байта				255 байта максимум					1 байт

Байтове CIB и SRC представляват физическите адреси на получателя и на изпращача на съобщението. Те вземат стойностите F0 Hex за специализираното логическо устройство и EE Hex за блока, монтиран на превозното средство.

Байтът LON указва дължината на полето за данни.

Байтът за контролна сума съответства на серия от суми по 8 бита по модул 256, които представляват всички байтове на съобщението с изключение на самата контролна сума.

Байтовете FMT, IDS, SD, PDT и PRT са също определени по-нататък в този документ.

⁽¹⁾ Поставянето на картата задейства активирането на съответните права за достъп както за данните, така и за функцията по прехвърляне.

- DDP_003 Ако дължината на данните, за които се смята, че се пренасят от съобщението, надхвърля свободното пространство в полето за данни, изпращането на това съобщение става под формата на няколко подсъобщения. Всяко от тези подсъобщения съдържа заглавна част, същите IDS и PRT, както и брояч на подсъобщения от 2 байта, който посочва поредния номер на всяко подсъобщение в рамките на цялото съобщение. С цел осигуряване на контрол за грешка и евентуално прекратяване на обмена на данни, специализираното логическо устройство потвърждава получаването на всяко подсъобщение. Специализираното логическо устройство е в състояние да приеме подсъобщение, да поиска повторното му предаване и да поиска от блока, монтиран на превозното средство, да възобнови или да прекрати предаването на данните.
- DDP_004 Ако полето за данни на последното подсъобщение съдържа точно 255 байта, е необходимо да се прибави към тях едно последно подсъобщение, което съдържа празно поле за данни (с изключение на IDS, PRT и брояча на подсъобщения) за да покаже края на съобщението.

Пример:

Заглавна част	IDS	PRT	Съобщение	ТС
4 байта	Дължина по-голяма от 255 байта			

Предадено под следната форма:

Заглавна част	IDS	PRT	00	01	Подсъобщение 1	ТС
4 байта	255 байта					

Заглавна част	IDS	PRT	00	02	Подсъобщение 2	ТС
4 байта	255 байта					

...

Заглавна част	IDS	PRT	xx	yy	Подсъобщение n	ТС
4 байта	Дължина по-малка от 255 байта					

Или под следната форма:

Заглавна част	IDS	PRT	00	01	Подсъобщение 1	ТС
4 байта	255 байта					

Заглавна част	IDS	PRT	00	02	Подсъобщение 2	ТС
4 байта	255 байта					

...

Заглавна част	IDS	PRT	xx	yy	Подсъобщение n	ТС
4 байта	255 байта					

Заглавна част	IDS	PRT	xx	yy+1	ТС
4 байта	4 байта				

2.2.2. Типове съобщения

Протоколът за връзка, който се прилага при прехвърляне на данни между блока, монтиран на превозното средство, и специализираното логическо устройство, изисква обмен на 8 типа различни съобщения.

Таблицата, която следва, представлява синтез на този процес.

Структура на съобщението		Заглавна част от максимум 4 байта				Данни от максимум 255 байта			Контролна сума на един байт
		FMT	CIB	SRC	LON	IDS	SD/PRT	ДАННИ	
ESI ->	<-UEV								
Искане за установяване на връзка		81	EE	FO		81			E0
Положителен отговор на искане за установяване на връзка		80	FO	EE	03	C1		8F,EA	9B
Искане за започване на сесия за диагностика		80	EE	FO	02	10	81		F1
Положителен отговор на искане за започване на сесия за диагностика		80	FO	EE	02	50	81		31
Връзка с контролната служба									
Проверка на скоростта в бодове (етап 1)									
9600 Bd		80	EE	FO	04	87		01,01,01	EC
19 200 Bd		80	EE	FO	04	87		01,01,02	ED
38 400 Bd		80	EE	FO	04	87		01,01,03	ED
57 600 Bd		80	EE	FO	04	87		01,01,04	EF
115 200 Bd		80	EE	FO	04	87		01,01,05	FO
Положителен отговор на искане за проверка на скоростта в бодове		80	FO	EE	02	C7		01	28
Скорост на транзитиране в бодове (етап 2)		80	EE	FO	03	87		02,03	ED
Искане за прехвърляне (upload)		80	EE	FO	0A	35		00,00,00,00,00,FF,FF,FF,FF	99
Положителен отговор на искане за прехвърляне на данни		80	FO	EE	03	75		00,FF	D5
Искане за прехвърляне на данни									
Рекапитулативен		80	EE	FO	02	36	01		97
Дейности		80	EE	FO	06	36	02	Date	CS
Събития и аномалии		80	EE	FO	02	36	03		99
Моментна скорост		80	EE	FO	02	36	04		9A
Технически данни		80	EE	FO	02	36	05		9B
Прехвърляне (download) на данни от карта		80	EE	FO	02	36	06		9C
Положителен отговор на искане на трансфер на данни		80	FO	EE	Len	76	TREP	Data	CS
Искане за край на трансфер на данни		80	EE	FO	01	37			96
Положителен отговор на искане за край на трансфер		80	FO	EE	01	77			D6
Искане за прекратяване на връзката		80	FO	EE	01	82			E1
Положителен отговор на искане за прекратяване на връзката		80	FO	EE	01	C2			21
Потвърждаване получаването на подсъобщение		80	EE	FO	Len	83		Data	CS
Отрицателни отговори									
Отказ за прехвърляне на данни		80	FO	EE	03	7F	IDS Req	10	CS
Несъвместима услуга		80	FO	EE	03	7F	IDS Req	11	CS
Несъвместива подфункция		80	FO	EE	03	7F	IDS Req	12	CS
Неправилна дължина на съобщението		80	FO	EE	03	7F	IDS Req	13	CS
Неправилни условия или грешка при последователността на запитванията		80	FO	EE	03	7F	IDS Req	22	CS
Прекомерно искане		80	FO	EE	03	7F	IDS Req	31	CS
Отказ за прехвърляне на данни		80	FO	EE	03	7F	IDS Req	50	CS
Изчакване на отговор		80	FO	EE	03	7F	IDS Req	78	CS
Данни, които са неналични		80	FO	EE	03	7F	IDS Req	FA	CS

Бележки:

- IDS Dem = IDS на съответното искане, IDL Dem = IDL на съответното искане.
- PRT = le PDT на съответното искане.
- Наличието на клетки, оцветени в черно, показва отсъствие на предаване на данни.
- Използването на термина „upload“ [прехвърляне от терминално устройство към главен компютър] (считано от специализираното логическо устройство) се налага за гарантиране на съвместимостта на системата със стандарта ISO 14229. Този термин притежава същото значение като „download“ [прехвърляне от главен компютър към терминално устройство] (считано от блока, монтиран на превозното средство).
- Тази таблица не представлява никакъв потенциален брояч за подсъобщения от 2 байта.

2.2.2.1. *Искане за установяване на връзка (IDS 81)*

DDP_005 Това съобщение се предава от специализираното логическо устройство за установяване на взаимна връзка с блока, монтиран на превозното средство. Началните връзки се извършват винаги със скорост от 9600 бода (до момента, когато тази пропускателна скорост се промени с помощта на съответните услуги за контрол на връзките).

2.2.2.2. *Положителен отговор на искане за установяване на връзка (IDS C1)*

DDP_006 Блокът, монтиран на превозното средство, изпраща това съобщение, за да отговори положително на искане за установяване на връзка. То съдържа двата ключови байта „8F“ „EA“, които посочват, че съответният блок осигурява приложението на съответния протокол, заглавната част на всяко съобщение, която включва набелязаните байтове, изходните байтове и байтовете за дължина.

2.2.2.3. *Искане за започване на сесия за диагностика (IDS 10)*

DDP_007 Специализираното логическо устройство изпраща съобщение за искане за започване на сесия за диагностика с цел установяване на нова сесия за диагностика с блока, монтиран на превозното средство. Подфункцията „сесия по подразбиране“ (81 Hex) указва, че ще започне стандартна сесия за диагностика.

2.2.2.4. *Положителен отговор на искане за започване на сесия за диагностика (IDS 50)*

DDP_008 Блокът, монтиран на превозното средство, изпраща положително ответно съобщение на искане за диагностика, за да отговори положително на искане за започване на сесия за диагностика.

2.2.2.5. *Услуга за контрол на връзка (IDS 87)*

DDP_052 Услугата за контрола на връзката се използва от специализираното логическо устройство, за да започне промяна в пропускателната скорост в бодове. Тази операция включва два етапа. През първия етап специализираното логическо устройство предлага промяна в пропускателната скорост в бодове, като посочва новата пропускателна скорост. При получаване на положително съобщение от блока, монтиран на превозното средство, специализираното логическо устройство изпраща потвърждение на промяната в пропускателната скорост в бодове до блока (втори етап). Тогава специализираното логическо устройство преминава към новата пропускателна скорост в бодове. След получаване на потвърждението блокът, монтиран на превозното средство, преминава към новата пропускателна скорост в бодове.

2.2.2.6. *Положителен отговор на контрол на връзка (IDS C7)*

DDP_053 Положителният отговор за контрола на връзка се получава от блока, монтиран на превозното средство, по искане на услугата за контрол на връзка (първи етап). Трябва да се отбележи, че на искането за потвърждение не се дава никакъв отговор (втори етап).

2.2.2.7. *Искане за прехвърляне на данни (IDS 35)*

DDP_009 Специализираното логическо устройство изпраща съобщение за искане за прехвърляне на данни с цел да уточни на блока, монтиран на превозното средство, че иска изпълнение на операция по прехвърляне на данни. За да се отговори на изискванията на стандарта ISO 14229, се включват данни относно адреса, размера и характеристиките на формата на исканите данни. Тъй като тези информации не са известни на специализираното логическо устройство преди прехвърлянето, адресът в паметта се нулира, структурата се декриптира и декомпресира и размерът на паметта се определя на максимум.

2.2.2.8. *Положителен отговор на искане за прехвърляне на данни (IDS 75)*

DDP_010 Блокът, монтиран на превозното средство, изпраща положително ответно съобщение на искане за прехвърляне на данни, за да съобщи на специализираното логическо устройство, че блокът, монтиран на превозното средство, е готов да прехвърля данните. За да отговори на изискванията на стандарт ISO 14229, положителното ответно съобщение съдържа данни, които показват на специализираното логическо устройство, че следващите положителни ответни съобщения на искане за трансфер на данни ще съдържат максимум 00FF hex байта.

2.2.2.9. *Искане за трансфер на данни (IDS 36)*

DDP_011 Специализираното логическо устройство изпраща искане за трансфер на данни с цел да уточни на блока, монтиран на превозното средство, вида на данните, които ще се прехвърлят. Параметърът за искане на трансфер (PDT) на определен байт показва за какъв тип трансфер става въпрос.

Съществуват шест типа трансфер на данни:

- рекапитулативен (PDT 01),
- дейности, свързани с определена дата (PDT 02),
- събития и аномалии (PDT 03),
- моментна скорост (PDT 04),
- технически данни (PDT 05),
- прехвърляне на данни от карта (PDT 06).

DDP_054 За специализираното логическо устройство е задължително да иска трансфер на данни от тип „рекапитулативен“ (PDT 01) по време на сесия за прехвърляне на данни, защото това единствено гарантира, че сертификатите на блока, монтиран на превозното средство, се регистрират върху прехвърляния файл (и по този начин позволява проверката на цифровия подпис).

Във втория случай (PDT 02), съобщението за искане на трансфер на данни съдържа указание за календарния ден (формат `TimeReal`), към който се отнася прехвърлянето.

2.2.2.10. *Положителен отговор на искане за трансфер на данни (IDS 76)*

DDP_012 Блокът, монтиран на превозното средство, изпраща положителното ответно съобщение на искане за трансфер на данни в отговор на искане от такъв вид. Това съобщение съдържа исканите данни, както и параметър за отговор на искане за трансфер (PRT), съответстващ на параметъра на искането.

DDP_055 В първия случай (PDT 01) блокът, монтиран на превозното средство, трябва да изпрати данни, предназначени да помогнат на оператора на специализираното логическо устройство при избирането на данните, които те желаят да прехвърлят. Информациите, които се съдържат в това съобщение, са следните:

- сертификати за сигурност,
- идентификация на превозното средство,
- новата дата и новия час на блока, монтиран на превозното средство,
- най-ранната и най-късната дата за прехвърляне (на данни от блока, монтиран на превозното средство),
- указания относно наличието на карти в блока, монтиран на превозното средство,
- предишни прехвърляния на данни към предприятие,
- блокировки от страна на предприятието,
- предишни контролни проверки.

2.2.2.11. *Искане за край на трансфер на данни (IDS 37)*

DDP_013 Специализираното логическо устройство изпраща съобщение за искане за край на трансфер на данни с цел да информира блока, монтиран на превозното средство, че сесията по прехвърляне е приключена.

2.2.2.12. *Положителен отговор на искане за край на трансфер на данни (IDS 77)*

DDP_014 Блокът, монтиран на превозното средство, изпраща положително ответно съобщение на искане за край на трансфер на данни, за да потвърди получаването на искането за край на трансфера.

2.2.2.13. *Искане за прекратяване на връзката (IDS 82)*

DDP_015 Специализираното логическо устройство изпраща съобщение за искане за прекратяване на връзката с цел преустановяване на взаимната връзка с блока, монтиран на превозното средство.

2.2.2.14. *Положителен отговор на искане за прекратяване на връзка (IDS C2)*

DDP_016 Блокът, монтиран на превозното средство, изпраща положително ответно съобщение на искане за край на връзката, за да потвърди получаването на искането за край на връзката.

2.2.2.15. *Потвърждаване на получаването на подсъобщение (IDS 83)*

DDP_017 Специализираното логическо устройство изпраща потвърждение за получено подсъобщение с цел потвърждение получаването на различните части от съобщението, изпратени под формата на подсъобщения. Полето за данни съдържа IDS, прехвърлен от блока, монтиран на превозното средство, както и код от 2 байта, който се изписва по следния начин:

- `MsgC + 1` потвърждава правилното получаване на подсъобщение номер `MsgC`.

Искане за изпращане на следващото подсъобщение, адресирано от специализираното логическо устройство до блока, монтиран на превозното средство,

- `MsgC` посочва появяването на проблем, който засяга получаването на подсъобщение номер `MsgC`.

Искане за връщане на въпросното подсъобщение, адресирано от специализираното логическо устройство до блока, монтиран на превозното средство,

- `FFFF` съобщава за прекъсването на съобщението по време на предаването на данните.

Специализираното логическо устройство може да прибегне до този код, за да сложи край на предаването на съобщението, изпратено от блока, монтиран на превозното средство, като това става без значение каква е причината.

Системата позволява да се потвърди (или не) получаването на последното подсъобщение от кое да е съобщение (байт `LON < 255`), като се прибегва или не до някой от тези кодове.

Съставен от няколко подсъобщения, отговорът на блока, монтиран на превозното средство, се изобразява, както следва:

- положителен отговор на искане за трансфер на данни (IDS 76).

2.2.2.16. *Отрицателен отговор (IDS 7F)*

DDP_018 Блокът, монтиран на превозното средство, изпраща отрицателно ответно съобщение в отговор на съобщенията по-горе, ако се окаже, че той не е в състояние да удовлетвори предаденото искане. Полетата за данни на съобщението съдържат IDS на отговора (7F), IDS на искането и код, който уточнява причината за отрицателния отговор. Прилагат се следните кодове:

- 10 — общо отхвърляне
Операцията не може да се изпълни по причина, която не се разглежда по-нататък,
- 11 — несъвместима услуга
IDS на искането не се разбира от блока, монтиран на превозното средство,
- 12 — несъвместима подфункция
SD или PDT на искането са неразбираеми за блока, монтиран на превозното средство, или предаването на подсъобщения е приключило,
- 13 — неправилна дължина на съобщение
Дължината на полученото съобщение е неправилна,
- 22 — неправилни условия или грешка, която засяга последователността на запитването
Исканата услуга не е налична или последователността на съобщенията за искане е неправилна,
- 31 — недопустимост на искането
Записването (полето за данни) на параметъра на искането не е валидно,
- 50 — отказ за прехвърляне на данни
Искането не може да бъде изпълнено (блокът, монтиран на превозното средство, се използва в несвойствен режим на работа или има наличие на някаква вътрешна аномалия),
- 78 — изчакване на отговор
Исканото действие не може да приключи в определеното време и блокът, монтиран на превозното средство, няма готовност да приеме друго искане,
- Данни FA, които не са на разположение
Обектът на искане за трансфер на данни не е достъпен в блока, монтиран на превозното средство (например липсва вкарана карта, ...).

2.2.3. Маршрутизация на съобщенията

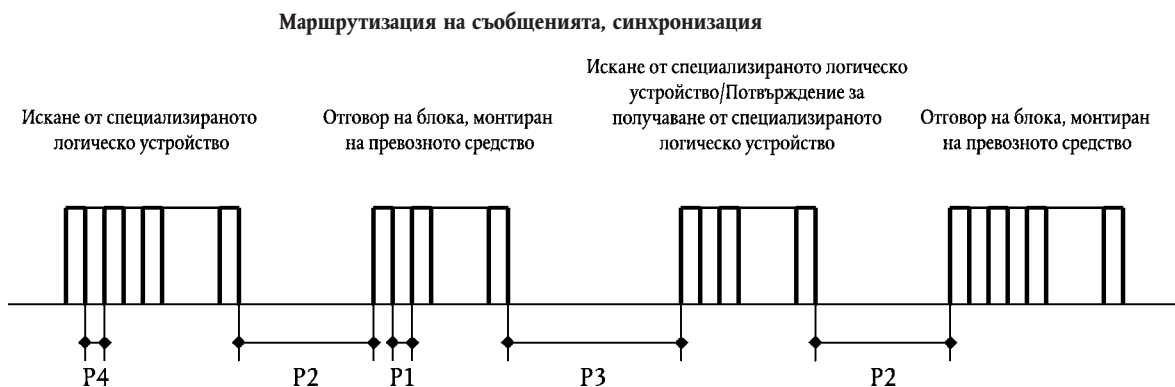
По време на нормална процедура по прехвърляне на данни маршрутизацията на съобщенията се извършва обикновено по следния начин:

Специализирано логическо устройство		Блок, монтиран на превозното средство
Искане за установяване на връзката	⇒ ⇐	Положителен отговор
Искане за започване на сесия за диагностика	⇒ ⇐	Положителен отговор
Искане за прехвърляне на данни	⇒ ⇐	Положителен отговор
Искане за трансфер на данни #1 Рекапитулативен	⇒ ⇐	Положителен отговор
Искане за трансфер на данни #2	⇒ ⇐	Положителен отговор #1
Потвърждение на получаването на подсъобщение #1	⇒ ⇐	Положителен отговор #2
Потвърждение на получаването на подсъобщение #2	⇒ ⇐	Положителен отговор #m
Потвърждение на получаването на подсъобщение #m	⇒ ⇐	Положителен отговор (поле за данни < 255 байта)
Потвърждаване на получаването на подсъобщение (опционално)	⇒	
...		
Искане за трансфер на данни #n	⇒ ⇐	Положителен отговор
Искане за край на трансфер на данни	⇒ ⇐	Положителен отговор
Искане за прекратяване на връзката	⇒ ⇐	Положителен отговор

2.2.4. Синхронизация

DDP_019 При нормални условия на експлоатация се прилагат следните параметри за синхронизация, илюстрирани на следващата фигура:

Фигура 1



където:

- P1 = Представява междубайтово време, характеризиращо отговор на блока, монтиран на превозното средство,
P2 = Представява времето между края на искане на специализираното логическо устройство или между края на получаване на потвърждение от специализираното логическо устройство и начало на следващ отговор от блока, монтиран на превозното средство,
P3 = Представява времето между края на отговор на блока, монтиран на превозното средство, и началото на ново искане на специализираното логическо устройство, между края на отговор на блока, монтиран на превозното средство, и началото на потвърждение за получаване от специализираното логическо устройство, или между края на искане от специализираното логическо устройство и началото на ново искане от специализираното логическо устройство, ако блокът не даде отговор,
P4 = представлява междубайтово време, характеризиращо искане на специализираното логическо устройство,
P5 = Разширена стойност на P3 за прехвърляне на данни от карти.

Следващата таблица представя стойностите, които параметрите за синхронизация са в състояние да приемат (разширен набор от параметри за синхронизация PMS, използвани в случай на физическо адресиране, целящо увеличаването на скоростта на връзките).

Параметър на синхронизация	Долна граница (в ms)	Горна граница (в ms)
P1	0	20
P2	20	1000 (*)
P3	10	5000
P4	5	20
P5	10	20 минути

(*) Ако блокът, монтиран на превозното средство, реагира, като изпрати отрицателен отговор, който съдържа код със следния смисъл: „правилно получено искане, изчакване на отговор“, тази стойност се отнася до същата горна граница, както стойността на P3

2.2.5. Обработка на грешките

Ако се появи грешка по време на обмена на съобщения, планът за маршрутизация на съобщенията се променя в зависимост от устройството, което е открило грешката, и от съобщението, което е в основата на тази грешка.

Фигури 2 и 3 показват процедурите за обработка на грешки, които се прилагат съответно за блока, монтиран на превозното средство и за специализираното логическо устройство.

2.2.5.1. Фаза за установяване на връзка

DDP_020 Ако специализираното логическо устройство открие грешка по време на фазата на установяване на връзка както на равнище синхронизация, така и на равнище последователност на битовете, тогава то изчаква за период от P3 min, преди да изпрати отново същото искане.

DDP_021 Ако блокът, монтиран на превозното средство, открие грешка в последователността, която идва от специализираното логическо устройство, той не изпраща никакъв отговор; блокът изчаква друго съобщение за искане за установяването на връзка в срок от P3 max.

2.2.5.2. Фаза на връзка

Могат да се определят две различни процедури по обработката на грешка:

1. Блокът, монтиран на превозното средство, открива грешка в предаването от специализираното логическо устройство.

DDP_022 Блокът, монтиран на превозното средство, извършва анализ на всяко получено съобщение, за да открие всяка евентуална грешка по синхронизирането, структурата на байтовете (например нарушения, които засягат началните битове и стоповите битове) или на загуба на блокировка, свързана със структурата на блоковете данни (приемане на погрешен брой байтове, погрешен байт за контролна сума).

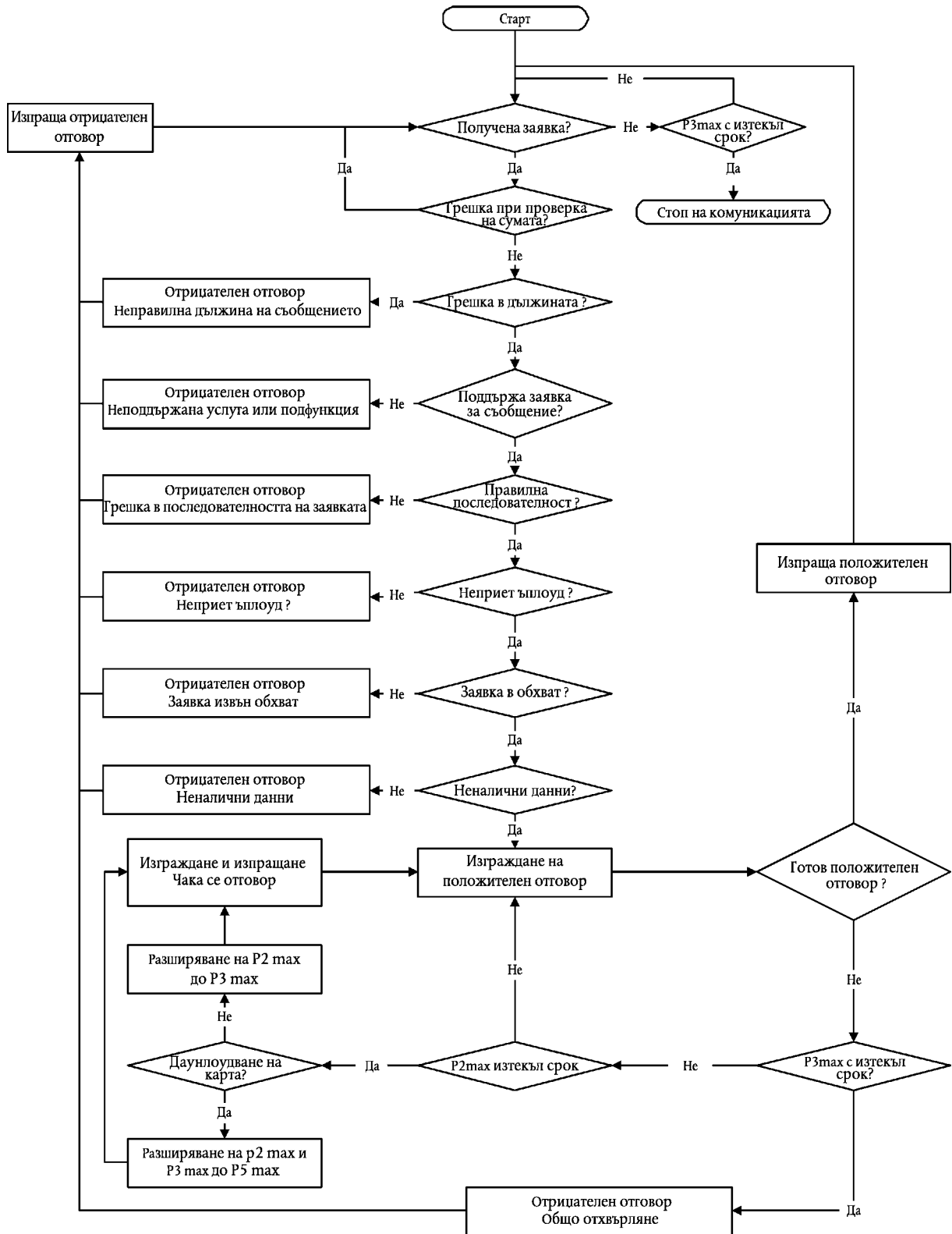
DDP_023 Ако блокът открие една от горепосочените грешки, той не изпраща никакъв отговор и не взема под внимание полученото съобщение.

DDP_024

Блокът, монтиран на превозното средство, е в състояние да открие други грешки, които засягат структурата или съдържанието на полученото съобщение (например несъвместимо съобщение), даже и ако съобщението отговаря на изискваните критерии за дължина и за контрол; в такъв случай блокът трябва да отговори на специализираното логическо устройство, като му адресира отрицателно ответно съобщение, което указва характера на грешката.

Фигура 2

Обработка на грешка на ниво на блока, монтиран на превозното средство

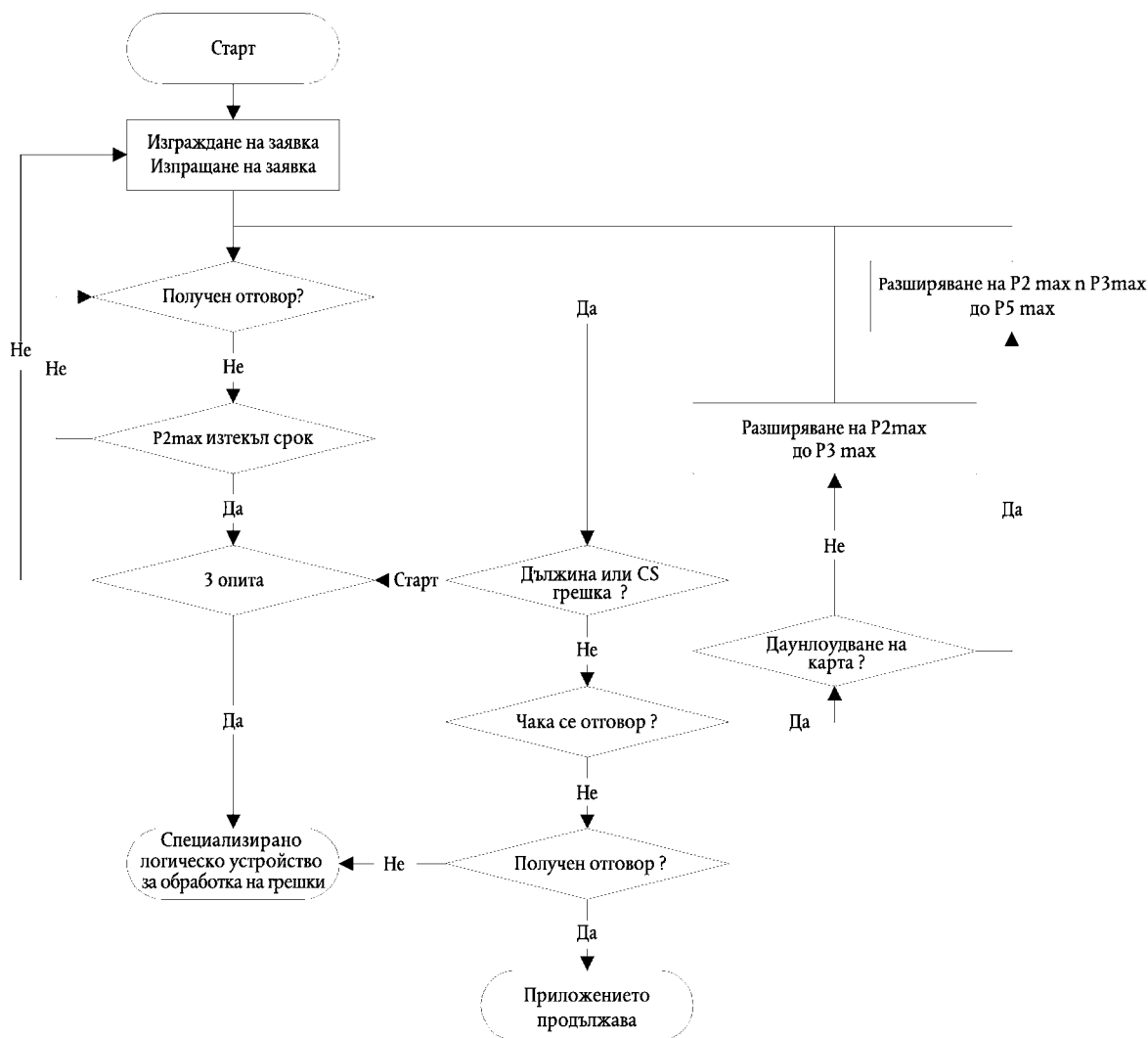


2. Специализираното логическо устройство открива грешка в предаването на данни от блока, монтиран на превозното средство.

- DDP_025 Специализираното логическо устройство извършва анализ на всяко получено съобщение, за да открие всяка евентуална грешка по синхронизирането, структурата на байтовете (например нарушения, които засягат началните битове и стоповите битове) или на загуба на блокировка, свързана със структурата на блоковете данни (приемане на погрешен брой байтове, погрешен байт за контролна сума).
- DDP_026 Ако специализираното логическо устройство открие грешки при последователността, като например погрешна инкрементация на брояча на подсъобщения, които съдържат последователно получените съобщения.
- DDP_027 Ако специализираното логическо устройство открие грешка или ако блокът, монтиран на превозното средство, не му изпрати никакъв отговор в срок от P2max, съответното съобщение за заявка ще бъде върнато максимум до три пъти на блока получател. За целите на това откриване на грешки, всяко потвърждение за получаване на някакво подсъобщение ще се разглежда като искане, което е адресирано до блока, монтиран на превозното средство.
- DDP_028 Специализираното логическо устройство трябва да изчака в продължение на отрязък от време P3min, преди да предприеме някакво предаване на данни; времето за изчакване се измерва от последната поява на бит за прекратяване, записан след откриване на въпросната грешка.

Фигура 3

Обработка на грешка на ниво на специализираното логическо устройство



2.2.6. Съдържание на съобщенията за отговор

Този параграф разглежда съдържанието на полетата за данни, които съдържат различни положителни ответни съобщения.

Елементите на информация са определени в Допълнение 1 (Речник на данни).

2.2.6.1. Положителен отговор на рекапитулация за трансфер на данни

DDP_029 Полето за данни на съобщението „Положителен отговор на рекапитулация за трансфер на данни“ трябва да дава следващите данни по реда, който следва, според изискванията на IDS 76 Hex, PRT 01 Hex и съответните критерии за разделяне и за преброяване на подсъобщенията:

Елемент на информация	Дължина (в байтове)	Коментар
MemberStateCertificate VUCertificate	194 194	Сертификат за сигурност на блока, монтиран на превозното средство
VehicleIdentificationNumber VehicleRegistrationIdentification vehicleRegistrationNation vehicleRegistrationNumber	17 1 14	Идентификация на превозното средство
CurrentDateTime	4	Текуща дата и час на блока, монтиран на превозното средство
VuDownloadablePeriod minDownloadableTime maxDownloadableTime	4 4	Период, данните за който ще бъдат прехвърляни
CardSlotsStatus	1	Характер на картите, вкарани в чезищите устройства на блока
VuDownloadActivityData downloadingTime fullCardNumber companyOrWorkshopName	4 18 36	Предишно прехвърляне на данни
VuCompanyLocksData noOfLocks ... Vu Company Locks Record lockInTime lockOutTime companyName companyAddress companyCardNumber ...	1 (98) 4 4 36 36 18	Записване на всички блокировки на предприятие. Ако този раздел е празен, се предава единствено информацията noOfLocks = 0.
VuControlActivityData noOfControls ... Vu Control Activity Record controlType controlTime controlCardNumber downloadPeriodBeginTime downloadPeriodEndTime ...	1 (31) 1 4 18 4 4	Записване на всички контролни записи в блока. Ако този раздел е празен, се предава единствено информацията noOfControl = 0
Signature	128	Подпис RSA за всички данни (с изключение на сертификатите): на идентификационния номер на превозното средство в последния байт на последния запис на контролна дейност на блока

2.2.6.2. Положителен отговор на искане за трансфер на данни относно дейностите

DDP_030 Полето за данни на съобщението „Положителен отговор на искане за трансфер на данни, свързани с дейностите“ трябва да доставя следните данни по реда, който следва, според изискванията на IDS 76 Hex, PRT 02 Hex и съответните критерии за разделяне и за преброяване на подсъобщенията:

Елемент на информация	Дължина (в байтове)	Коментар
TimeReal	4	Дата на деня, данните за който се прехвърлят
OdometerValueMidnight	3	Показание на километража за деня, данните за който се прехвърлят
VuCarGIWData		Данни относно циклите на поставяне и изваждане на картите.
noOfVuCardIWRecords	2	
...	(129)	— Ако този раздел не съдържа никакви налични данни, се предава единствено информацията noOVuCardIWRecords = 0
cardHolderName	36	
holderSurname	36	
holderFirstNames	36	
fullCardNumber	18	— Ако даден запис на поставяне/изваждане на карта в блока покрива период, започващ преди 00.00 ч. (карта, поставена предния ден) или завършващ след 24 ч. (изваждане на карта на следващия ден), този запис фигурира изцяло в директориите, които се отнасят за двата въпросни дни.
cardExpiryDate	4	
cardInsertionTime	4	
vehicleOdometerValueAtInsertion	3	
cardSlotNumber	1	
cardWithdrawalTime	4	
vehicleOdometerValueAtWithdrawal	3	
previousVehicleInfo		
vehicleRegistrationIdentification		
vehicleRegistrationNation	1	
vehicleRegistrationNumber	14	
cardWithdrawalTime	4	
manualInputFlag	1	
...		
VuActivityDailyData		Състояние на четящите устройства в 00:00 ч. и записана смяна на дейността за деня, данните за който се прехвърлят
noOfActivityChanges	2	
...		
ActivityChangeInfo	2	
...		
VuPlaceDailyWorkPeriodData		Местоположения, свързани с деня, данните за който се прехвърлят. Ако този раздел е празен, се предава единствено информацията noOfPlaceRecords = 0.
noOfPlaceRecords	1	
...	(28)	
fullCardNumber	18	
placeRecord		
entryTime	4	
entryTypeDailyWorkPeriod	1	
dailyWorkPeriodCountry	1	
dailyWorkPeriodRegion	1	
vehicleOdometerValue	3	
...		
VuSpecificConditionData		Данни относно записаните особенни условия за деня, данните за който се прехвърлят. Ако този раздел е празен, се предава единствено информацията noOfSpecificConditionRecords = 0
noOfSpecificConditionRecords	2	
...	(5)	
SpecificConditionRecord		
EntryTime	4	
specificConditionType	1	
...		
Signature	128	Подпис RSA за всички данни; за елемента Реално време в последния байт на последния запис относно особените условия

2.2.6.3. Положителен отговор на искане за трансфер на данни относно събитията и аномалиите

DDP_031 Полето за данни на съобщението „Положителен отговор на искане за трансфер на данни, свързани със събитията и аномалиите“ трябва да доставя следните данни по реда, който следва, според изискванията на IDS 76 Hex, PRT 03 Hex и съответните критерии за разделяне и за преброяване на подсъобщенията:

Елемент на информация		Дължина (в байтове)	Коментар
VuFaultData			
NoOfVuFaults		1	Всички записани аномалии или в процес на протичане в блока, монтиран на превозното средство. Ако този раздел е празен, се предава единствено информацията noOfVuFaults = 0
...		(82)	
VuFaultRecord	FaultType	1	
	FaultRecordPurpose	1	
	FaultBeginTime	4	
	FaultEndTime	4	
	CardNumberDriverSlotBegin	18	
	CardNumberCodriverSlotBegin	18	
	CardNumberDriverSlotEnd	18	
CardNumberCodriverSlotEnd	18		
...			
VuEventData			
NoOfVuEvents		1	Всички събития (с изключение на превишаването на допустимата скорост) записани или в процес на извършване в блока. Ако този раздел е празен, се предава единствено информацията noOfVuEvents = 0
...		(83)	
VuEventRecord	EventType	1	
	EventRecordPurpose	1	
	EventBeginTime	4	
	EventEndTime	4	
	CardNumberDriverSlotBegin	18	
	CardNumberCodriverSlotBegin	18	
	CardNumberDriverSlotEnd	18	
	CardNumberCodriverSlotEnd	18	
	SimilarEventsNumber	1	
...			
VuOverSpeedingControlData			
LastOverSpeedControlTime		4	Данни относно последния контрол на превишаването на допустимата скорост (стойност по подразбиране при липса на данни)
FirstOverSpeedSince		4	
NumberOfOverSpeedSince		1	
VuOverSpeedingEventData			
NoOfVuOverSpeedingEvents		1	Всички събития от типа превишаване на допустимата скорост, записани в блока. Ако този раздел е празен, се предава единствено информацията noOfVuOverSpeedingEvents = 0
...		(31)	
VuOverSpeedingEventRecord	EventType	1	
	EventRecordPurpose	1	
	EventBeginTime	4	
	EventEndTime	4	
	MaxSpeedValue	1	
	AverageSpeedValue	1	
	CardNumberDriverSlotBegin	18	
	SimilarEventsNumber	1	
...			
VuTimeAdjustmentData			
NoOfVuTimeAdjRecords		1	Всички събития, свързани със сверяването на часовника, записани в блока (извън пълното еталониране). Ако този раздел е празен, се предава единствено информацията noOfVuTimeAdjRecords = 0
...		(98)	
VuTimeAdjustmentRecord	OldTimeValue	4	
	NewTimeValue	4	
	WorkshopName	36	
	WorkshopAddress	36	
	WorkshopCardNumber	18	
...			
Signature		128	Подпис RSA за всички данни за броя на аномалиите, засягащи блока, в последния байт на последния запис за сверяването на часовника.

2.2.6.4. Положителен отговор на искане за трансфер на данни относно скоростта на превозното средство

DDP_032 Полето за данни на съобщението „Положителен отговор на искане за трансфер на данни, свързани със скоростта на превозното средство“ трябва да доставя следните данни по реда, които следва, според изискванията на IDS 76 Hex, PRT 04 Hex и съответните критерии за разделяне и за преброяване на подсъобщенията:

Елемент на информация		Дължина (в байтове)	Коментар
VuDetailedSpeedData			
NoOfSpeedBlocks		2	Всички данни, свързани с моментната скорост, записани в блока, монтиран на превозното средство (един блок със запис на скоростта за всяка минута, през която превозното средство е било в движение). По 60 моментни скорости на минута (една в секунда)
...			
VuDetailedSpeedBlock	SpeedBlockBeginDate	4	
	speedsPerSecond	60	
...			
Signature		128	Подпис RSA на всички данни за броя на блоковете с данни за скоростта в последния байт на последния блок с данни за скоростта

2.2.6.5. Положителен отговор на искане за трансфер на технически данни

DDP_033 Полето за данни на съобщението „Положителен отговор на искане за трансфер на технически данни“ трябва да доставя следните данни по реда, които следва, според изискванията на IDS 76 Hex, PRT 05 Hex и съответните критерии за разделяне и за преброяване на подсъобщенията:

Елемент на информация		Дължина (в байтове)	Коментар
VuIdentification			
vuManufacturerName		36	
vuManufacturerAddress		36	
vuPartNumber		16	
vuSerialNumber		8	
vuSoftwareIdentification			
vuSoftwareVersion		4	
vuSoftInstallationDate		4	
vuManufacturingDate		4	
vuApprovalNumber		8	
SensorPaired			
sensorSerialNumber		8	
sensorApprovalNumber		8	
sensorPairingDateFirst		4	
VuCalibrationData			Всички записи от еталониране, записани в блока, монтиран на превозното средство.
noOfVuCalibrationRecords		1	
...		(164)	
VuCalibrationRecord	calibrationPurpose	1	
	workshopName	36	
	workshopAddress	36	
	workshopCardNumber	18	
	workshopCardExpiryDate	4	
	vehicleIdentificationNumber	17	
	vehicleRegistrationIdentification		
	vehicleRegistrationNation	1	
	vehicleRegistrationNumber	14	
	wVehicleCharacteristicConstant	2	
	kConstantOfRecordingEquipment	2	
	lTyreCircumference	2	
	tyreSize	15	
	authorisedSpeed	1	
	oldOdometerValue	3	
newOdometerValue	3		
oldTimeValue	4		
newTimeValue	4		
nextCalibrationDate	4		
...			
Signature		128	Подпис RSA за всички данни за името на производителя на блока в последния байт на последния запис от еталониране на блока

2.3. Архивиране на файлове върху външно запаметяващо устройство

DDP_034 Ако дадена сесия на трансфер на данни е съдържала операция по трансфер на данни от блока, монтиран на превозното средство, специализираното логическо устройство записва в един-единствен физически файл всички данни, прехвърлени от блока по време на тази сесия за прехвърляне на данни в положителни ответни съобщения относно трансфера на данни. Съхраняването на тези данни става, като се изключат заглавните части на съобщенията, броячите на подсъобщения, празните подсъобщения и контролните суми; но то включва IDS и PRT (на първото подсъобщение при положение, че има повече подсъобщения).

3. ПРОТОКОЛ ЗА ПРЕХВЪРЛЯНЕ НА ДАННИ ОТ ТАХОГРАФСКИТЕ КАРТИ

3.1. Обхват

Този параграф съдържа описание на директното прехвърляне на данни към специализираното логическо устройство на запаметени върху тахографска карта данни. Специализираното логическо устройство не е съставна част от средата, свързана със защита от неотризиран достъп, следователно системата не извършва никаква процедура по удостоверяване на картата и на устройството.

3.2. Определения

Сесия по прехвърляне на данни: Всеки път, когато системата извършва операция по прехвърляне на данни, които са записани върху карта с вграден/и чип/ове. Тази сесия покрива цялата процедура от реинициализацията на CCI чрез PIF до дезактивирането на CCI (изваждане на картата или следващо реинициализиране).

Подписан файл за данни: Файл, записан върху CCI. Този файл се прехвърля в некодирен вид към PIF. Върху CCI файлът се сегментира и подписва, подписът се прехвърля към PIF.

3.3. Прехвърляне на данни от карта

DDP_035 Прехвърлянето на данни от тахографска карта съдържа следните операции:

- прехвърляне на общи информации, които съдържа картата в FE (елементарните файлове) ICC и IC. Тези информации с незадължителен характер не са защитени от никакъв цифров подпис,
- прехвърляне на елементарните файлове FE Card_Download и. Тези информации не са защитени от никакъв цифров подпис,

Тези файлове трябва задължително да се прехвърлят по време на всяка сесия за прехвърляне на данни.

- прехвърляне на данни от други елементарни файлове с данни за приложение (в специализирания файл Tachograph), освен елементарния файл Card_Download. Тези информации са защитени с цифров подпис,
- трябва да се прехвърлят задължително елементарните файлове Application_Identification и ID по време на всяка сесия FE Application_Identification и ID за прехвърляне на данни,
- когато се извършва прехвърляне на данни от карта на водач, е необходимо също да бъдат задължително прехвърлени следните елементарни файлове:

- Events_Data,
- Faults_Data,
- Driver_Activity_Data,
- Vehicles_Used,
- Places,
- Control_Activity_Data,
- Specific_Conditions.

- когато се извършва прехвърляне на данни от карта на водач, е целесъобразно да се актуализира датата на последното прехвърляне на данни във LastCardDownload date in FE Card_Download,
- когато се извършва прехвърляне на данни от цехова карта, е необходимо да се реинициализира броячът за еталониране, чиито показания са записани във FE Card_Download.

3.3.1. Последователност на инициализиране

DDP_036 Специализираното логическо устройство трябва да стартира последователността, както следва:

Карта	Посока	ESI/PIF	Значение/Бележки
	↩	Реинициализация на хардуера	
RAR	↪		

Потребителят има възможност да прибере до SPP, за да премине към по-висока пропускателна скорост, при условие, че CCI може да осигури нейното прилагане.

3.3.2. Последователност за прехвърляне на неподписани файлове с данни

DDP_037 Последователността на прехвърляне на елементарните файлове ICC, IC, Card_Certificate и CA_Certificate има следния вид:

Карта	Посока	ESI/PIF	Значение/Бележки
	↩	SELECT FILE	Селектиране посредством идентификаторите на файла
OK	↪		
	↩	READ BINARY	Ако обемът на данните, които се съдържат във файла, е по-голям от капацитета на буферната памет на четящото устройство или на картата, командата трябва да се повтори, докато данните, които се съдържат във файла, бъдат извлечени в пълния си обем
Данни OK	↪	Съхраняване на данните върху SME	В съответствие с параграф 3.4 Формат за архивиране на данни

Забележка: преди да се избере елементарният файл Card_Certificate, е целесъобразно да се избере предварително тахографското приложение (избирането се извършва от IDA).

3.3.3. Последователност за прехвърляне на подписани файлове с данни

DDP_038 Трябва да се прибере да следната последователност при извършването на процедура по прехвърлянето на данни от всеки от следните файлове, които са придружени от техния подпис:

Карта	Посока	ESI/PIF	Значение/Бележка
	↩	SELECT FILE	
OK	↪		
	↩	PERFORM HASH OF FILE	Позволява да се изчисли стойността на сегментирането по отношение на съдържанието на избрания файл, като се прилага алгоритъмът за сегментиране, предписан съгласно Допълнение 11. Тази команда не е команда ISO
Изчислява се сегментирането на файла и се записва временно приетата стойност за сегментирането			
OK	↪		
	↩	READ BINARY	Ако обемът на данните, които се съдържат във файла, е по-голям от капацитета на буферната памет на четящото устройство или на картата, командата трябва да се повтори, докато данните, които се съдържат във файла, бъдат извлечени в пълния си обем
Данни OK	↪	Съхраняват се данните в SME	В съответствие с параграф 3.4 Формат за архивиране на данни
	↩	PSO: COMPUTE DIGITAL SIGNATURE	
Изпълнение на операция за сигурност „Изчисление на електронен подпис“ с помощта на временно записаната стойност за сегментиране			
Подпис OK	↪	Добавяне на данни към тези, които са съхранени преди това върху SME	В съответствие с параграф 3.4 Формат за архивиране на данни

3.3.4. Последователност за реинициализиране на брояч за еталониране

DDP_039 Последователността на реинициализиране на брояча NoOfCalibrationsSinceDownload nell'EF Card_Download на дадена цехова карта, има следния вид:

Карта	Посока	ESI/PIF	Значение/Забележки
	↶	Select File EF Card_Download	Селектиране посредством идентификаторите на файла
OK	↶		
	↶	UPDATE BINARY NoOfCalibrations- SinceDownload = '00 00'	
Реинициализира броя на прехвърлянията на данни от картата			
OK	↷		

3.4. Формат на архивиране на данните

3.4.1. Въведение

DDP_040 Прехвърлените данни трябва да бъдат записани при следните условия:

- записването на данните трябва да не зависи от използвания код. С други думи, редът, по който се представят байтовете и битовете, които съставляват тези байтове, трябва да бъде запазен по време на операцията по архивирането, извършена след трансфера им от картата,
- всички данни, които са прехвърлени от картата в рамките на една сесия за прехвърляне, трябва да бъдат записани в един и същ файл в SME.

3.4.2. Формат на файловете

DDP_041 Форматът на файловете представлява конкатенация на няколко обекта VLB.

DDP_042 Тагът, свързан с елементарния файл, трябва да приеме формата на IDF на файла, придружен от допълнението „00“.

DDP_043 Тагът, свързан с подписа на един елементарен файл, трябва да приеме формата на IDF на файла, придружен от допълнението „01“.

DDP_044 Дължината отговаря на стойност, изразена от два байта. Тази стойност определя броя на байтовете, предназначени за полето стойност. Стойността „FF FF“, която съдържа полето дължина, се запазва за по-късно използване.

DDP_045 По липса на прехвърляне на данни, никаква информация за определен файл не се запазва (няма наличие на таг и няма дължина нула).

DDP_046 Всеки подпис трябва да бъде запазен под формата на обект VLB веднага след обекта VLB, който съдържа данните, събрани в разглеждания файл.

Определения	Значение	Дължина
IDF (2 байта) „00“	Таг за FE (IDF)	3 байта
IDF (2 байта) „01“	Таг за подпис FE	3 байта
xx xx	Дължина на полето стойност	2 байта

Пример за данни, записани във файл за прехвърляне в SME:

Таг	Дължина	Стойност
00 02 00	00 11	Данни от елементарния файл ICC
01 00 00	00 02	Данни от елементарния файл Card_Certificate
		...
05 05 00	0A 2E	Данни от елементарния файл Vehicles_Used
05 05 01	00 80	Подпис на елементарния файл Vehicles_Used

4. ПРЕХВЪРЛЯНЕ НА ДАННИ ОТ ТАХОГРАФСКА КАРТА С ПОМОЩТА НА БЛОК, МОНТИРАН НА ПРЕВОЗНОТО СРЕДСТВО

- DDP_047 Блокът, монтиран на превозното средство, трябва да позволява прехвърлянето на съдържанието на карта на водач, която е поставена в четящото устройство на свързано с него специализирано логическо устройство.
- DDP_048 Това специализираното логическо устройство трябва да изпрати съобщение „Искане за трансфер на данни от типа прехвърляне на данни от карта“ до блока, монтиран на превозното средство, за да се стартира този режим на предаване на данни (виж 2.2.2.9).
- DDP_049 На този етап блокът, монтиран на превозното средство, трябва да извърши цялостното прехвърляне на данни от картата, файл по файл, в съответствие с протокола за прехвърляне от карта, дефиниран в параграф 3, както и да извърши изпращане към специализираното логическо устройство на всички данни, които са извлечени от картата в съответния файлов формат VLB (виж 3.4.2) и са формирани в границите на съобщение „Положителен отговор на искане за трансфер на данни“.
- DDP_050 Специализираното логическо устройство трябва да извлече данни от картата, включени в съобщението „Положителен отговор на искане за трансфер на данни“ (като премахне всички заглавни части, IDS, PRT, броячи на подсъобщения и контролни суми) и да ги запише във физически файл в съответствие с описанието, направено в параграф 2.3.
- DDP_051 След което, в зависимост от случая, блокът, монтиран на превозното средство, трябва да извърши актуализиране на файла с данните за контролните дейности или да извърши прехвърляне на file ControlActivity Data or file Card_Download данни от карти върху картата на водача.
-

Допълнение 8

ПРОТОКОЛ ЗА ЕТАЛОНИРАНЕ

СЪДЪРЖАНИЕ

1.	Въведение	172
2.	Терминология, определения и изходна база	172
3.	Общ преглед на услугите	172
3.1.	Услуги на разположение	172
3.2.	Кодове за отговор	173
4.	Услуги за връзка	173
4.1.	Услуга StartCommunication	173
4.2.	Услуга StopCommunication	175
4.2.1.	Описание на съобщенията	175
4.2.2.	Структура на съобщенията	176
4.2.3.	Определяне на параметрите	177
4.3.	Услуга TesterPresent	177
4.3.1.	Описание на съобщението	177
4.3.2.	Формат на съобщението	177
5.	Услуги за управление	178
5.1.	Услуги StartDiagnosticSession	178
5.1.1.	Описание на съобщенията	178
5.1.2.	Структура на съобщенията	179
5.1.3.	Определяне на параметрите	180
5.2.	Услуга SecurityAccess	180
5.2.1.	Описания на съобщенията	180
5.2.2.	Структура на съобщенията - SecurityAccessRequest#1	181
5.2.3.	Структура на съобщенията - SecurityAccess - sendKey	182
6.	Услуги за предаване на данни	183
6.1.	Услуга ReadDataByIdentifier	183
6.1.1.	Описание на съобщенията	183
6.1.2.	Структура на съобщенията	183
6.1.3.	Определяне на параметрите	184
6.2.	Услуга WriteDataByIdentifier	185
6.2.1.	Описание на съобщенията	185
6.2.2.	Структура на съобщенията	185
6.2.3.	Определяне на параметрите	186
7.	Контрол на тестовите импулси — Функционален блок за контрол на входно/изходните данни...	186
7.1.	Услуга InputOutputControlByIdentifier	186

7.1.1.	Описание на съобщенията	186
7.1.2.	Структура на съобщенията	187
7.1.3.	Определяне на параметрите	188
8.	Структури на записите с данни	189
8.1.	Диапазони от предадени параметри	189
8.2.	Структури на записите с данни	190

1. ВЪВЕДЕНИЕ

Това допълнение разглежда начините на обмен на данни между тестова апаратура и блок, монтиран на превозното средство, посредством линията К. Тази линия представлява неразделна част от интерфейса за еталониране, който е описан в допълнение 6. Настоящото допълнение разглежда също контрола на линията на входно/изходната сигнализация, който се извършва на нивото на конектора за еталониране.

Установяването на връзките по линия К се описва в раздел 4 „Услуги за връзка“.

Настоящото допълнение се основава на концепцията за „сесии за диагностика“ за определяне на обхвата на контрола на линията К в зависимост от развитието на начините на обмен. Сесията по подразбиране е „StandardDiagnosticSession“, при която е възможно всички данни, които се съдържат в блока, монтиран на превозното средство, да бъдат извлечени от него, но никакви данни не могат да бъдат записани в този блок.

Избирането на опцията „Сесия за диагностика“ е обект на подробно описание в раздел 5 „Услуги за управление“.

CPR_001 „ECUProgrammingSession“ разрешава въвеждането на данни в блока, монтиран на превозното средство. Освен това, в случай, когато се въвеждат данни за еталониране (изисквания 097 и 098), блокът, монтиран на превозното средство, трябва работи в режим ЕТАЛОНИРАНЕ.

Трансферът на данни посредством линията К е обект на подробно описание в Раздел 6 „Услуги за прехвърляне на данни“. Форматите на предадените данни са описани подробно в Раздел 8 „Структури на записите с данни“.

CPR_002 Сесията за настройка „ECUAdjustmentSession“ позволява избиране на режим на функциониране за линията за входно/изходната сигнализация за еталониране посредством интерфейса с линията К. Контролът на линията за входно/изходната сигнализация за еталониране е обект на подробно описание в Раздел 7 „Контрол на тестовите импулси — Функционален блок за контрол на входно/изходните импулси“.

CPR_003 В настоящия документ тестовата апаратура притежава следния адрес: „tt“. Въпреки че някои адреси на тестовата апаратура имат привилегировано положение, блокът, монтиран на превозното средство, трябва да реагира правилно на всеки адрес на тестовата апаратура. Физическият адрес на блока, монтиран на превозното средство, се изобразява по следния начин: 0xEE.

2. ТЕРМИНОЛОГИЯ, ОПРЕДЕЛЕНИЯ И ИЗХОДНА БАЗА

Протоколите, съобщенията и кодовете за грешка се основават главно върху настоящия вариант на проекта за стандарт ISO 14229-1 (Пътни превозни средства — системи за диагностика — Част I: служби за диагностика, версия 6 от 22 февруари 2001 г.).

Кодиранията на байтове и други шестнадесетични стойности се използват по време на определянето на идентификаторите на услуги, при изработването на служебните заявки и отговори и при конфигурирането на стандартните параметри.

Терминът „тестова апаратура“ отправя към оборудването, което се използва за въвеждане на данни за програмиране/еталониране в блока.

Термините „клиент“ и „сървър“ се отнасят съответно за тестовата апаратура и за блока, монтиран на превозното средство.

Терминът UCE означава „блок за електронно управление“ и се прилага за блока, монтиран на превозното средство.

Изходна база:

ISO 14230-2: Пътни превозни средства — Системи за диагностика — Протокол с ключови думи 2000 — Част 2: Слой за връзка между данните. Първо издание: 1999 г. Пътни превозни средства — Системи за диагностика

3. ОБЩ ПРЕГЛЕД НА УСЛУГИТЕ

3.1. Услуги на разположение

Следващата таблица представя общ преглед на услугите, определени в настоящия документ, които апаратурата за контрол трябва да може да осигурява.

CPR_004 Тази таблица посочва кои са услугите на разположение по време на активна сесия за диагностика.

— първата колона посочва услугите, които са на разположение,

— втората колона посочва номера на параграфа, в който се прави подробно описание на разглежданата услуга в настоящото допълнение,

- третата колона посочва стойността, която е определена за разглеждания идентификатор на услуга в съобщенията за искане на услуга,
- четвъртата колона уточнява кои са услугите на „StandardDiagnosticSession“ (SD), чието използване в блока, монтиран на превозното средство, е абсолютно необходимо,
- петата колона уточнява кои са услугите на „ECUAdjustmentSession“ (ECUAS), чието използване е абсолютно необходимо, за да се позволи извършване на адекватен контрол на линията за входно/изходната сигнализация на равнището на конектора за еталониране, монтиран на предния панел на блока, монтиран на превозното средство,
- шестата колона уточнява кои са услугите на „ECUProgrammingSession“ (ECUPS), чието използване в блока, монтиран на превозното средство, е абсолютно необходимо за извършване на програмирането на експлоатационните параметри в блока.

Таблица 1

Таблица — рекапитулация на стойностите, които са определени за идентификаторите на услуги

Име на услугите за диагностика	Параграфи	Стойности на идентификаторите на услуги	Сесии за диагностика		
			SD	ECUAS	ECUPS
StartCommunication	4.1	81	■	■	■
StopCommunication	4.2	82	■		
TesterPresent	4.3	3E	■	■	■
StartDiagnosticSession	5.1	10	■	■	■
SecurityAccess	5.2	27	■	■	■
ReadDataByIdentifier	6.1	22	■	■	■
WriteDataByIdentifier	6.2	2E			■
InputOutputControlByIdentifier	7.1	2F		■	

■ Този знак напомня за задължителния характер на услугата по време на тази сесия за диагностика.
Няма символ, който да посочва, че изпълнението на съответната услуга не е разрешено по време на тази сесия за диагностика.

3.2. Кодове за отговор

Кодовете за отговор се определят за всяка услуга.

4. УСЛУГИ ЗА ВРЪЗКА

Някои услуги са необходими за установяването и за поддържането на връзките. Те не се появяват в слоя на приложението. Таблицата, която следва, посочва различните услуги, които са на разположение:

Таблица 2

Услуги за връзка

Названия на услугите	Описание
StartCommunication	Клиентът иска започване на сесия за връзка с един или няколко сървъра.
StopCommunication	Клиентът иска прекъсване на текущата сесия за връзка.
TesterPresent	Клиентът указва на сървъра, че е той е все още на линия.

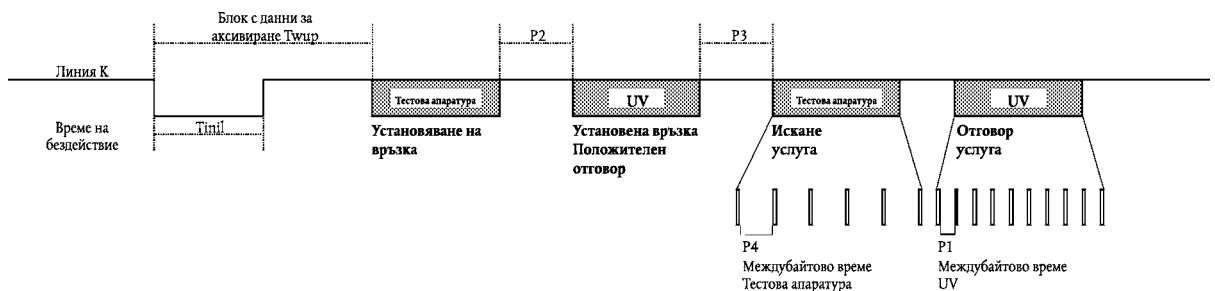
CPR_005 Услугата StartCommunication се използва за установяване на връзка. Изпълнението на всяка услуга предполага установяването на връзка и избирането на параметри, които са адаптирани за желания режим на експлоатация.

4.1. Услуга StartCommunication

CPR_006 При получаването на примитив за указване StartCommunication блокът, монтиран на превозното средство, проверява дали установяването на необходимата вътрешна връзка може да се осъществи при наличните условия. Условието за установяване на вътрешна връзка са обект на подробно описание в документ ISO 14230-2.

CPR_007 След това блокът, монтиран на превозното средство, трябва да изпълни всички необходими действия за установяването на необходимата вътрешна връзка и да изпрати примитив за отговор StartCommunication с избраните параметри за положителен отговор.

- CPR_008 Ако един вече инициализиран блок, монтиран на превозното средство (и влязъл в сесия за диагностика), получи нова команда за установяване на вътрешна връзка (например поради повторно стартиране при грешка на нивото на тестовата апаратура), това искане трябва да бъде прието и блокът да бъде реинициализиран.
- CPR_009 Ако по една или друга причина установяването на вътрешната връзка се окаже невъзможно, блокът трябва да продължи да работи при същите условия, каквито са съществували непосредствено преди опита за установяване на вътрешна връзка.
- CPR_010 Съобщението за искане за установяване на връзка трябва да се адресира физически.
- CPR_011 Инициализирането на блока, монтиран на превозното средство за осигуряването на услугите, се осъществява по метода за бързото инициализиране:
- време на активност/бездействие, предхождащо всяка дейност,
 - предаване на конфигурация за инициализиране от тестовата апаратура,
 - всички необходими информации за установяването на връзка се съдържат в отговора на блока, монтиран на превозното средство.
- CPR_012 След инициализиране,
- стойностите, които са определени за всички параметри за връзка, са описани в таблица 4 в зависимост от ключовите байтове,
 - блокът изчаква първото искане, изпратено от тестовата апаратура,
 - блокът работи в режим за диагностика по подразбиране, тоест в режим StandardDiagnosticSession,
 - линията за входно/изходната сигнализация за еталониране се намира в режим на експлоатация по подразбиране, тоест е дезактивирана.
- CPR_014 Пропускателната скорост на данните по линията K е равна на 10 400 бода.
- CPR_016 Бързата инициализация се задейства от тестовата апаратура, която изпраща блок с данни за активиране (Wup) по линията K. Този блок започва след период на бездействие на линията K, последван от времеви период Tinil. Тестовата апаратура изпраща първия бит на StartCommunicationService след времеви период Twup, последван от първия низходящ фронт на импулса.



- CPR_017 Стойностите за синхронизиране, определени за бързото инициализиране и за връзките по принцип, са обект на подробно описание в следващите таблици. Що се отнася до времето на бездействие, могат да се разгледат три възможности:
- първо предаване на данни след включване под напрежение, T. бездействие = 300 милисекунди,
 - след преустановяване със StopCommunicationService, T. бездействие = P3 min,
 - след прекъсване на връзка поради превишаване на определеното време P3 max, T бездействие = 0.

Таблица 3

Стойности за синхронизация, определени за бързото инициализиране

Параметър	Стойност min	Стойност max
Tinil	25 ± 1 ms	24 ms
Twup	50 ± 1 ms	49 ms

Таблица 4

Стойности, определени за параметрите за синхронизация на връзките

Параметър за синхронизация	Синхронизация	Допустими минимални стойности (ms)	Допустими максимални стойности (ms)
		min.	max.
P1	Междубайтово време, който трябва да се спазва в очакването на отговор от страна на блока, монтиран на превозното средство	0	20
P2	Отрязък от време между едно искане от тестовата апаратура и един или два отговора от блока, монтиран на превозното средство	25	250
P3	Отрязък от време между края на отговорите на блока и началото на ново искане, изпратено от тестовата апаратура	55	5000
P4	Междубайтово време, което трябва да се спазва в очакването на искане, изпратено от тестовата апаратура	5	20

CPR_018 Структурата на изпратените съобщения в рамките на бърза инициализация е обект на подробно описание в таблиците, които следват.

Таблица 5

Съобщение за искане за установяване на връзка

Байт #	Название на параметъра	Стойност hex.	Мнемоничен код
#1	Байт за структура — физическо адресиране	81	FMT
#2	Байт за адреса на набелязаното състояние	EE	CIB
#3	Байт за адреса на източника	tt	SRC
#4	ID на услугата „Искане за установяване на връзка“	81	DEC
#5	Байт за контролна сума	00-FF	TC

Таблица 6

Съобщение за положителен отговор на искане за установяване на връзка

Байт #	Название на параметъра	Стойност hex.	Мнемоничен код
#1	Байт за структура — физическо адресиране	80	FMT
#2	Байт за адреса на набелязаното състояние	tt	CIB
#3	Байт за адреса на източника	EE	SRC
#4	Байт за допълнителна дължина	03	LON
#5	ID на услугата „Положителен отговор на искане за установяване на връзка“	C1	RPDEC
#6	Ключов байт 1	EA	OC1
#7	Ключов байт 2	8F	OC2
#8	Байт за контролна сума	00-FF	TC

CPR_019 Няма отрицателен отговор на съобщението за искане за установяване на връзка. Поради липса на положително съобщение за изпращане блокът не се инициализира, никакви данни не се предават и системата остава в режим на нормална експлоатация.

4.2. Услуга StopCommunication

4.2.1. Описание на съобщенията

Тази услуга, която обхваща слоя, свързан с осъществяването на връзка, цели да сложи край на всяка сесия за връзка.

CPR_020 При получаването на примитив за указване StopCommunication блокът, монтиран на превозното средство, проверява дали наличните условия позволяват прекъсването на текущата връзка. Ако случаят е именно такъв, блокът трябва да извърши всички изисквани операции, за да прекрати връзката.

- CPR_021 Ако е възможно прекъсване на връзката, блокът трябва да изпрати примитив за отговор StopCommunication, като използва избраните параметри за положителен отговор, преди да прекрати връзката.
- CPR_022 Ако по една или друга причина се окаже невъзможно прекратяването на определената връзка, блокът трябва да изпрати примитив за отговор StopCommunication, като прибегне до използването на избрания параметър за отрицателен отговор.
- CPR_023 Ако блокът открие надвишаване на времетраенето P3max, връзката се прекратява, без да се придружава от изпращане на какъвто и да е примитив за отговор.

4.2.2. Структура на съобщенията

- CPR_024 Структурата на съобщенията, свързани с примитивите StopCommunication, е обект на подробно описание в таблиците, които следват.

Таблица 7

Съобщение за искане за прекратяване на връзка

Байт #	Название на параметъра	Стойност hex.	Мнемоничен код
#1	Байт за структура — физическо адресиране	80	FMT
#2	Байт за адреса на набелязаното състояние	EE	CIB
#3	Байт за адреса на източника	tt	SRC
#4	Байт за допълнителна дължина	01	LON
#5	ID на услугата „Искане за прекратяване на връзка“	82	DIC
#6	Байт за контролна сума	00-FF	TC

Таблица 8

Съобщение за положителен отговор на искане за прекъсване на връзка

Байт #	Название на параметъра	Стойност hex.	Мнемоничен код
#1	Байт за структура — физическо адресиране	80	FMT
#2	Байт за адреса на набелязаното състояние	tt	CIB
#3	Байт за адреса на източника	EE	SRC
#4	Байт за допълнителна дължина	01	LON
#5	ID на услугата „Положителен отговор на искане за прекратяване на връзка“	C2	RPDIC
#6	Байт за контролна сума	00-FF	CS

Таблица 9

Съобщение за отрицателен отговор на искане за прекъсване на връзка

Байт #	Название на параметъра	Стойност hex.	Мнемоничен код
#1	Байт за структура — физическо адресиране	80	FMT
#2	Байт за адреса на набелязаното състояние	tt	CIB
#3	Байт за адреса на източника	EE	SRC
#4	Байт за допълнителна дължина	03	LON
#5	ID на услугата Отрицателен отговор	7F	RN
#6	ID на услугата „Искане за прекратяване на връзка“	82	DIC
#7	Код за отговор = generalReject	10	CR_GR
#8	Байт за контролна сума	00-FF	TC

4.2.3. **Определяне на параметрите**

Тази услуга не налага определяне на никакъв параметър.

4.3. Услуга TesterPresent

4.3.1. **Описание на съобщението**

Услугата TesterPresent се използва от тестовата апаратура, за да посочи на сървъра, че тя все още е на разположение, с цел да се попречи на автоматичното връщане на сървъра към режим на нормална работа и да се избегне евентуалното прекъсване на връзката. Тази услуга, изпращана периодично, поддържа активна сесията за диагностика и връзката, като нулира брояча P3 при всяко искане на услуга.

4.3.2. **Формат на съобщението**

CPR_079 Структурата на съобщенията, свързани с примитивите TesterPresent, е обект на подробно описание в таблиците, които следват.

Таблица 10

Съобщение за искане за указване на наличие на тестова апаратура

Байт #	Название на параметъра	Стойност hex.	Мнемоничен код
#1	Байт за структура — физическо адресиране	80	FMT
#2	Байт за адреса на набеязаното състояние	EE	CIB
#3	Байт за адреса на източника	tt	SRC
#4	Байт за допълнителна дължина	02	LON
#5	ID на услугата „Искане за указване на присъствие на тестова апаратура“	3E	IPAE
#6	Подфункция = responseRequired (изискван отговор) [да не]	01	RESPREQ_Y
		02	RESPREQ_NO
#7	Байт за контролна сума	00-FF	TC

CPR_080 Ако параметърът responseRequired (искан отговор) е „да“, сървърът ще отговори с последващо положително съобщение. Ако параметърът е „не“, сървърът не изпраща отговор.

Таблица 11

Съобщение за положителен отговор на индикатора за наличие на тестова апаратура

Байт #	Название на параметъра	Стойност hex.	Мнемоничен код
#1	Байт за структура — физическо адресиране	80	FMT
#2	Байт за адреса на набеязаното състояние	tt	CIB
#3	Байт за адреса на източника	EE	SRC
#4	Байт за допълнителна дължина	01	LON
#5	ID на услугата „Положителен отговор на индикатора за наличие на тестова апаратура“	7E	RPIPAE
#6	Байт за контролна сума	00-FF	TC

CPR_081 Услугата приема следните кодове за отрицателен отговор:

Таблица 12

Съобщение за отрицателен отговор на индикатора за наличие на тестова апаратура

Байт #	Название на параметъра	Стойност hex.	Мнемоничен код
#1	Байт за структура — физическо адресиране	80	FMT
#2	Байт за адреса на набелязаното състояние	tt	CIB
#3	Байт за адреса на източника	EE	SRC
#4	Байт за допълнителна дължина	03	LON
#5	ID на услугата Отрицателен отговор	7F	RN
#6	ID на услугата „Искане на индикатора за наличие“е	3E	TP
#7	Код за отговор = [SubFunctionNotSupported-InvalidFormatincorrectMessageLength]	12 13	RC_SFNS_IF RC_IML
#8	Байт за контролна сума	00-FF	CS

5. УСЛУГИ ЗА УПРАВЛЕНИЕ

Таблицата, която следва, представя опис на различните услуги, които са на разположение:

Таблица 13

Услуги за управление

Наименование на услугите	Описание
StartDiagnosticSession	Клиентът иска отваряне на сесия за диагностика с определен блок, монтиран на превозното средство
SecurityAccess	Клиентът иска достъп до някои функции, които са запазени за оторизирани потребители

5.1. Услуга StartDiagnosticSession

5.1.1. *Описание на съобщенията*

CPR_025 Услугата StartDiagnosticSession позволява активиране на различни сесии за диагностика в сървъра. Сесията за диагностика разрешава използването на специфичен набор от услуги в съответствие с указанията, които са дадени в таблица 17. Една сесия може да позволи извършването на специфични услуги на производителя на превозното средство, които не фигурират в настоящия документ. Правилата за тяхното извършване отговарят на следните изисквания:

- винаги има само една текуща сесия в блока, монтиран на превозното средство,
- блокът винаги отваря стандартната сесия за диагностика, когато е включен под напрежение, ако няма отворена друга сесия за диагностика, стандартната сесия за диагностика остава отворена толкова дълго време, колкото време блокът е под напрежение,
- ако една вече отворена сесия за диагностика е поискана от тестовата апаратура, блокът изпраща съобщение за положителен отговор,
- когато тестовата апаратура поиска нова сесия за диагностика, блокът, монтиран на превозното средство, изпраща първоначално съобщение за положителен отговор на искането за отваряне на сесията за диагностика, преди новата сесия да бъде отворена в блока. Ако блокът не е успял да отвори исканата нова сесия за диагностика, той изпраща съобщение за отрицателен отговор на искането за отваряне на сесията за диагностика и текущата сесия продължава.

CPR_026 Започването на сесия за диагностика може да се осъществи само при условие, че е била установена предварително връзка между клиента и блока, монтиран на превозното средство.

CPR_027 Параметрите за синхронизиране, определени в таблица 4, се активират след успешното изпълнение на услуга StartDiagnosticSession при положение, че съобщението за заявка съдържа параметъра на сесията за диагностика „Session standard“ и ако предварително е била активна друга сесия за диагностика.

5.1.2. Структура на съобщенията

CPR_028 Структурата на съобщенията, свързани с примитивите StartDiagnosticSession, е обект на подробно описание в следващите таблици.

Таблица 14

Съобщение за искане за започване на сесия за диагностика

Байт #	Название на параметъра	Стойност hex.	Мнемоничен код
#1	Байт за структура — физическо адресиране	80	FMT
#2	Байт за адреса на набелязаното състояние	EE	CIB
#3	Байт за адреса на източника	tt	SRC
#4	Байт за допълнителна дължина	02	LON
#5	ID на услугата „Искане за започване на сесия за диагностика“	10	DLSD
#6	Сесия за диагностика = [стойност от таблица 17]	xx	SD_...
#7	Байт за контролна сума	00-FF	TC

Таблица 15

Съобщение за положителен отговор на искане за започване на сесия за диагностика

Байт #	Название на параметъра	Стойност hex.	Мнемоничен код
#1	Байт за структура — физическо адресиране	80	FMT
#2	Байт за адреса на набелязаното състояние	tt	CIB
#3	Байт за адреса на източника	EE	SRC
#4	Байт за допълнителна дължина	02	LON
#5	ID на услугата „Положителен отговор на искане за започване на сесия за диагностика“	50	RPDLSD
#6	Сесия за диагностика = [същата стойност като байт #6 от таблица 14]	xx	SD_...
#7	Байт за контролна сума	00-FF	TC

Таблица 16

Съобщение за отрицателен отговор на искане за започване на сесия за диагностика

Байт #	Название на параметъра	Стойност hex.	Мнемоничен код
#1	Байт за структура — физическо адресиране	80	FMT
#2	Байт за адреса на набелязаното състояние	tt	CIB
#3	Байт за адреса на източника	EE	SRC
#4	Байт за допълнителна дължина	03	LON
#5	ID на услугата Отрицателен отговор	7F	RN
#6	ID на услугата „Искане за започване на сесия за диагностика“	10	DLSD_...
#7	Код за отговор = [subFunctionNotSupported - (неподдръжана подфункция) ^(a) incorrectMessageLength - (неправилна дължина на съобщение) ^(b) conditionsNotCorrect - (неправилни условия) ^(c)]	12 13 22	RC_SFNS RC_IML RC_CNC
#8	Байт за контролна сума	00-FF	TC

^(a) Въведената стойност в байт #6 на съобщението за искане не се взема под внимание, тоест не е в таблица 17.

^(b) Дължината на съобщението е неправилна.

^(c) Критериите за искане за започване на сесия за диагностика (StartDiagnosticSession) не са изпълнени.

5.1.3. Определение на параметрите

CPR_029 Услугата StartDiagnosticSession използва параметъра „Сесия за диагностика“ (SDC) за избор на особен режим на поведение на сървъра или на сървърите. Сесиите за диагностика, които следват, са уточнени в настоящия документ:

Таблица 17

Определяне на стойностите, използвани при сесиите за диагностика

Hex	Описание	Мнемоничен код
81	Стандартна сесия за диагностика (StandardDiagnosticSession) Тази сесия за диагностика позволява да се активират всички услуги, посочени в таблица 1, колона 4, „SD“. Тези услуги разрешават изтеглянето на данни, записани в сървър (блок, монтиран на превозното средство). Тази сесия за диагностика става активна след успешна фаза на инициализиране между клиент (тестовата апаратура) и сървър (блока, монтиран на превозното средство). Възможно е тази сесия да бъде заменена от други други сесии за диагностика, специфицирани в този раздел.	SD
85	Сесия за програмиране на UCE (ECUProgrammingSession) Тази сесия за диагностика позволява да се активират всички услуги, изредени в таблица 1, колона 6, „ECUPS“. Тези услуги поемат осигуряването на програмирането на паметта на сървър (блок, монтиран на превозното средство). Възможно е тази сесия да бъде заменена от други други сесии за диагностика, специфицирани в този раздел.	SPUCE
87	Сесия за настройка на UCE (ECUAdjustmentSession) Тази сесия за диагностика позволява да се активират всички услуги, посочени в таблица 1, колона 5, „ECUAS“. Тези услуги поемат осигуряването на контрола на входно/изходните данни на сървър (блок, монтиран на превозното средство). Възможно е тази сесия да бъде заменена от други други сесии за диагностика, специфицирани в този раздел.	SRUCE

5.2. Услуга SecurityAccess

За да може да се извърши записването на данните за еталониране или да се получи достъп до входно/изходната линия за еталониране, е необходимо блокът, монтиран на превозното средство, да работи в режим ЕТАЛОНИРАНЕ. Освен поставянето на валидна цехова карта в съответното четиращо устройство на блока, е задължително да се въведе съответният индивидуален идентификационен номер в блока, за да се получи достъп до режима ЕТАЛОНИРАНЕ.

Услугата SecurityAccess позволява въвеждане на индивидуалния идентификационен номер и посочване на тестовата апаратура дали блокът работи или не в режим ЕТАЛОНИРАНЕ.

Системата позволява използване на други методи за въвеждане на този индивидуален идентификационен номер.

5.2.1. Описания на съобщенията

Услугата SecurityAccess съдържа изпълнение на съобщение „requestSeed“ (искане за стартиране на удостоверяване), което при необходимост се последва от съобщението „sendKey“ (искане за изпращане на ключ). Услугата SecurityAccess трябва да бъде изпълнена след услугата StartDiagnosticSession.

CPR_033 Тестовата апаратура трябва да прибегне до използването на съобщение SecurityAccess „requestSeed“, за да провери дали блокът е в готовност да приеме индивидуалния идентификационен номер.

CPR_034 Ако блокът, монтиран на превозното средство, е вече в режим ЕТАЛОНИРАНЕ, той отговаря на искането, което му е отправено чрез изпращане на „Начало на удостоверяване“ от 0x0000, като използва услугата „Положителен отговор на искането SecurityAccess“.

CPR_035 Ако блокът е готов да приеме даден индивидуален номер за извършването на операция по проверка чрез цехова карта, той трябва да отговори на искането, което му е отправено, чрез изпращане на „Начало на удостоверяване“ със стойност, по-висока от 0x0000, като използва услугата „Положителен отговор на искането SecurityAccess“.

CPR_036 Ако блокът не е готов да приеме даден индивидуален идентификационен номер, изпратен от тестовата апаратура, защото поставената цехова карта в четиращото устройство не е валидна, защото в това устройство няма никаква карта или защото блокът изчаква предаването на изисквания индивидуален идентификационен номер по друг начин, той трябва да отговори на искането, което му е отправено, чрез изпращане на отрицателен отговор, придружен от код за отговор conditionsNotCorrect или ResquestSequenceError.

CPR_037 В крайна сметка тестовата апаратура трябва да прибегне до използването на съобщение SecurityAccess „sendKey“, за да предаде определен индивидуален идентификационен номер на блока, монтиран на превозното средство. За управлението на времето, необходимо за извършването на процеса по удостоверяване на картата, блокът трябва да прибегне до кода за отрицателен отговор requestCorrectlyReceived-ResponsePending (нормално получено искане — следва отговор) с цел да се продължи времето за отговор. Времето за отговор не трябва обаче да надхвърля 5 минути. След като бъде изпълнена исканата услуга, блокът изпраща съобщение за положителен или отрицателен отговор с код за отговор, който е различен от цитирания преди това код. Кодът за отрицателен отговор requestCorrectlyReceived-ResponsePending може да бъде повторен от блока дотогава, докато исканата услуга бъде изпълнена и съобщението за краен отговор изпратено.

CPR_038 Блокът, монтиран на превозното средство, трябва да отговоря на това искане, прибягвайки до услугата „Положителен отговор на искане SecurityAccessRequest“ само при условие, че работи в режим ЕТАЛОНИРАНЕ.

CPR_039 В случаите, които са изброени по-долу, блокът трябва да отговори на това искане с отрицателен отговор, придружен от един от следните кодове за отговор:

- subFunctionNotSupported: невалиден формат за параметъра на подфункцията (accessType),
- conditionsNotCorrectorRequestSequenceError: блокът, монтиран на превозното средство, не е готов за приемане на индивидуалния идентификационен номер,
- invalidKey: Невалиден индивидуален идентификационен номер без надхвърляне на броя на опитите за проверка на този номер,
- exceedNumberOfAttempts: Невалиден индивидуален идентификационен номер с надхвърляне на броя на опитите за проверка на този номер,
- generalReject: Редовен индивидуален идентификационен номер, но неуспешен опит за взаимно удостоверяване с използваната цехова карта.

5.2.2. Структура на съобщенията – SecurityAccess — requestSeed

CPR_040 Структурата на съобщенията, свързани с примитивите SecurityAccess „requestSeed“ е обект на подробно описание в таблиците, които следват.

Таблица 18

Съобщение за искане за SecurityAccess — requestSeed

Байт #	Название на параметъра	Стойност hex.	Мнемоничен код
#1	Байт за структура — физическо адресиране	80	FMT
#2	Байт за адреса на набеязаното състояние	EE	CIB
#3	Байт за адреса на източника	tt	SRC
#4	Байт за допълнителна дължина	02	LON
#5	ID на услугата „Искане SecurityAccess“	27	SA
#6	Режим на достъп — искане за начало на удостоверяване (requestSeed)	7D	MA_DG
#7	Байт за контролна сума	00-FF	TC

Таблица 19

Положителен отговор на искане за SecurityAccess — requestSeed

Байт #	Название на параметъра	Стойност hex.	Мнемоничен код
#1	Байт за структура — физическо адресиране	80	FMT
#2	Байт за адреса на набеязаното състояние	tt	CIB
#3	Байт за адреса на източника	EE	SRC
#4	Байт за допълнителна дължина	04	LON
#5	ID на услугата „Положителен отговор на искане SecurityAccess“	67	RPAS
#6	Режим на достъп — искане за начало за удостоверяване (requestSeed)	7D	MA_DG
#7	Удостоверяване от високо ниво	00-FF	GERMSUP
#8	Удостоверяване от ниско ниво	00-FF	GERMINF
#9	Байт за контролна сума	00-FF	TC

Таблица 20

Съобщение за отрицателен отговор на искане за SecurityAccess

Байт #	Название на параметъра	Стойност hex.	Мнемоничен код
#1	Байт за структура — физическо адресиране	80	FMT
#2	Байт за адреса на набелязаното състояние	tt	CIB
#3	Байт за адреса на източника	EE	SRC
#4	Байт за допълнителна дължина	03	LON
#5	ID на услугата „Отрицателен отговор“	7F	RN
#6	ID на услугата „Искане SecurityAccess“	27	AS
#7	Код за отговор = [conditionsNotCorrectOrRequestSequenceError incorrectMessageLength]	22 13	CR_CNC RC_IML
#8	Байт за контролна сума	00-FF	TC

5.2.3. Структура на съобщенията - SecurityAccess - sendKey

CPR_041 Структурата на съобщенията, свързани с примитивите SecurityAccess „sendKey“ е обект на подробно описание в таблиците, които следват.

Таблица 21

Съобщение за заявка SecurityAccess — sendKey

Байт #	Название на параметъра	Стойност hex.	Мнемоничен код
#1	Байт за структура — физическо адресиране	80	FMT
#2	Байт за адреса на набелязаното състояние	EE	CIB
#3	Байт за адреса на източника	tt	SRC
#4	Байт за допълнителна дължина	m+2	LON
#5	ID на услугата „Искане SecurityAccess“	27	AS
#6	Режим на достъп – изпращане на ключ (sendKey)	7E	MA_EC
#7 до #m+6	Ключ#1 (от високо ниво) ... Ключ #m (от ниско ниво, стойността на m трябва да бъде в интервала между 4 и 8 включително)	xx ... xx	CLE
#m+7	Байт за контролна сума	00-FF	TC

Таблица 22

Съобщение за положителен отговор на искане SecurityAccess — sendKey

Байт #	Название на параметъра	Стойност hex.	Мнемоничен код
#1	Байт за структура — физическо адресиране	80	FMT
#2	Байт за адреса на набелязаното състояние	tt	CIB
#3	Байт за адреса на източника	EE	SRC
#4	Байт за допълнителна дължина	02	LON
#5	ID на услугата „Положителен отговор на искане SecurityAccess“	67	RPAS
#6	Режим на достъп – изпращане на ключ (sendKey)	7E	MA_EC
#7	Байт за контролна сума	00-FF	TC

Таблица 23

Съобщение за отрицателен отговор на искане SecurityAccess

Байт #	Название на параметъра	Стойност hex.	Мнемоничен код
#1	Байт за структура — физическо адресиране	80	FMT
#2	Байт за адреса на набелязаното състояние	tt	CIB
#3	Байт за адреса на източника	EE	SRC
#4	Байт за допълнителна дължина	03	LON
#5	ID на услугата „Отрицателен отговор“	7F	NR
#6	ID на услугата SecurityAccess	27	AS
#7	Код за отговор = [generalReject subFunctionNotSupported incorrectMessageLength conditionsNotCorrectOrRequest SequenceError invalidKey exceededNumberOfAttempts requestCorrectlyReceived- ResponsePending]	10 12 13 22 35 36 78	CR_GR CR_SFNS CR_IML CR_CNC CR_IK CR_ENA CR_RCR_RP
#8	Байт за контролна сума	00-FF	TC

6. УСЛУГИ ЗА ПРЕДАВАНЕ НА ДАННИ

Услугите, които са на разположение, са обект на подробно описание в следващата таблица:

Таблица 24

Услуги за предаване на данни

Наименование на услугите	Описание
ReadDataByIdentifier	Клиентът иска предаването на настоящата стойност на запис, до който общ идентификатор позволява получаването на достъп
WriteDataByIdentifier	Клиентът иска запамяване на запис, до който получаването на достъп е било позволено от идентификатор

6.1. Услуга ReadDataByIdentifier**6.1.1. Описание на съобщенията**

CPR_050 Съобщението за заявка ReadDataByIdentifier се използва от клиента, за да поиска извличането на стойности, които са записани в сървър. Данните се идентифицират от „Идентификатор на записи“. Производителят на блока, монтиран на превозното средство, има задължение да следи за изпълнението на условията на сървъра по време на извършването на тази услуга.

6.1.2. Структура на съобщенията

CPR_051 Структурата на съобщенията, свързани с примитивите ReadDataByIdentifier, е обект на подробно описание в таблиците, които следват.

Таблица 25

Съобщение за искане за четене на данни от идентификатор

Байт #	Название на параметъра	Стойност hex.	Мнемоничен код
#1	Байт за структура — физическо адресиране	80	FMT
#2	Байт за адреса на набелязаното състояние	EE	CIB
#3	Байт за адреса на източника	tt	SRC
#4	Байт за допълнителна дължина	03	LON
#5	ID на услугата Искане ReadDataByIdentifier	22	RDBI
#6 до #7	Идентификатор на записи = [една стойност, извлечена от Таблица 28]	xxxx	ILR_...
#8	Байт за контролна сума	00-FF	TC

Таблица 26

Съобщение за положителен отговор на искане за четене на данни от идентификатор

Байт #	Название на параметъра	Стойност hex.	Мнемоничен код
#1	Байт за структура — физическо адресиране	80	FMT
#2	Байт за адреса на набеязаното състояние	tt	CIB
#3	Байт за адреса на източника	EE	SRC
#4	Байт за допълнителна дължина	m+3	LON
#5	ID на услугата „Положителен отговор на искане ReadDataByIdentifier“	62	RPDRDBI
#6 и #7	Локален идентификатор на записи = [същата стойност като байтовете #6 и #7 от Таблица 25]	xxxx	ILR_...
#8 до #m+7	Стойност на запис = (#1 : стойност на запис#m)	xx : xx	VR_... : VR_...
#8	Байт за контролна сума	00-FF	TC

Таблица 27

Съобщение за отрицателен отговор на искане за четене на данни от идентификатор

Байт #	Название на параметъра	Стойност hex.	Мнемоничен код
#1	Байт за структура — физическо адресиране	80	FMT
#2	Байт за адреса на набеязаното състояние	tt	CIB
#3	Байт за адреса на източника	EE	SRC
#4	Байт за допълнителна дължина	03	LON
#5	ID на услугата „Отрицателен отговор“	7F	RN
#6	ID на услугата „Искане ReadDataByIdentifier“	22	RDBI
#7	Код за отговор = [requestOutOfRange incorrectMessageLength conditionsNotCorrect]	31 13 22	RC_ROOR RC_IML RC_CNC
#8	Байт за контролна сума	00-FF	TC

6.1.3. Определяне на параметрите

CPR_052 Параметърът „Идентификатор на записи“ (IR_) в съобщението за заявка ReadDataByIdentifier идентифицира запис на данни.

CPR_053 Стойностите, които един идентификатор на записи (recordDataIdentifier) може да приема, са посочени в следващата таблица.

Тази таблица на идентификаторите на записи се състои от четири колони и известен брой редове.

— първата колона (Hex.) указва „Valeur hex.“ (стойността hex.), която се определя за идентификатора на записи, указан в третата колона,

— втората колона (Елемент на данни) показва елемента на данни от допълнение 1, на който се основава идентификаторът на записи (понякога е необходимо преобразуване на кода),

— третата колона (Описание) указва името на съответния идентификатор на записи,

— четвъртата колона (Мнемоничен код) показва мнемоничния код, свързан с този идентификатор на записи.

Таблица 28

Определяне на стойностите, които се определят за идентификаторите на записи

Hex.	Елемент на данни	Име на идентификатора на записи (виж структурата, посочена в Раздел 8, част 2)	Мнемоничен код
F90B	CurrentDateTime	Дата и час	IR_DH
F912	HighResOdometer	Общ километраж на превозното средство при висока разделителна способност	IR_KTVHD
F918	K-ConstantOfRecordingEquipment	Коефициент К	IR_FK
F91C	L-TyreCircumference	Окръжност на търкаляне на гумите Коефициент L	IR_FL
F91D	W-VehicleCharacteristicConstant	Характеристичен коефициент W на превозното средство	IR_CWCV
F921	TyreSize	Размери на гумите	IR_DP
F922	nextCalibrationDate	Дата на следващото еталониране	IR_DPE
F92C	SpeedAuthorised	Разрешена скорост	IR_VA
F97D	vehicleRegistrationNation	Държава-членка, извършила регистрацията	IR_EMI
F97E	VehicleRegistrationNumber	Регистрационен номер на превозното средство	IR_NIMV
F190	VehicleIdentificationNumber	Идентификационен номер на превозното средство	IR_NIDV

CPR_054 Параметърът „Стойност на запис“ (VR_) се използва при съобщението за положителен отговор ReadDataByIdentifier, за да достави на клиента (тестовата апаратура) записа на данни, идентифициран от идентификатора на записи. Структурите на данни са посочени в раздел 8. Други записи на данни, като входящите съобщения в блока, монтиран на превозното средство, както и изходните данни — вътрешни и външни, могат да се получат по избор от потребителя, но те не са предмет на определяне в настоящия документ.

6.2. Услуга WriteDataByIdentifier**6.2.1. Описание на съобщенията**

CPR_056 Клиентът прибягва да услугата WriteDataByIdentifier, за да извърши записване на стойностите, които са свързани със записите на данни на даден сървър. Данните се идентифицират от идентификатор на записи. Производителят на блока, монтиран на превозното средство, е длъжен да се увери, че необходимите нормални условия на работа на сървъра по време на извършването на тази услуга са налице. За извършване на актуализацията на параметрите, изброени в таблица 28, е необходимо блокът да бъде в режим ЕТАЛОНИРАНЕ.

6.2.2. Структура на съобщенията

CPR_057 Структурата на съобщенията, свързани с примитивите WriteDataByIdentifier, е обект на подробно описание в следващите таблици.

Таблица 29

Съобщение за искане за записване на данни от идентификатор

Байт #	Название на параметъра	Стойност hex.	Мнемоничен код
#1	Байт за структура — физическо адресиране	80	FMT
#2	Байт за адреса на набелязаното състояние	EE	CIB
#3	Байт за адреса на източника	tt	SRC
#4	Байт за допълнителна дължина	m+3	LON
#5	ID на услугата „Искане WriteDataByIdentifier“	2E	WDBI
#6 до #7	Идентификатор на записи = [стойност, извлечена от Таблица 28]	xxxx	IR_...
#8 до #m+7	Стойност на запис = (#1 : Стойност на запис #m)	xx : xx	VR_V1 : VR_Vm
#m+8	Байт за контролна сума	00-FF	TC

Таблица 30

Съобщение за положителен отговор на искане за записване на данни от идентификатор

Байт #	Название на параметъра	Стойност hex.	Мнемоничен код
#1	Байт за структура — физическо адресиране	80	FMT
#2	Байт за адреса на набелязаното състояние	tt	CIB
#3	Байт за адреса на източника	EE	SRC
#4	Байт за допълнителна дължина	03	LON
#5	ID на услугата „Положителен отговор на искане WriteDataByIdentifier“	6E	WDBIPR
#6 до #7	Локален идентификатор на записи = [същата стойност като байтове #6 и #7 Таблица 29]	xxxx	IR_...
#8	Байт за контролна сума	00-FF	TC

Таблица 31

Съобщение за отрицателен отговор на искане за записване на данни от идентификатор

Байт #	Название на параметъра	Стойност hex.	Мнемоничен код
#1	Байт за структура — физическо адресиране	80	FMT
#2	Байт за адреса на набелязаното състояние	tt	CIB
#3	Байт за адреса на източника	EE	SRC
#4	Байт за допълнителна дължина	03	LON
#5	ID на услугата „Отрицателен отговор“	7F	RN
#6	ID на услугата „Искане WriteDataByIdentifier“	2E	WDBLI
#7	Код за отговор = [requestOutOfRange incorrectMessageLength conditionsNotCorrect]	31 13 22	CR_ROR CR_IML CR_CNC
#8	Байт за контролна сума	00-FF	TC

6.2.3. Определяне на параметрите

Параметърът „Идентификатор на записи“ (ILR_) е определен в таблица 28.

Параметърът „Стойност на запис“ (VR) се използва при съобщението за заявка WriteDataByIdentifier, за да достави на сървъра (блок, монтиран на превозното средство) стойностите на записите, идентифицирани от recordDataIdentifier. Структурите на данните са указани в Раздел 8.

7. КОНТРОЛ НА ТЕСТОВИТЕ ИМПУЛСИ — ФУНКЦИОНАЛЕН БЛОК ЗА КОНТРОЛ НА ВХОДНО/ИЗХОДНИТЕ ДАННИ

Услугите, които са на разположение, са обект на подробно описание в следващата таблица:

Таблица 32

Функционален блок за контрол на входно/изходните данни

Название на услугата	Описание
InputOutputControlByIdentifier	Клиентът иска извършване на контрол на определени входно/изходни данни на сървъра

7.1. Услуга InputOutputControlByIdentifier**7.1.1. Описание на съобщенията**

Връзката, която се осъществява посредством фронтално разположения конектор, позволява контролирането или наблюдението на тестовите импулси с помощта на съответна тестова апаратура.

CPR_058 Възможно е да се конфигурира тази линия за входно/изходна сигнализация с помощта на команда, изпратена по линията K, като се използва услугата InputOutputControlByIdentifier за избирането на необходимата за разглежданата линия входна или изходна функция. Съществуват следните налични състояния по линията:

- деактивиран,
- speedSignalInput, когато линията за входно/изходна сигнализация се използва за въвеждане на сигнал за скорост (тестов сигнал), който замества сигнала за скорост на датчика за движение,
- realTimeSpeedSignalOutputSensor, когато линията за входно/изходна сигнализация се използва за извеждане на сигнала за скорост на датчика за движение,
- RTCTOutput, когато линията за входно/изходна сигнализация се използва за извеждане на сигнала на часовника, работещ по координираното универсално време.

CPR_059 За да бъде в състояние да конфигурира състоянието на линията, е необходимо блокът, монтиран на превозното средство, да е започнал сесия за настройка и да работи в режим ЕТАЛОНИРАНЕ. Когато операторът завърши сесия за настройка или реши да излезе от режим ЕТАЛОНИРАНЕ, блокът трябва да се увери, че линията за входно/изходна сигнализация се е върнала в деактивирано положение (по подразбиране).

CPR_060 В случай на получаване на импулси за скорост по входящата линия на сигнала за моментна скорост на блока, монтиран на превозното средство, при положение, че линията за входно/изходна сигнализация работи в режим на въвеждане на данни, тази линия за сигнализация преминава в режим на извеждане на данни или се връща в своето деактивирано положение.

CPR_061 Ето последователността на операциите:

- установяване на взаимна връзка посредством услугата StartCommunication,
- влизане в сесия за настройка посредством услугата StartDiagnosticSession и преминаване в режим на работа ЕТАЛОНИРАНЕ (редът на изпълнение на тези две операции е без значение),
- променяне на състоянието на изхода посредством услугата InputOutputControlByIdentifier.

7.1.2. Структура на съобщенията

CPR_062 Структурата на съобщенията, свързани с примитивите InputOutputControlByIdentifier, е обект на подробно описание в следващите таблици.

Таблица 33

Съобщение за искане на входно/изходен контрол от идентификатор

Байт #	Название на параметъра	Стойност hex.	Мнемоничен код
#1	Байт за структура — физическо адресиране	80	FMT
#2	Байт за адреса на набелязаното състояние	EE	CIB
#3	Байт за адреса на източника	tt	SRC
#4	Байт за допълнителна дължина	xx	LON
#5	ID на услугата Искане InputOutputControlByIdentifier	2F	IOCBLI
#6 и #7	Локален входно/изходен идентификатор = [CalibrationInputOutput]	F960	ILES_CIO
#8 или #8 до #9	Опция за контрол = [Параметър за входно/изходен контрол — стойност, извлечена от Таблица 36 Състояние на контрол – Стойност, извлечена от Таблица 38 (виж. Следващата забележка)]	xx xx	OC_... PCES_... ETC_...
#9 или #10	Байт за контролна сума	00-FF	TC

Забележка: Параметърът „Състояние на контрол“ се появява само в някои случаи (виж параграф 7.1.3).

Таблица 34

Съобщение за положителен отговор на искане за входно/изходен контрол от идентификатор

Байт #	Название на параметъра	Стойност hex.	Мнемоничен код
#1	Байт за структура — физическо адресиране	80	FMT
#2	Байт за адреса на набеязаното състояние	tt	CIB
#3	Байт за адреса на източника	EE	SRC
#4	Байт за допълнителна дължина	xx	LON
#5	ID на услугата „Положителен отговор на искане InputOutputControlByIdentifier“	6F	RPIOCBI
#6 и #7	Локален входно/изходен идентификатор = [CalibrationInputOutput]	F960	ILES_CIO
#8 или #8 до #9	Състояние на контрол = [Параметър на входно/изходен контрол - (същата стойност, като байт #7 от Таблица 33) Състояние на контрол – (същата стойност като байт #9 от Таблица 33)]	xx	STC_ PCES_...
		xx	ETC_...
#9 или #10	Байт за контролна сума	00-FF	TC

Таблица 35

Съобщение за отрицателен отговор на искане за входно/изходен контрол от идентификатор

Байт #	Название на параметъра	Стойност hex.	Мнемоничен код
#1	Байт за структура — физическо адресиране	80	FMT
#2	Байт за адреса на набеязаното състояние	tt	CIB
#3	Байт за адреса на източника	EE	SRC
#4	Байт за допълнителна дължина	03	LON
#5	ID на услугата „Отрицателен отговор“	7F	RN
#6	ID на услугата „Искане inputOutputControlByIdentifier“	2F	IOCBI
#7	Код за отговор = [incorrectMessageLength conditionsNotCorrect requestOutOfRange deviceControlLimitsExceeded]	13	CR_IML
		22	CR_CNC
		31	CR_ROOR
		7A	CR_DCLE
#8	Байт за контролна сума	00-FF	TC

7.1.3. Определяне на параметрите

CPR_064 Параметърът „Параметър за входно/изходен контрол“ (PCES_) е определен в следната таблица.

Таблица 36

Определяне на стойностите, които приемат параметрите за входно/изходен контрол

Hex	Описание	Мнемоничен код
00	Връщане на команда на UCE Тази стойност трябва да посочва на сървъра (блок, монтиран на превозното средство), че тестовата апаратура не управлява повече линията за входно/изходна сигнализация.	RCUCE
01	Възстановяване на конфигурацията по подразбиране Тази стойност трябва да посочва на сървъра (блок, монтиран на превозното средство), че той трябва да върне към своето начално състояние входящия сигнал, вътрешния параметър или изходящия сигнал, указан от локалния входно/изходен идентификатор.	RCD
03	Краткосрочна настройка Тази стойност трябва да посочва на сървъра (блок, монтиран на превозното средство), че той трябва да настрои входящия сигнал, вътрешния параметър или изходящия сигнал, указан от локалния входно/изходен идентификатор в RAM-паметта, като му определи една от стойностите, които са включени в параметрите за състояние на контрол.	RCT

CPR_065 Параметърът „Състояние на контрол“ се появява само когато параметърът за входно/изходен контрол е конфигуриран като параметър за краткосрочна настройка и е определен в следната таблица:

Таблица 37

Определяне на стойностите, които приема параметърът „Състояние на контрол“

Режим	Стойност hex.	Описание
Деактивиране	00	Деактивирана входно/изходна линия (по подразбиране)
Активиране	01	Активирана входно/изходна линия за въвеждане на сигнали за скорост (speedSignalInput)
Активиране	02	Активирана входно/изходна линия за извеждане от датчика на сигнал на скорост в реално време (realTimeSpeedSignalOutputSensor)
Активиране	03	Активирана входно/изходна линия за RTCOutput

8. СТРУКТУРИ НА ЗАПИСИТЕ НА ДАННИ

Настоящият раздел излага подробно:

- общите правила, които се прилагат към диапазона от параметри, прехвърляни от блока, монтиран на превозното средство, към тестовата апаратура,
- структурите, които се използват за прехвърлените данни посредством услугите за предаване на данни, изложени в раздел 6.

CPR_067 Прилагането на всички посочени параметри се осигурява от блока, монтиран на превозното средство.

CPR_068 Данните, предавани от блока към тестовата апаратура в отговор на искане, са от измерим тип (тоест актуалната стойност на искания параметър е такава, каквато е измерена или наблюдавана от блока).

8.1. Диапазони от предавани параметри

CPR_069 Таблица 38 определя използваните диапазони за определяне валидността на даден предаван параметър.

CPR_070 Стойностите от диапазона „Индикатор за грешка“ позволяват на блока да посочи веднага, че в момента не е налице никаква валидна параметрична стойност поради някаква грешка в тестовата апаратура.

CPR_071 Стойностите от диапазона „Не на разположение“ позволяват на блока да изпрати съобщение, което съдържа параметър, който не е на разположение или поддръжката на който не се осигурява от въпросния модул. Стойностите от диапазона „Непоискан“ позволяват предаването на командно съобщение и дават информация за параметрите, за които получателят не очаква отговор.

CPR_072 Когато неизправност в даден компонент попречи на предаването на валидни данни за даден параметър, е целесъобразно да се използва индикаторът за грешка така, както е описан в таблица 38, вместо данните за този параметър. Въпреки това, ако измерените или изчислените данни показват валидна стойност, която обаче се намира извън определения за този параметър диапазон, индикаторът за грешка не трябва да бъде използван. Целесъобразно е в този случай да се предадат данните, като се използва подходящата минимална или максимална параметрична стойност.

Таблица 38

Диапазони на записите на данни

Име на диапазона	1 байт (стойност hex.)	2 байта (стойност hex.)	4 байта (стойност hex.)	ASCII
Валиден сигнал	00 до FA	0000 до FAFF	00000000 до FAFFFFFF	1 до 254
Индикатор, отнасящ се до този параметър	FB	FB00 до FBFF	FB000000 до FBFFFFFF	няма
Диапазон, запазен за бъдещите байтове на индикатора	FC до FD	FC00 до FDFF	FC000000 до FDFFFFFF	няма
Индикатор за грешка	FE	FE00 до FEFF	FE000000 до FEFFFFFF	0
Не е на разположение или не е поискан	FF	FF00 до FFFF	FF000000 до FFFFFFFF	FF

CPR_073 За параметрите, кодирани в ASCII, символът ASCII „*“ се резервира като разграничител.

8.2. Структури на записите на данни

Таблиците, които следват от 40 до 44, излагат подробно структурите, които трябва да се използват посредством услугите ReadDataByIdentifier и WriteDataByIdentifier.

CPR_074 Таблица 40 указва дължината, разделителната способност и оперативния диапазон на всеки параметър, идентифициран от своя идентификатор за запис (recordDataIdentifier).

Таблица 39

Структура на записите

Име на параметъра	Дължина на данните (в байтове)	Разделителна способност	Оперативен диапазон
Дата и час	8	За повече уточнения виж таблица 40	
Общ километраж на превозното средство при висока разделителна способност	4	усилване 5 m/bit, отместване 0 m	0 до + 21 055 406 km
Коефициент К	2	усилване 0,001 imp/m/bit, отместване 0	0 до 64,255 imp/m
Окръжност на търкаляне на гумите Коефициент L	2	усилване 0,125 10 ⁻³ m/bit, отместване 0	0 до 8031 m
Характеристичен коефициент W на превозното средство	2	усилване 0,001 imp/m/bit, отместване 0	0 до 64,255 imp/m
Размери на гумите	15	ASCII	ASCII
Дата на следващото еталониране	3	За повече уточнения виж таблица 41	
Разрешена скорост	2	усилване 1/256 km/h/bit, отместване 0	0 до 250 996 km/h
Държава-членка, извършила регистрацията	3	ASCII	ASCII
Регистрационен номер на превозното средство	14	За повече уточнения виж таблица 44	
Идентификационен номер на превозното средство	17	ASCII	ASCII

CPR_075 Таблица 40 показва подробно структурите на различните байтове на параметъра „дата и час“:

Таблица 40

Подробна структура на параметъра „дата и час“ (стойност на идентификатора за запис # F00B)

Байт	Определяне на параметъра	Разделителна способност	Оперативен диапазон
1	Секунди	усилване 0,25 сек/бит, отместване 0 сек	0 до 59,75 сек
2	Минути	усилване 1 мин/бит, отместване 0 мин	0 до 59 мин
3	Часове	усилване 1 ч/бит, отместване 0 ч	0 до 23 ч
4	Месец	усилване 1 месец/бит, отместване 0 месеца	1 до 12 месеца
5	Ден	усилване 0,25 ден/бит, отместване 0 дена (виж по-долу бележката към Таблица 41)	0,25 до 31,75 дена
6	Година	усилване 1 година/бит, отместване + 1985 година (виж по-долу бележката към Таблица 41)	1985 до 2235
7	Корекция на минути спрямо местното време	усилване 1 мин/бит, отместване – 125 мин	– 59 до 59 мин
8	Корекция на часове спрямо местното време	усилване 1 ч/бит, отместване – 125 ч	– 23 до + 23 ч

CPR_076 Таблица 41 показва подробно структурите на различните байтове на параметъра „Дата на следващото еталониране“.

Таблица 41

Подробна структура на параметъра „Дата на следващото еталониране“ (стойност на идентификатора за запис # F022)

Байт	Определяне на параметъра	Разделителна способност	Оперативен диапазон
1	Месец	усилване 1 месец/бит, отместване 0 месеца	1 до 12 месеца
2	Ден	усилване 0,25 ден/бит, отместване 0 дена (виж следващата бележка)	0,25 до 31,75 дена
3	Година	усилване 1 година/бит, отместване + 1985 година (виж следващата бележка)	1985 до 2235 г.

Бележка относно използването на параметъра „Ден“:

- 1) Стойност 0 за датата е нулева. Стойностите 1, 2, 3 и 4 се използват, за да идентифицират първия ден от месеца; стойностите 5, 6, 7 и 8 указват втория ден на месеца; и т. н.
- 2) Този параметър не влияе и не променя параметъра за часовете.

Бележка относно използването на байта на параметъра „година“:

Стойност 0 за годината отговаря на година 1985; стойност от 1 отговаря на година 1986, и т.н.

CPR_078 Таблица 42 показва подробно структурата на различните байтове на параметъра „Регистрационен номер на превозното средство“.

Таблица 42

Подробна структура на параметъра „Регистрационен номер на превозното средство“ (стойност на идентификатора за запис # F07E)

Байт	Определяне на параметъра	Разделителна способност	Оперативен диапазон
1	Кодова страница (както е определена в допълнение 1)	ASCII	от 01 до 0A
от 2 до 14	Регистрационен номер на превозното средство (както е определен в допълнение 1)	ASCII	ASCII

Допълнение 9

ТИПОВО ОДОБРЕНИЕ — СПИСЪК НА МИНИМАЛНО ИЗИСКВАНИТЕ ИЗПИТАНИЯ

СЪДЪРЖАНИЕ

1.	Въведение.....	193
1.1.	Типово одобрение	193
1.2.	Изходна база	193
2.	Изпитания за функциониране на блока, монтиран на превозното средство.....	194
3.	Изпитания за функциониране на датчика за движение.....	197
4.	Изпитания за функциониране на тахографските карти	199
5.	Изпитания относно възможността за взаимна работа	200

1. ВЪВЕДЕНИЕ

1.1. Типово одобрение

Типовото одобрение в рамките на ЕИО на уреди за регистриране на движението (на компонент от тази апаратура) или на тахографска карта се основава на следните сертифицирания:

- сертифициране за сигурност, извършено от един от компетентните органи на ITSEC срещу зададено състояние на сигурност на системата, която е в пълно съответствие с Допълнение 10 от настоящия анекс,
- сертифициране за функциониране, извършено от компетентните власти на дадена държава-членка, удостоверяващо, че тестваният елемент отговаря на изискванията от настоящия анекс по отношение на изпълнените функции, на точността на измерванията и на характеристиките, свързани с околната среда,
- сертифициране на възможността за взаимна работа, извършено от компетентния орган, натоварен с одобрението на възможността за взаимна работа на апаратурата за контрол (или на тахографската карта), разглеждана заедно с необходимата тахографска карта (или уреди за регистриране на движението) (виж Раздел VIII от настоящия анекс).

Настоящото допълнение уточнява минималния брой тестове, които компетентните власти на дадена държава-членка трябва да проведат по време на серия от изпитания за функциониране, както и минималния брой тестове, които компетентният орган е длъжен да извърши по време на изпитанията за възможността за взаимна работа. Нито процедурите по провеждането на тези изпитания, нито техният тип са обект на по-подробни обяснения.

Настоящото допълнение не разглежда различните аспекти на одобрението за сигурност. Ако някои изпитания за типово одобрение са извършени по време на процеса по оценка и одобрение на сигурността, тяхното повторно провеждане по-късно е ненужно. В тези случаи единствено резултатите от тези изпитания за сигурност са обект на проверка. За сведение, изискванията, които трябва да са обект на изпитания (или са тясно свързани с изпитанията, които трябва да се провеждат) по време на одобрението за сигурност, са отбелязани със звездичка („*“) в настоящото допълнение.

Настоящото допълнение разглежда отделно типовото одобрение на датчика за движение и това на блока, монтиран на превозното средство, които са считани съответно като два отделни компонента на апаратурата за контрол. Възможността за взаимна работа между всеки модул на датчик за движение и всеки модул на блок, монтиран на превозното средство, не е задължителна; следователно типовото одобрение на датчик за движение може да се извърши само ако е свързано с типовото одобрение на блок, монтиран на превозното средство, и обратно.

1.2. Изходна база

Настоящото допълнение се позовава на следното:

CEI 68-2-1	Изпитания в околна среда — Част 2: Изпитания — Изпитания А: Студ. 1990 г. + изменение 2: 1994 г.
CEI 68-2-2	Изпитания в околна среда — Част 2: Изпитания — Изпитания В: Суха топлина. 1974 г. + изменение 2: 1994 г.
CEI 68-2-6	Основни процедури на изпитания в околна среда — Методи на изпитание — Тест Fc и директиви: Трептения (синусоидни). Шесто издание: 1985 г.
CEI 68-2-14	Основни процедури за изпитания в околна среда — Методи на изпитание — Тест N: Промяна на температурата. Изменение 1: 1986 г.
CEI 68-2-27	Основни процедури на изпитания в околна среда — Методи на изпитание — Тест Ea и директиви: Удари. Издание 3: 1987 г.
CEI 68-2-30	Основни процедури на изпитания в околна среда — Методи на изпитание — Тест Db и директиви: Влажна топлина, циклична (12 + 12 — времеви цикъл). Модификация 1: 1985 г.
CEI 68-2-35	Основна процедура за изпитания в околна среда — Методи на изпитание — Тест Fda: Случайни широколентови вибрации — Висока възпроизводимост. Модификация 1: 1983 г.
CEI 529	Степени на защита, осигурявани от корпусите (код IP). Издание 2: 1989 г.
CEI 61000-4-2	Електромагнитна съвместимост (СЕМ) — Техники на изпитание и на измерване — Изпитание за защитеност срещу електростатични разряди: 1995 г./Изменение 1: 1998 г.:
ISO 7637-1	Пътни превозни средства — Радиоелектрически смущения, предизвикани от проводимост и свързвания — Част -1: Леки автомобили и лекотоварни превозни средства, оборудвани с електрическо захранване с номинално напрежение от 12 V — Преходна електрическа проводимост изключително по дължината на линиите за захранване. Второ издание: 1990 г.

- ISO 7637-2 Пътни превозни средства — Радиоелектрически смущения, предизвикани от проводимост и свързвания — Част 2: Лекотоварни автомобили, оборудвани с електрическа система с номинално напрежение от 12 или от 24 V — Преходна електрическа проводимост изключително по дължината на линиите за захранване. Първо издание: 1990 г.
- ISO 7637-3 Пътни превозни средства — Радиоелектрически смущения, предизвикани от проводимост и свързвания — Част 3: Превозни средства, оборудвани с електрическа система с номинално напрежение от 12 или от 24 V — Преходна електрическа емисия чрез кондензаторна и индуктивна връзка по дължината на линии, които са различни от линиите за захранване. Първо издание: 1995 г. + Cor 1: 1995 г.
- ISO/CEI 7816-1 Идентификационни карти — Карти с вградена/и интегрална/и схема/и с контакти — Част 1: Физически характеристики. Първо издание: 1998 г.
- ISO/CEI 7816-2 Информатика — Идентификационни карти — Карти с вградена/и интегрална/и схема/и с контакти — Част 2: Размери и местоположение на контактите. Първо издание: 1999 г.
- ISO/CEI 7816-3 Информатика — Идентификационни карти — Карти с вградена/и интегрална/и схема/и с контакти — Част 3: Електронни сигнали и протокол за предаване на данни. Второ издание: 1997 г.
- ISO/CEI 10373 Идентификационни карти — Методи на изпитание. Първо издание: 1993 г.

2. ИЗПИТАНИЯ ЗА ФУНКЦИОНИРАНЕ НА БЛОКА, МОНТИРАН НА ПРЕВОЗНОТО СРЕДСТВО

№	Изпитание	Описание	Изисквания, свързани с това изпитание
1.	Административно инспектиране		
1.1.	Документация	Точност на документацията	
1.2.	Резултати от изпитанията, провеждани от производителя	Резултати от изпитанията, провеждани от производителя по време на фазата на интегриране. Доказателства върху книжен носител.	070, 071, 073
2.	Визуално инспектиране		
2.1.	Съответствие с документацията		
2.2.	Идентификация/маркировка		168, 169
2.3.	Материали		от 163 до 167
2.4.	Пломбиране		251
2.5.	Външни интерфейси		
3.	Изпитание за функциониране		
3.1.	Предвидени функции		002, 004, 244
3.2.	Режими на експлоатация		006*, 007*, 008*, 009*, 106, 107
3.3.	Права за достъп до функции и данни		010*, 011*, 240, 246, 247
3.4.	Контрол на вкарването и изваждането на картите		013, 014, 015*, 016*, 106
3.5.	Измерване на скоростта и разстоянието		от 017 до 026
3.6.	Хронометриране (изпитание, провеждано при 20 °C)		от 027 до 032
3.7.	Контрол на дейностите на водача		от 033 до 043, 106
3.8.	Контрол на състоянието на кормуване		044, 045, 106
3.9.	Ръчно въведени данни		от 046 до 0506
3.10.	Управление на устройствата за блокировка от страна на предприятието		от 051 до 055
3.11.	Проследяване на дейностите по контрол		056, 057
3.12.	Откриване на събития и/или аномалии		от 059 до 069, 106

№	Изпитание	Описание	Изисквания, свързани с това изпитание
3.1.3.	Данни относно идентифицирането на оборудванията		075*, 076*, 079
3.1.4.	Данни за вкарването и изваждането на картата на водача		от 081* до 083*
3.1.5.	Данни относно дейностите на водача		от 084* до 086*
3.1.6.	Данни относно местоположенията		от 087* до 089*
3.1.7.	Данни относно показанията на километража		от 090* до 092*
3.1.8.	Подробни данни относно скоростта		093*
3.1.9.	Данни относно събитията		094*, 095
3.2.0.	Данни относно аномалиите		096*
3.2.1.	Данни за еталониране		097*, 098*
3.2.2.	Данни за сверяване на часовника		100*, 101*
3.2.3.	Данни относно дейностите по контрол		102*, 103*
3.2.4.	Данни относно устройствата за блокировка от страна на предприятието		104*
3.2.5.	Прехвърляне на данни относно дейностите		105*
3.2.6.	Данни относно особените условия		105a*, 105b*
3.2.7.	Записване и запаметяване върху тахографските карти		108, 109*, 109a*, 110*, 111, 112
3.2.8.	Изобразяване на данните		072, 106, от 113 до 128, PIC_001, DIS_001
3.2.9.	Отпечатване		072, 106, от 129 до 138, PIC_001, от PRT_001 до PRT_012
3.3.0.	Предупреждение		106, от 139 до 148, PIC_001
3.3.1.	Прехвърляни на данни към външни носители		072, 106, от 149 до 151
3.3.2.	Изходни данни, предназначени за допълнителни външни периферни устройства		152, 153
3.3.3.	Еталониране		154*, 155*, 156*, 245
3.3.4.	Сверяване на часовника		157*, 158*
3.3.5.	Отсъствие на интерференция от страна на допълнителните функции		003, 269

№	Изпитание	Описание	Изисквания, свързани с това изпитание
4.	Изпитания в околна среда		
4.1.	Температура	<p>Удостоверява се функционирането, като се извършат следните изпитания:</p> <ul style="list-style-type: none"> — CEI 68-2-1, тест Ad, като се извърши изпитание с времетраене от 72 часа при ниска температура ($-20\text{ }^{\circ}\text{C}$), като тестваното оборудване редува интервали на работа и на почивка от по 1 час, — CEI 68-2-2, тест Bd, като се извърши изпитание с времетраене от 72 часа при висока температура ($+70\text{ }^{\circ}\text{C}$), като тестваното оборудване редува интервали на работа и на почивка от по 1 час, <p>Температурни цикли: удостоверява се, че блокът, монтиран на превозното средство, е в състояние да понесе бърза смяна на околната температура, като се проведе изпитание CEI 68-2-14 тест Na, включващо 20 цикъла, по време на които температурата варира между минималната температура (от $-20\text{ }^{\circ}\text{C}$) и максимална температура (от $+70\text{ }^{\circ}\text{C}$), както и един цикъл на изпитание при поддържане на тези две крайни температури в продължение на 2 часа</p> <p>Възможно е да се проведат ограничен брой изпитания (от определените в раздел 3 на тази таблица) при указаните минимални и максимални температури, както и по време на циклите на изпитания при колебания на температурата</p>	159
4.2.	Влажност	<p>Удостоверява се, че блокът, монтиран на превозното средство, е в състояние да понесе цикъл на влажна горещина (изпитание за устойчивост на горещина), като се провежда изпитание CEI 68-2-30, тест Db, който се състои от шест цикъла по 24 часа, при вариране на температурата от $+25\text{ }^{\circ}\text{C}$ до $+55\text{ }^{\circ}\text{C}$ и процент на относителна влажност, достигащ 97 % при $+25\text{ }^{\circ}\text{C}$ и 93 % при $+55\text{ }^{\circ}\text{C}$</p>	160
4.3.	Вибрации	<p>1. Синусоидни вибрации: удостоверява се, че блокът, монтиран на превозното средство, е в състояние да понесе синусоидни вибрации, които притежават следните характеристики: постоянно изместване в границите между 5 и 11 Hz: 10 mm max. постоянно ускорение в границите между 11 и 300 Hz: 5 g Изпитанието CEI 68-2-6, тест Fc, позволява да се провери дали това изискване е спазено. Минималното времетраене на това изпитание е 3 x 12 часа (12 часа на ос)</p> <p>2. Случайни вибрации: удостоверява се, че блокът, монтиран на превозното средство, е в състояние да понесе случайни вибрации, които притежават следните характеристики: честота от 5 до 150 Hz, ниво $0,02\text{ g}^2/\text{Hz}$ Изпитание CEI 68-2-35, тест Ffda, позволява да се провери дали това изискване е спазено. Минималното времетраене на това изпитание е 3 x 12 часа (12 часа на ос), като тестваното оборудване редува интервали на работа и почивка от по 1 час</p> <p>Целесъобразно е двете описани по-горе изпитания да се проведат върху две различни мостри на тествания тип оборудване</p>	163
4.4.	Защита срещу вода и чужди тела	<p>Удостоверява се, че индексът на защита на блока, монтиран на превозното средство, който съответства на стандарт CEI 529, е равен на минимум IP 40, когато този блок е монтиран за работа при нормални условия на експлоатация</p>	164, 165
4.5.	Защита срещу свръхнапрежения	<p>Удостоверява се, че блокът, монтиран на превозното средство, е в състояние да понесе захранващо напрежение от: версии 24 V: 34 V при $+40\text{ }^{\circ}\text{C}$ в продължение на 1 час версии 12 V: 17 V при $+40\text{ }^{\circ}\text{C}$ в продължение на 1 час</p>	161
4.6.	Защита срещу размяна на полюсите на електрическото захранване	<p>Удостоверява се, че блокът, монтиран на превозното средство, е в състояние да понесе размяна на полюсите на своето електрическо захранване</p>	161

№	Изпитание	Описание	Изисквания, свързани с това изпитание
4.7.	Защита срещу къси съединения	Удостоверява се, че входно/изходните сигнали са защитени срещу късите съединения в електрическото захранване и в заземяването.	161
5.	Изпитание за електромагнитна съвместимост		
5.1.	Излъчване и чувствителност към него	В съответствие с Директива 95/54/ЕИО	162
5.2.	Електростатичен разряд	В съответствие със стандарт CEI 61000-4-2, ± 2 kV (ниво 1)	162
5.3.	Преходна чувствителност към проводимост на ниво на захранването	<p>За версиите 24 V: съгласно стандарт ISO 7637-2:</p> <p>импулс 1a: $V_s = -100\text{ V}$, $R_i = 10\text{ ohms}$</p> <p>импулс 2: $V_s = +100\text{ V}$, $R_i = 10\text{ ohms}$</p> <p>импулс 3a: $V_s = -100\text{ V}$, $R_i = 50\text{ ohms}$</p> <p>импулс 3б: $V_s = +100\text{ V}$, $R_i = 50\text{ ohms}$</p> <p>импулс 4: $V_s = -16\text{ V}$, $V_a = -12\text{ V}$, $t_6 = 100\text{ ms}$</p> <p>импулс 5: $V_s = +120\text{ V}$, $R_i = 2,2\text{ ohms}$, $t_d = 250\text{ ms}$</p> <p>За версиите 12 V: съгласно стандарт ISO 7637-1:</p> <p>импулс 1: $V_s = -100\text{ V}$, $R_i = 10\text{ ohms}$</p> <p>импулс 2: $V_s = +100\text{ V}$, $R_i = 10\text{ ohms}$</p> <p>импулс 3a: $V_s = -100\text{ V}$, $R_i = 50\text{ ohms}$</p> <p>импулс 3б: $V_s = +100\text{ V}$, $R_i = 50\text{ ohms}$</p> <p>импулс 4: $V_s = -6\text{ V}$, $V_a = -5\text{ V}$, $t_6 = 15\text{ ms}$</p> <p>импулс 5: $V_s = +65\text{ V}$, $R_i = 3\text{ ohms}$, $t_d = 100\text{ ms}$</p> <p>Импулс 5 се тества само за блокове, предвидени за монтиране на превозни средства, които не разполагат с устройство за външна защита срещу утечка на пренасания електрически заряд</p>	162

3. ИЗПИТАНИЯ ЗА ФУНКЦИОНИРАНЕ НА ДАТЧИКА ЗА ДВИЖЕНИЕ

№	Изпитание	Описание	Изисквания, свързани с това изпитание
1.	Административно инспектиране		
1.1.	Документация	Точност на документацията	
2.	Визуално инспектиране		
2.1.	Съответствие с документацията		
2.2.	Идентификация/маркировка		169, 170
2.3.	Материали		от 163 до 167
2.4.	Пломбиране		251
3.	Изпитания за функциониране		
3.1.	Данни за идентифициране на датчика		077*
3.2.	Датчик за движение - комплектуване с блока, монтиран на превозното средство		099*, 155
3.3.	Засичане на движение		
	Точност на измерване на движението		от 022 до 026

№	Изпитание	Описание	Изисквания, свързани с това изпитание
4.	Изпитания в околна среда		
4.1.	Работна температура	Удостоверява се функционалността на този компонент (така, както тя е определена в тест № 3.3) за обхвата от температури $[-40\text{ }^{\circ}\text{C} + 135\text{ }^{\circ}\text{C}]$, като се проведат следните изпитания: — CEI 68-2-1, тест Ad, като се извърши изпитание с продължителност от 96 часа при минимална температура $T_{o_{\min}}$ — CEI 68-2-2, тест Bd, като се извърши изпитание с продължителност от 96 часа при максимална температура $T_{o_{\max}}$	159
4.2.	Температурни цикли	Удостоверява се функционалността на този компонент (така, както тя е определена в тест № 3.3) като се проведе изпитание CEI 68-2-14 тест Na, което включва 20 цикъла, по време на които температурата варира между минимална температура (от $-40\text{ }^{\circ}\text{C}$) и максимална температура (от $+135\text{ }^{\circ}\text{C}$), както и по един цикъл на изпитание със задържане при тези две крайни температури в продължение на 2 часа Възможно е да се проведат ограничен брой изпитания (от определените в тест 3.3) при указаните минимални и максимални температури, както и по време на циклите на изпитания при колебания на температурата	159
4.3.	Цикли на влажност	Удостоверява се функционалността на този компонент (така, както тя е определена в тест № 3.3), като се проведе изпитание CEI 68-2-30, test Db, което се състои от шест цикъла по 24 часа при вариране на температурата от $+25\text{ }^{\circ}\text{C}$ до $+55\text{ }^{\circ}\text{C}$ и процент на относителна влажност, който достига 97 % при $+25\text{ }^{\circ}\text{C}$ и 93 % при $+55\text{ }^{\circ}\text{C}$	160
4.4.	Вибрации	Удостоверява се функционалността на този компонент (така, както тя е определена в тест № 3.3), като се проведе изпитание CEI 68-2-6, тест Fc, като се приложи времетраене от 100 цикъла на смяна на честотите: Постоянно изместване в границите между 10 и 57 Hz: 1,5 mm max. Постоянно укорение в границите между 57 и 500 Hz: 20 g	163
4.5.	Механични удари	Удостоверява се функционалността на този компонент (така, както тя е определена в тест № 3.3), като се проведе изпитание CEI 68-2-27, тест Ea, 3 удара в двете посоки по трите перпендикулярни референтни оси	163
4.6.	Защита срещу вода и чужди тела	Удостоверява се, че индексът на защита на датчика за движение, съответстващ на стандарт CEI 529, е равен на минимум IP 64, когато този датчик за движение е монтиран на превозно средство, за да работи при нормални условия на експлоатация	165
4.7.	Защита срещу размяна на полюсите на електрическото захранване	Удостоверява се, че блокът, монтиран на превозното средство, е в състояние да понесе размяна на полюсите на своето електрическо захранване	161
4.8.	Защита срещу къси съединения	Удостоверява се, че входно/изходните сигнали са защитени срещу късите съединения в електрическото захранване и в заземяването	161
5.	Изпитание за електромагнитна съвместимост		
5.1.	Излъчване и чувствителност спрямо тях	Проверява се съответствието с Директива 95/54/ЕИО	162
5.2.	Електростатичен разряд	В съответствие със стандарт CEI 61000-4-2, $\pm 2\text{ kV}$ (ниво 1)	162
5.3.	Преходна чувствителност към проводимост на ниво на линиите за предаване на данни)	В съответствие със стандарт ISO 7637-3 (ниво III)	162

4. ИЗПИТАНИЯ ЗА ФУНКЦИОНИРАНЕ НА ТАХОГРАФСКИТЕ КАРТИ

№	Изпитание	Описание	Изисквания, свързани с това изпитание
1.	Административно инспектиране		
1.1.	Документация	Точност на документацията	
2.	Визуално инспектиране		
2.1.		Проверява се съответствието и качеството на отпечатване на всички функции за защита и на видимите данни	от 171 до 181
3.	Механични изпитания		
3.1.		Проверяват се размерите на картата, както и местоположението на контактите	184 ISO/CEI 7816-1 ISO/CEI 7816-2
4.	Изпитания за протокол		
4.1.	ATR	Удостоверява се съответствието на ATR	ISO/CEI 7816-3 TCS 304, 307, 308
4.2.	T = 0	Удостоверява се съответствието на протокола T = 0	ISO/CEI 7816-3 TCS 302, 303, 305
4.3.	PTS	Удостоверява се съответствието на командата PTS, като се преминава от T = 0 към T = 1	ISO/CEI 7816-3 от TCS 309 до 311
4.4.	T = 1	Удостоверява се съответствието на протокола T = 1	ISO/CEI 7816-3 TCS 303, 306
5.	Структура на картата		
5.1.		Удостоверява се съответствието на записаната на картата структура на файловете, като се провери наличието на задължителните файлове на картата, както и условията за достъп до тях	TCS 312 TCS 400*, 401, 402, 403*, 404, 405*, 406, 407, 408*, 409, 410*, 411, 412, 413*, 414, 415*, 416, 417, 418*, 419
6.	Изпитания за функциониране		
6.1.	Нормален режим на функциониране	Целесъобразно е да се тества поне веднъж всяко разрешено ползване за всяка команда (например: изпробва се командата UPDATE BINARY със CLA = „00“, CLA = „0С“ за различни параметри P1, P2 и Lc). Удостоверява се, че исканите операции са правилно изпълнени върху картата (например: като се извлече файлът, върху който разглежданата команда е била изпълнена)	от TCS 313 до TCS 379
6.2.	Съобщения за грешка	Целесъобразно е да се тества поне веднъж всяко съобщение за грешка (както е посочено в допълнение 2) за всяка команда. Трябва да се тества поне веднъж всяка генерична грешка (с изключение на грешките за цялост „6400“, които се контролират по време на фазата по одобрението за сигурност)	
7.	Изпитания за функциониране в околна среда		
7.1.		Проверява се дали картите функционират добре в пределните условия, определени съгласно стандарт ISO/CEI 10373	от 185 до 188 ISO/CEI 7816-1

5. ИЗПИТАНИЯ ЗА ВЪЗМОЖНОСТ ЗА ВЗАИМНА РАБОТА

№	Изпитание	Описание
1.	Взаимно удостоверяване	Проверява се правилното изпълнение на процедурата по взаимното удостоверяване между блока, монтиран на превозното средство, и тахографската карта
2.	Изпитания за четене /записване	<p>Проиграва се сценарий на класическа дейност, като се тръгне от блока, монтиран на превозното средство. Сценарият трябва да бъде адаптиран към тестовия тип карта и да включва изпълнение на операции по записване във възможно най-голям брой елементарни файлове, които са налични в картата</p> <p>Извършва се прехвърляне на данни върху карта, за да се провери правилното изпълнение на всички операции по записване</p> <p>Удостоверява се правилното извличане на всички съответни записи чрез извършване на ежедневната разпечатка на данните, които съдържа картата</p>

Допълнение 10

ОБЩИ ЦЕЛИ ОТНОСНО СИГУРНОСТТА

Настоящото допълнение определя необходимите минимални изисквания относно целите, свързани със сигурността на датчика за движение на блока, монтиран на превозното средство, и на тахографските карти.

За да се формулират целите относно сигурността по отношение на получаването на сертификати за сигурност, производителите ще бъдат упълномощени да подготвят грижливо и, при необходимост, да комплектуват документите, без да премахват или да внасят каквато и да е промяна в съдържащите се в тях характеристики на заплахите, целите, процесуалните източници и функциите, свързани със сигурността.

СЪДЪРЖАНИЕ

Общи цели по обезпечаване на сигурността на датчика за движение

1.	Въведение	206
2.	Съкращения, определения и изходна база	206
2.1.	Съкращения	206
2.2.	Определения	206
2.3.	Изходна база	207
3.	Аргументация на продукта	207
3.1.	Описание на датчика за движение и метод на използване	207
3.2.	Цикъл на живот на датчика за движение	208
3.3.	Заплахи	208
3.3.1.	Заплахи, съществуващи относно политиките на контрол на достъпа	208
3.3.2.	Заплахи, произтичащи от концепцията	209
3.3.3.	Заплахи, произтичащи от експлоатацията	209
3.4.	Цели, свързани със сигурността	209
3.5.	Цели, свързани с информационната сигурност	209
3.6.	Ресурси, свързани с материалите, процедурите и личния състав	210
3.6.1.	Концепция на оборудването	210
3.6.2.	Доставка на оборудването	210
3.6.3.	Генериране и доставка на данни, свързани със сигурността	210
3.6.4.	Монтиране, еталониране и инспектиране на оборудването за запис	210
3.6.5.	Контрол на прилагането на закона	210
3.6.6.	Ъпгрейдване на софтуера	210
4.	Функции, свързани със сигурността	210
4.1.	Идентифициране и удостоверяване	210
4.2.	Управление на достъпа	211
4.2.1.	Политика на контрол на достъпа	211
4.2.2.	Права за достъп до данните	211
4.2.3.	Структура на файловете и условия за достъп	211
4.3.	Отговорност	211

4.4.	Анализ	212
4.5.	Прецизност	212
4.5.1.	Политика за контрол на информационните потоци	212
4.5.2.	Трансфер на вътрешни данни	212
4.5.3.	Цялост на записаните данни	212
4.6.	Надеждност на услугата	212
4.6.1.	Тестови изпитания	212
4.6.2.	Софтуер	213
4.6.3.	Хардуерна защита	213
4.6.4.	Прекъсвания в захранването	213
4.6.5.	Условия за реинициализиране	213
4.6.6.	Наличност на данните	213
4.6.7.	Наличие на няколко приложения	213
4.7.	Обмен на данни	213
4.8.	Криптографска поддръжка	213
5.	Определяне на механизмите за сигурност	214
6.	Минимална мощност на механизмите за сигурност	214
7.	Степен на гаранция	214
8.	Логически анализ	214
Общи цели относно сигурността на блока, монтиран на превозното средство		
1.	Въведение	216
2.	Съкращения, определения и изходна база	216
2.1.	Съкращения	216
2.2.	Определения	216
2.3.	Изходна база	216
3.	Аргументация на продукта	216
3.1.	Описание на блока, монтиран на превозното средство, и метод на използване	216
3.2.	Цикъл на живот на блока, монтиран на превозното средство	218
3.3.	Заплахи	218
3.3.1.	Заплахи, съществуващи относно политиките на идентифициране и на контрол на достъпа	218
3.3.2.	Заплахи, произтичащи от концепцията	219
3.3.3.	Заплахи, произтичащи от експлоатацията	219
3.4.	Цели, свързани със сигурността	219
3.5.	Цели, свързани с информационната сигурност	220
3.6.	Ресурси, свързани с материалите, процедурите и личния състав	220
3.6.1.	Концепция на оборудването	220
3.6.2.	Доставка и активиране на оборудването	220

3.6.3.	Генериране и доставка на данни, свързани със сигурността	220
3.6.4.	Доставка на картите	221
3.6.5.	Монтиране, еталониране и инспектиране на оборудването за запис	221
3.6.6.	Експлоатация на оборудването	221
3.6.7.	Контрол по прилагане на закона	221
3.6.8.	Ъпгрейдване на софтуера	221
4.	Функции, свързани с обезпечаване на сигурността	221
4.1.	Идентифициране и удостоверяване	221
4.1.1.	Идентифициране и удостоверяване на датчика за движение	221
4.1.2.	Идентифициране и удостоверяване на потребителя	221
4.1.3.	Идентифициране и удостоверяване на предприятието, което е свързано дистанционно	223
4.1.4.	Идентифициране и удостоверяване на блока за управление	223
4.2.	Управление на достъпа	223
4.2.1.	Политика на контрол на достъпа	223
4.2.2.	Права на достъп до функциите	223
4.2.3.	Права на достъп до данните	223
4.2.4.	Структура на файловете и условия за достъп	224
4.3.	Отговорност	224
4.4.	Анализ	224
4.5.	Повторна употреба на информационни обекти	225
4.6.	Прецизност	225
4.6.1.	Политика на контрол на информационните потоци	225
4.6.2.	Трансфер на вътрешни данни	225
4.6.3.	Цялост на записаните данни	225
4.7.	Надеждност на услугата	225
4.7.1.	Изпитания	225
4.7.2.	Софтуер	226
4.7.3.	Хардуерна защита	226
4.7.4.	Прекъсвания в храненето	226
4.7.5.	Условия за реинициализиране	226
4.7.6.	Наличност на данните	226
4.7.7.	Наличие на няколко приложения	226
4.8.	Обмен на данни	226
4.8.1.	Обмен на данни с датчика за движение	226
4.8.2.	Обмен на данни с тахографските карти	227
4.8.3.	Обмен на данни с външни запамятаващи устройства (функция за прехвърляне на данни)	227
4.9.	Криптографска поддръжка	227

5.	Определяне на механизмите за сигурност	227
6.	Минимална мощност на механизмите за сигурност	227
7.	Степен на гаранция	227
8.	Логически анализ	228

Общи цели относно сигурността на тахографските карти

1.	Въведение	232
2.	Съкращения, определения и изходни данни	232
2.1.	Съкращения	232
2.2.	Определения	233
2.3.	Изходни данни	233
3.	Аргументация на продукта	233
3.1.	Описание на тахографска карта и метод на използване	233
3.2.	Цикъл на живот на тахографска карта	233
3.3.	Заплахи	234
3.3.1.	Крайни цели	234
3.3.2.	Пътища на проникване	234
3.4.	Цели, свързани със сигурността	234
3.5.	Цели, свързани с информационната сигурност	234
3.6.	Ресурси свързани с материалите, процедурите и личния състав	234
4.	Функции свързани със сигурността	235
4.1.	Съответствие с профилите на защита	235
4.2.	Идентифициране и удостоверяване на потребителя	235
4.2.1.	Идентифициране на потребителя	235
4.2.2.	Удостоверяване на потребителя	235
4.2.3.	Неуспешни операции при процедурата по удостоверяване	235
4.3.	Управление на достъпа	236
4.3.1.	Политика за контрола на достъпа	236
4.3.2.	Функции на контрола на достъпа	236
4.4.	Отговорност	236
4.5.	Анализ	236
4.6.	Прецизност	236
4.6.1.	Цялост на записаните данни	236
4.6.2.	Удостоверяване на базовите данни	236
4.7.	Надеждност на услугата	237
4.7.1.	Изпитания	237
4.7.2.	Софтуер	237
4.7.3.	Електрическо захранване	237

4.7.4.	Условия за реинициализиране	237
4.8.	Обмен на данни	237
4.8.1.	Обмен на данни с блока, монтиран на превозното средство	237
4.8.2.	Експортиране на данни към независим блок (функция по прехвърляне на данни)	237
4.9.	Криптографска поддръжка	237
5.	Определяне на механизмите за сигурност	237
6.	Минимална мощност на механизмите за сигурност	238
7.	Степен на гаранция	238
8.	Логически анализ	238

ОБЩИ ЦЕЛИ ОТНОСНО СИГУРНОСТТА НА ДАТЧИКА ЗА ДВИЖЕНИЕ

1. Въведение

Настоящият документ съдържа описание на датчика за движение, на заплахите, които той трябва да е в състояние да неутрализира, и на целите относно сигурността, които той трябва да изпълнява. Той указва характера на функциите за обезпечаване на сигурността, които системата изисква. Освен това, той уточнява минималната мощност на механизмите за сигурност, както и изискваната степен на сигурност както по отношение на разработката им, така и по отношение на оценката на качествата на разглежданото оборудване.

Изискванията, които са изложени в настоящия документ, присъстват като съставна част на приложение I Б. Изискванията, представени за по-голяма яснота в текста на приложение I Б, понякога се припокриват с изискванията, свързани с целите относно сигурността. В случай на разминаване в смисъла между някое от необходимите изисквания, свързани с целите относно сигурността, и някое от изискванията от приложение I Б, към което първото препраща, за меродавно се приема изискването, което е изложено в приложение I Б.

Изискванията, изложени в приложение I Б, към които целите относно сигурността не правят никакво препращане, нямат отношение към функциите, свързани с обезпечаване на сигурността.

За целите на проследяването са въведени индивидуални маркери за заплахите, целите, свързаните с процедурите ресурси и спецификации на функциите, свързани с обезпечаване на сигурността, поместени в документацията по тяхното разработване и оценяване.

2. Съкращения, определения и изходна база**2.1. Съкращения**

ROM Постоянна памет

SEF Функция, свързана с обезпечаване на сигурността

TBD За определяне

TOE Зададено състояние за оценка на системата

UEV Блок, монтиран на превозното средство.

2.2. Определения

Цифров тахограф	Уреди за регистриране на движението
Устройство	Периферно устройство, свързано към датчика за движение
Данни за движение	Данни, обменени с блока, монтиран на превозното средство, които отчитат скоростта на превозното средство и изминатото разстояние
Разделени физически части	Материални компоненти на датчика за движение, разположени на различни места в превозното средство, за разлика от материалните компоненти, монтирани в корпуса на датчика за движение
Данни за обезпечаване на сигурността	Особени данни, необходими за изпълнението на функциите, свързани с обезпечаване на сигурността (например криптографски ключове)
Система	Оборудване, личен състав или предприятия, които поддържат определена връзка с оборудването за запис
Потребител	Човек, който използва датчика за движение (когато този термин не влиза в състава на израза „данни на потребител“)
Данни на потребител	Всички данни без данните за движението или тези относно сигурността, които са записани или запазени от датчика за движение.

2.3. Изходна база

ITSEC Information Technology Security Evaluation Criteria 1991 (Критерии за оценка на информационната сигурност)

3. Аргументация на продукта

3.1. Описание на датчика за движение и метод на използване

Датчикът за движение е разработен за използване на пътни превозни средства. Неговата функция е да предава на блок, монтиран на превозното средство, данни, защитени срещу неоторизиран достъп данни за движение, които указват скоростта на превозното средство и изминатото разстояние.

Датчикът за движение е свързан механично към подвижен елемент от превозното средство, движението на което позволява извличането на информация за скоростта на превозното средство или за изминатото разстояние. Той се монтира в скоростната кутия или на всяка друга точка на превозното средство.

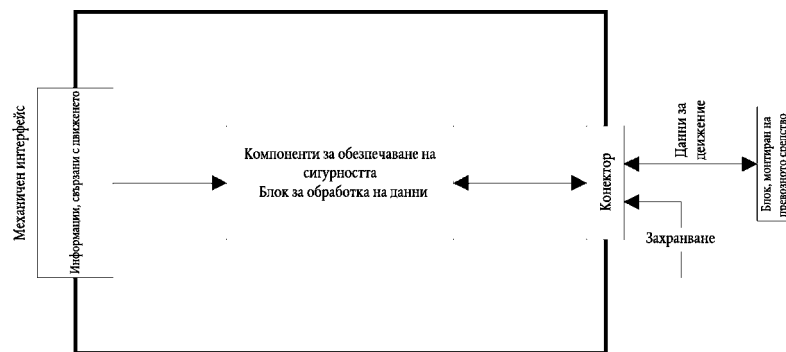
В режим „оперативен“ датчикът за движение е свързан към блок, монтиран на превозното средство.

Възможно е също този датчик да бъде свързан към специализирано оборудване с функции на управление (определя се от производителя)

Следващата фигура показва функционирането на класически датчик за движение:

Фигура 1

Класически датчик за движение

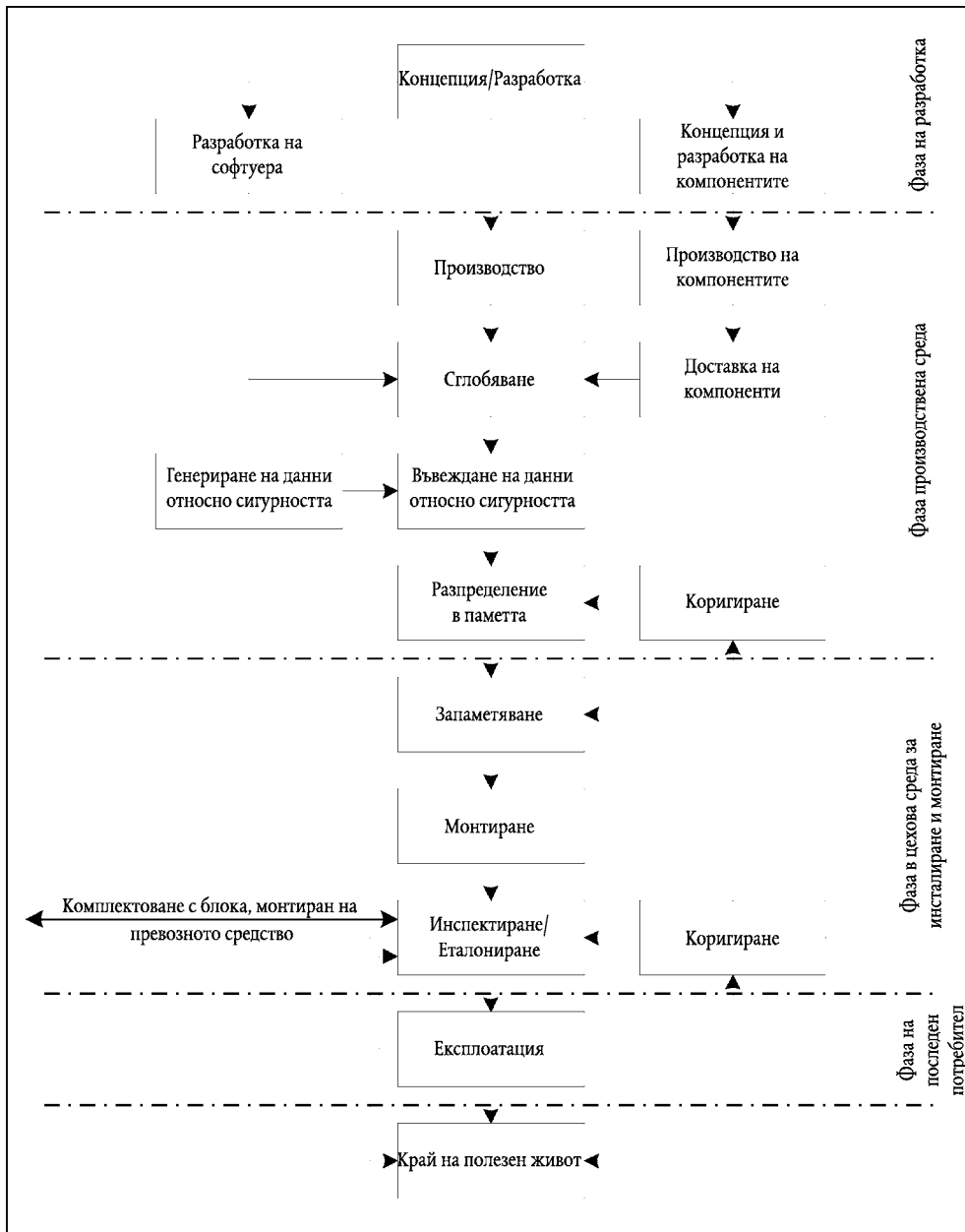


3.2. Цикъл на живот на датчика за движение

Следващата фигура показва характерния цикъл на живот на датчика за движение:

Фигура 2

Характерен цикъл на живот на датчика за движение



3.3. Заплахи

Настоящият параграф представя описание на заплахите, които съществуват относно датчика за движение.

3.3.1. Заплахи, които съществуват относно политиките за контрола на достъпа

3.Достъп Някои потребители могат да се опитат да получат достъп до функции, които са им забранени

3.3.2. Заплахи, произтичащи от концепцията

3.Неизправности	Някои аномалии, които засягат оборудването, софтуера и процедурите по свързване, могат да поставят датчика за движение в непредвидено положение, което може да наруши сигурността
3.Изпитания	Прибягването до невалидни начини на изпитание или до скрити вентилни схеми могат да нарушат сигурността на датчика за движение
3.Концепция	Някои потребители могат да се опитат да получат по незаконен начин конфиденциални данни относно концепцията на въпросния датчик, като ги извлекат от оборудването, с което разполага производителят (кражба, подкуп и т. н.) или чрез извършване на инженерно-проучвателна работа по обратен път

3.3.3. Заплахи, произтичащи от експлоатацията

3.Околна среда	Някои потребители могат да нарушат сигурността на датчика за движение чрез подлагането му на агресивни въздействия в околна среда (термични, електромагнитни, оптически, химически, механични и др въздействия.)
3.Оборудване	Някои потребители могат да се опитат да повредят съставни елементи на датчика за движение
3.Механичен_произход	Някои потребители могат да се опитат да направят неоторизирано манипулиране на входа за данни на датчика за движение (например, като го свалят от скоростната кутия, и т. н.)
3.Данни_движение	Някои потребители могат да се опитат да внесат промени в данните за движение на превозното средство (добавки, изменения, изтривания, възстановяване на сигнала)
3.Захранване	Някои потребители могат да се опитат да извършат промяна в разрез с целите за сигурност на датчика за движение, като променят захранването му (прекъсване, намаляване, усилване)
3.Данни_сигурност	Някои потребители могат да се опитат да получат по незаконен начин конфиденциални данни относно сигурността по време на тяхното генериране, на техния трансфер или на техното записване в оборудването
3.Софтуер	Някои потребители могат да се опитат да внесат промени в софтуера на датчика за движение
3.Запометени_данни	Някои потребители могат да се опитат да променят запометените данни (данните на потребителя или относно сигурността)

3.4. Цели относно сигурността

Главната цел относно сигурността на тахографската цифрова система се представя в следния вид:

Цел.Главна	Данните, които контролните служби подлагат на проверка, трябва да бъдат на разположение и да отразяват точно и с необходимата прецизност дейностите на контролираните водачи и на техните превозни средства както по отношение на скоростта на определеното превозно средство, така и по отношение на периодите на кормуване, на работа, на разположение и на почивка
------------	---

Следователно целта относно сигурността на датчика за движение, която спомага на целта по осигуряване на общата сигурност, се представя в следния вид:

Ц.Главна_датчик	Блокът, монтиран на превозното средство, трябва да има достъп до данните, предавани от датчика за движение, за да бъде в състояние да възпроизведе в цялостен вид и с изискваната прецизност движението на превозното средство както по отношение на скоростта, така и по отношение на изминатото разстояние.
-----------------	---

3.5. Цели по осигуряване на информационната сигурност

Целите по осигуряване на информационната сигурност на датчика за движение, които спомагат на целта по осигуряване на общата сигурност, се представят в следния вид:

Ц.Достъп	Датчикът за движение трябва да контролира достъпа до устройствата, свързани с функциите и данните
Ц.Анализ	Датчикът за движение трябва да следи опитите, целящи намаляване на неговата сигурност, и да засича устройствата, които се използват при тези операции
Ц.Удостоверяване	Датчикът за движение трябва да извършва удостоверяване на свързаните устройства

Ц.Обработка	Датчикът за движение трябва да се увери, че обработката на входящите данни, от които идват данните за движение, се извършва с необходимата прецизност
Ц.Надеждност	Датчикът за движение трябва да осигурява услуга с достатъчна надеждност
Ц.Обмен_защитени_данни	Датчикът за движение трябва да защитава обмена на данни с блока, монтиран на превозното средство

3.6. Ресурси свързани с материалите, процедурите и личния състав

Настоящият параграф представя описание на ресурсите, свързани с материалите, процедурите и личния състав, които допринасят за сигурността на датчика за движение.

3.6.1. Концепция на оборудването

О.Разработка	Конструкторите на датчика за движение трябва да следят да не се изложи на опасност информационната сигурност на проекта при разпределението на отговорностите по време на фазата на неговата разработка
О.Производство	Производителите на датчици за движение трябва да следят да не се изложи на опасност информационната сигурност на проекта при разпределението на отговорностите по време на фазата на неговото производство, както и датчикът за движение да бъде защитен срещу риск от физически въздействия, които могат да повредят информационната му сигурност по време на производствения процес

3.6.2. Доставка на оборудването

О.Доставка	Производителите на датчици за движение, производителите на автомобили, както и цеховете за инсталиране или за механичен монтаж, трябва да следят да не се допусне никакво действие, което може да наруши информационната сигурност на датчика за движение
------------	---

3.6.3. Генериране и доставка на данни, свързани със сигурността

С.Генериране_данни_сигурност	Алгоритмите за генериране на данни относно сигурността трябва да бъдат достъпни само за упълномощени лица и за такива, на които може да се има доверие
С.Транспорт_данни_сигурност	Данните относно сигурността трябва да бъдат генерирани, отправени и въведени в датчика за движение по такъв начин, че да бъде съхранена тяхната конфиденциалност и тяхната цялост

3.6.4. Монтиране, еталониране и инспектиране на оборудването за запис

М.Лицензирани_цехове	Инсталирането, еталонирането и ремонтването на оборудването за запис трябва да бъдат поверени на лицензирани цехове за инсталиране или монтаж, на които може да се има доверие
М.Механичен_интерфейс	Оборудването трябва да бъде снабдено с устройства за откриване на опитите за повреждане на механичния интерфейс (например чрез поставяне на пломби)
М.Редовни_инспекции	Оборудването за запис трябва да бъде обект на периодични инспекции и еталонирания

3.6.5. Контрол на прилагането на закона

З.Контрол	Оборудването трябва да бъде подлагано редовно и инцидентно на контролни проверки относно прилагането на закона. Тези контролни проверки трябва да бъдат придружавани от анализи относно сигурността
-----------	---

3.6.6. Ъпгрейдване на софтуера

С.Актуализация_софтуер	При всяко ъпгрейдване на софтуера трябва да се издава сертификат за сигурност преди пускането му в действие в датчика за движение
------------------------	---

4. Функции, свързани със сигурността

4.1. Идентифициране и удостоверяване

UIA_101 Датчикът за движение е в състояние да установи по време на всяко взаимодействие идентичността на всяко устройство, към което той може да бъде свързан.

- UIA_102 Идентичността на определено свързано устройство се състои от следните елементи:
- група от устройства:
 - блок, монтиран на превозното средство,
 - периферни устройства за управление,
 - други,
 - идентификатор на устройство (единствено за блока, монтиран на превозното средство - UEV).
- UIA_103 Идентификаторът на устройството, свързан с UEV, се състои от сертификационния номер и серийния номер на UEV.
- UIA_104 Датчикът за движение трябва да е в състояние да удостовери всеки UEV или периферно устройство за управление, към което той може да бъде свързан:
- по време на свързване на всяко устройство,
 - по време на всяко възстановяване на електрическото захранване.
- UIA_105 Датчикът за движение е в състояние да извърши повторно удостоверяване на UEV, към който той е свързан.
- UIA_106 Датчикът за движение е в състояние да открие и да предупреди за всеки опит за използване на копирани или възстановени данни за удостоверяване.
- UIA_107 След откриване на X последователни, но безрезултатни опити за удостоверяване (производителят е този, който трябва да определи техния брой, но този брой не трябва да надвишава 20), функцията, свързана със сигурността (SEF) трябва:
- да генерира отчет за анализ на това събитие,
 - да предупреди съответното устройство,
 - да продължи изпращането на данни за движение в незащитен режим на работа.

4.2. Управление на достъпа

Контролът на достъпа гарантира, че извличането на информации от зададеното състояние за оценка на системата, тяхното създаване в нея или внасянето на промени в тези данни са операции, които могат да бъдат извършвани единствено от надлежно упълномощени лица.

4.2.1. Политика на контрола на достъпа

- ACC_101 Датчикът за движение контролира правата за достъп до функциите и данните.

4.2.2. Права на достъп до данните

- ACC_102 Датчикът за движение трябва да гарантира, че неговите данни за идентифициране могат да бъдат обект само на една операция по записване (изискване 078).
- ACC_103 Датчикът за движение приема и/или записва само данни на потребител, които постъпват от удостоверени устройства.
- ACC_104 Датчикът за движение трябва да прилага към данните относно сигурността съответните права за достъп до функциите за четене и записване.

4.2.3. Структура на файловете и условия за достъп

- ACC_105 Структурата на файловете на приложение и на данните, както и условията за достъп до тези файлове, трябва да се определят в процеса на производството, след което да се блокират, за да се попречи на всякакъв опит да извършване на промяна или изтриване.

4.3. Отговорност

- AST_101 Датчикът за движение трябва да съхранява в паметта си данните за идентифициране на датчика за движение (изискване 077).
- AST_102 Датчикът за движение трябва да съхранява в паметта си данни, съдържащи полезна информация относно инсталирането (изискване 099).
- AST_103 Датчикът за движение трябва да е в състояние да прехвърля данни за дейности към удостоверените устройства по тяхно искане.

4.4. Анализ

AUD_101 Датчикът за движение трябва да генерира отчети за анализ, които обхващат събитията, водещи до нарушаване на неговата сигурност.

AUD_102 Събитията, които засягат сигурността на датчика за движение, са следните:

- опити за нарушаване на сигурността:
 - неуспех на процедурата по удостоверяване,
 - нарушена цялост на записаните данни,
 - грешка при трансфер на вътрешни данни,
 - неправомерно отваряне на корпус,
 - саботиране на оборудването,
- неизправност на датчика.

AUD_103 Анализите съдържат следните данни:

- дата и час на събитието,
- тип събитие,
- идентичност на свързаното устройство.

Ако изискваните данни не са на разположение, тези отчети въпреки това да предоставят съответно указание за аномалията (уточнява се от производителя).

AUD_104 Датчикът за движение трябва да предава анализи, които се генерират в UEV, веднага след създаването им. Той трябва да може също така да ги записва в паметта.

AUD_105 Ако датчикът за движение е разработен да записва анализи, той също трябва да бъде в състояние да съхранява 20 отчета за анализ, независимо от степента на запълване на паметта му, определена за записване на тези анализи, и да предава запаменените отчети за анализ на удостоверените устройства при искане за това от тяхна страна.

4.5. Прецизност

4.5.1. Политика на контрол на информационните потоци

ACR_101 Датчикът за движение трябва да дава пълна гаранция, че обработените данни за движение произхождат единствено от механичното устройство на датчика.

4.5.2. Трансфер на вътрешни данни

Изискванията, които са изложени в този параграф, се прилагат само ако датчикът за движение използва компоненти, които са физически разделени.

ACR_102 Ако трябва данните да бъдат прехвърлени между физически разделените части на датчика за движение, тогава е необходимо те да бъдат подсиgurени срещу всякакъв опит за тяхната промяна.

ACR_103 В случай че се открие грешка при трансфера на данни по време на вътрешен трансфер, датчикът трябва да извърши ново прехвърляне на данни, а функцията, свързана със сигурността, трябва да генерира анализ за събитието.

4.5.3. Цялост на записаните данни

ACR_104 Датчикът за движение извършва проверка на данните на потребителя, записани в паметта му, за да открие всяко евентуално нарушение на целостта им.

ACR_105 В случай на откриване на нарушение на целостта на запаменените данни на потребителя функцията, свързана със сигурността, извършва генериране на отчет за анализ.

4.6. Надеждност на услугата

4.6.1. Тестови изпитания

RLB_101 Всички команди, действия или точки на тестови изпитания, използвани за нуждите на изпитанията във фазата на производство, трябва да се деактивират или изтрият преди края на фазата на производство. Няма възможност за тяхното възстановяване с цел по-късното им използване.

- RLB_102 Датчикът за движение изпълнява процедура по автоматични тествания по време на началната фаза на пускане в действие, както и по време на нормалната му експлоатация, с цел да се потвърди правилното му функциониране. Автоматичните тествания на датчика за движение трябва да включват проверка на целостта на данните относно сигурността, както и проверка на целостта на записания изпълним код (при положение, че той не е записан в постоянната памет).
- RLB_103 В случай на откриване на вътрешна аномалия по време на автоматично изпитание функцията, свързана със сигурността, трябва да генерира отчет за анализ (неизправност на датчика).
- 4.6.2. *Софтуер*
- RLB_104 Следва да бъде невъзможно софтуерът на датчика за движение да бъде анализиран или коригиран по месторабота на потребителя.
- RLB_105 Входящите данни, произхождащи от външни източници, в никакъв случай не се възприемат като изпълними кодове.
- 4.6.3. *Хардуерна защита*
- RLB_106 Ако корпусът на датчика за движение е разработен да се отваря, датчикът трябва да бъде в състояние да открие всяко отваряне на корпуса, извършено в период минимум от 6 месеца дори и в случай, когато няма външно захранване. В такъв случай функцията, свързана със сигурността, трябва да генерира отчет за анализ на събитието (приема се, че отчетите за анализ от този характер трябва да се генерират и запамятват след евентуалното възстановяване на електрическото захранване).
- Ако корпусът на датчика за движение е разработен да не се отваря, датчикът трябва да бъде разработен така, че всеки опит за нерегламентиран достъп да бъде лесно откриван (например, чрез извършване на визуална проверка).
- RLB_107 Датчикът за движение трябва да е в състояние да открива някои опити за саботиране на оборудването (те се определят от производителя).
- RLB_108 При евентуален опит за саботиране функцията, свързана със сигурността, трябва да генерира отчет за анализ, а датчикът за движение трябва да извърши следното: (определя се от производителя).
- 4.6.4. *Прекъсвания в захранването*
- RLB_109 Датчикът за движение трябва да преминава в състояние на достатъчна безопасност по време на прекъсванията или колебанията в захранването.
- 4.6.5. *Условия за реинициализиране*
- RLB_110 В случай на прекъсване на захранването, на преждевременното прекъсване на определена операция или при всяко друго положение, което налага неговото реинициализиране, датчикът за движение трябва да се рестартира безконфликтно.
- 4.6.6. *Наличност на данните*
- RLB_111 Датчикът за движение трябва да гарантира достъпа до източниците на данни, когато това се наложи, без те да се изискват или задържат излишно.
- 4.6.7. *Наличие на няколко приложения*
- RLB_112 Ако датчикът за движение съдържа приложения, които са различни от тахографското приложение, всички тези приложения трябва да бъдат отделени едно от друго на физическо и/или логическо равнище. Тези приложения не трябва да използват съвместно никакви данни, свързани със сигурността. Едновременно може да бъде активирана една-единствена задача.
- 4.7. **Обмен на данни**
- DEX_101 Датчикът за движение трябва да изпраща данните за движението към UEV, като ги придружава със съответните им атрибути за сигурност така, че UEV да е в състояние да провери тяхната цялостност и автентичност.
- 4.8. **Криптографска поддръжка**
- Изискванията, които са изложени в този параграф, се прилагат само в случай на необходимост, в зависимост от използваните механизми за сигурност и от приетите от производителя решения.
- CSP_101 Всяка криптографска операция, изпълнена от датчика за движение, трябва да отговаря на точен алгоритъм и на определен формат на ключ.
- CSP_102 Ако датчикът за движение генерира криптографски ключове, той изпълнява тази задача, като спазва някои формати и алгоритми за генериране на криптографски ключове.
- CSP_103 Ако датчикът за движение разпределя криптографски ключове, той изпълнява тази задача, като спазва някои формати и алгоритми за генериране на криптографски ключове.
- CSP_104 Ако датчикът за движение получава достъп до криптографски ключове, той изпълнява тази задача, като спазва някои методи за достъп до криптографските ключове.
- CSP_105 Ако датчикът за движение унищожава криптографски ключове, той трябва да изпълнява тази задача, като спазва някои методи за унищожение на криптографски ключове.

5. Определяне на механизмите за сигурност

Механизмите за сигурност, които изпълняват функциите, свързани със сигурността, се определят от производителите на датчици за движение.

6. Минимална мощност на механизмите за сигурност

Изискваната минимална мощност за механизмите на сигурност на датчика за движение е висока, в съответствие с критериите, които са определени в референтния документ на ITSEC.

7. Степен на гаранция

Степента на гаранция, визирана за датчика за движение, съответства на ниво Е3 в съответствие с критериите, които са определени в референтния документ на ITSEC.

8. Логически анализ

Матриците, които следват, представляват логически анализ на функциите, свързани със сигурността, като акцентират на следните елементи:

- функциите, свързани със сигурността и другите средства за неутрализиране на различните заплахи,
- функциите, свързани със сигурността, които изпълняват различните цели, свързани с информационната сигурност.

	Заплахи										Цели на информационната сигурност							
	Достъп	Неизправност	Изпитания	Концепция	Околна среда	Оборудване	Механичен_Проляход	Данни_Движение	Захранване	Данни_Сигурност	Софтуер	Запазени_Данни	Достъп	Анализ	Удостоверяване	Обработка	Надеждност	Обмен_Защитени_Данни
Ресурси, свързани с материалите, процедурите и или личния състав																		
Разработване		x	x	x														
Производство			x	x														
Доставка						x					x	x						
Генериране на данни, свързани със сигурността										x								
Маршрутизация на данни, свързани със сигурността										x								
Лицензирани цехове							x											
Механичен интерфейс							x											
Редовна инспекция						x	x	x	x	x								
Контрол по прилагането на закона					x	x	x	x	x	x								
Ъпгрейдване на софтуера										x								
Функции, свързани със сигурността																		
Идентифициране и удостоверяване																		
UIA_101 Идентифициране на устройствата	x						x					x		x				x
UIA_102 Идентичност на устройствата	x											x		x				
UIA_103 Идентичност на UEV													x					
UIA_104 Удостоверяване на устройствата	x						x					x		x				x
UIA_105 Ново удостоверяване	x						x					x		x				x
UIA_106 Удостоверяване, неподлежащо на фалшификация	x						x					x		x				
UIA_107 Неуспешно удостоверяване							x						x				x	
Управление на достъпа																		
ACC_101 Политика на контрола на достъпа	x									x	x	x						
ACC_102 ID Идентификатор на датчика за движение											x	x						

ОБЩИ ЦЕЛИ ОТНОСНО СИГУРНОСТТА НА БЛОКА, МОНТИРАН НА ПРЕВОЗНОТО СРЕДСТВО

1. Въведение

Настоящият документ съдържа описание на блока, монтиран на превозното средство, на заплахите, които той трябва да неутрализира, и на целите, свързани със сигурността, които той трябва да изпълнява. Той указва характера на функциите за обезпечаване на сигурността, които системата изисква. Освен това, той уточнява минималната мощност на механизмите за сигурност, както и изискваната степен на сигурност както по отношение на разработката им, така и по отношение на оценката на качествата на разглежданото оборудване.

Изискванията, които са изложени в настоящия документ, присъстват като съставна част на приложение I Б. Изискванията, представени за по-голяма яснота в текста на приложение I Б, понякога се припокриват с изискванията, свързани с целите относно сигурността. В случай на разминаване в смисъла между някое от необходимите изисквания, свързани с целите относно сигурността, и някое от изискванията от приложение I Б, към което първото препраща, за меродавно се приема изискването, което е изложено в приложение I Б.

Изискванията, изложени в приложение I Б, към които целите относно сигурността не правят никакво препращане, нямат отношение към функциите, свързани с обезпечаване на сигурността.

За целите на проследяването са въведени индивидуални маркери за заплахите, целите, свързаните с процедурите ресурси и спецификации на функциите, свързани с обезпечаване на сигурността, поместени в документацията по тяхното разработване и оценяване.

2. Съкращения, определения и изходна база

2.1. Съкращения

PIN	Индивидуален идентификационен номер
ROM	Постоянна памет
SEF	Функция, свързана с обезпечаване на сигурността
TBD	За определяне
TOE	Зададено състояние за оценка на системата
UEV	Блок, монтиран на превозното средство

2.2. Определения

Цифров тахограф	Уреди за регистриране на движението
Данни за движение	Данни, обменени с датчика за движение, които отчитат скоростта на превозното средство и изминатото разстояние
Разделени физически части	Материални компоненти на блока, монтиран на превозното средство, разположени на различни места в превозното средство, за разлика от материалните компоненти, монтирани в корпуса на UEV
Данни за обезпечаване на сигурността	Особени данни, необходими за изпълнението на функциите, свързани с обезпечаване на сигурността (например криптографски ключове)
Система	Оборудване, личен състав или предприятия, които поддържат определена връзка с оборудването за запис
Потребител	Хората, които използват оборудването като потребители. Обичайни потребители на блока, монтиран на превозното средство: водачи, контролбори, цехове и предприятия
Данни на потребител	Всички данни, без данните, свързани със сигурността, които са записани или запаметени от блока, монтиран на превозното средство, в съответствие на разпоредбите, изложени в раздел III.12

2.3. Изходна база

ITSEC ITSEC Information Technology Security Evaluation Criteria 1991 (Критерии за оценка на информационната сигурност)

3. Аргументация на продукта

3.1. Описание на блока, монтиран на превозното средство, и метод на използване

Блокът, монтиран на превозното средство, е разработен за монтиране на превозни средства от пътният транспорт. Неговата функция е да регистрира, запаметява, изобразява, отпечатва и извежда данни, свързани с дейностите на водача или на водачите.

UEV се свързва с датчик за движение, с когото обменя данни за движение относно даденото превозно средство.

Потребителите се идентифицират пред UEV с помощта на тахографски карти.

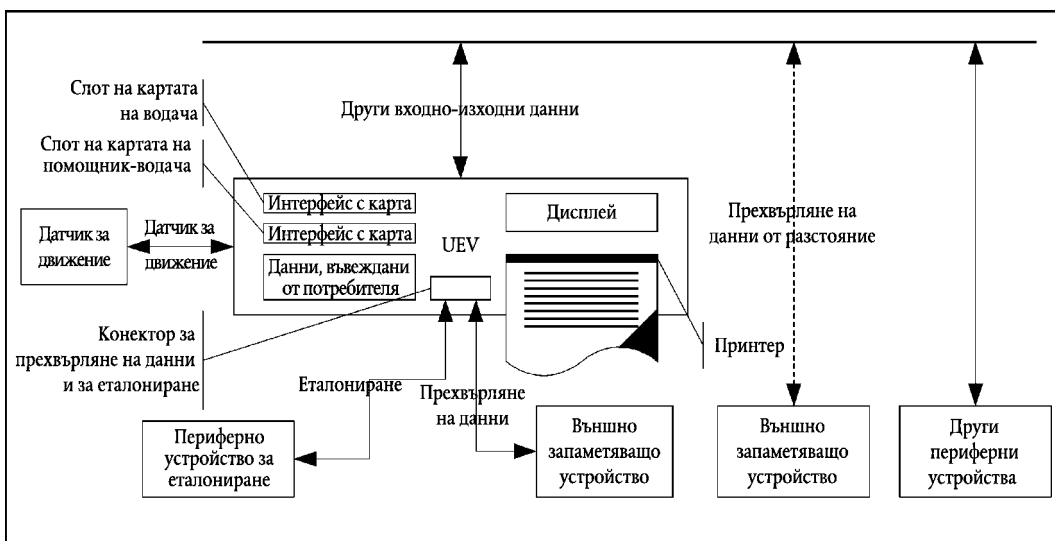
UEV регистрира и запазва данните за дейностите на потребителя в своята памет за данни, той записва също данните за дейностите на потребителя, записани върху тахографските карти.

UEV извършва извеждане на данни за изобразяване на своя дисплей, за принтера и за външните периферни устройства.

Следващата фигура показва операционната среда на блока, монтиран на превозното средство, когато той е монтиран на дадено превозно средство:

Фигура 1

Операционна среда на блока, монтиран на превозното средство



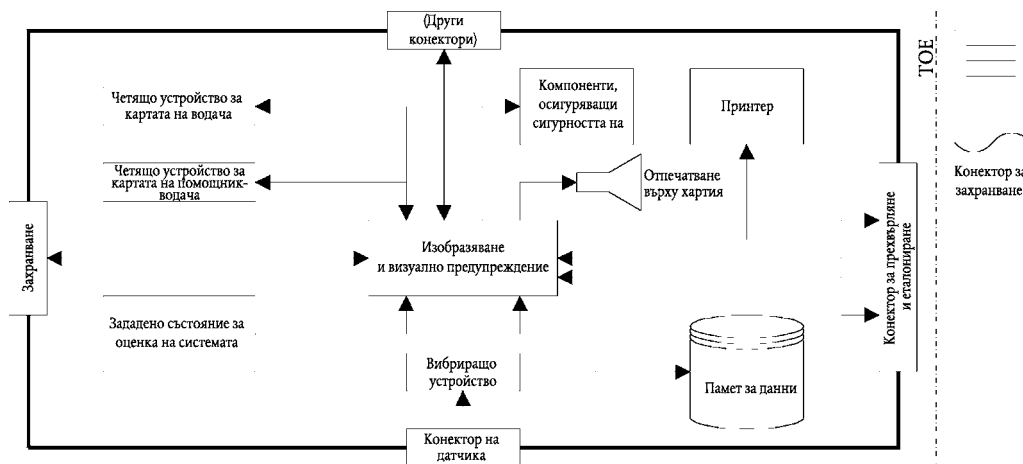
Раздел II на приложение I (Б) представя подробно описание на характеристиките, функциите и режимите на работа на UEV.

Функционалните изисквания, на които трябва да отговоря UEV, са указани в раздел III на приложение I (Б).

Следващата фигура показва един класически UEV:

Фигура 2

Класически UEV (...) опционален



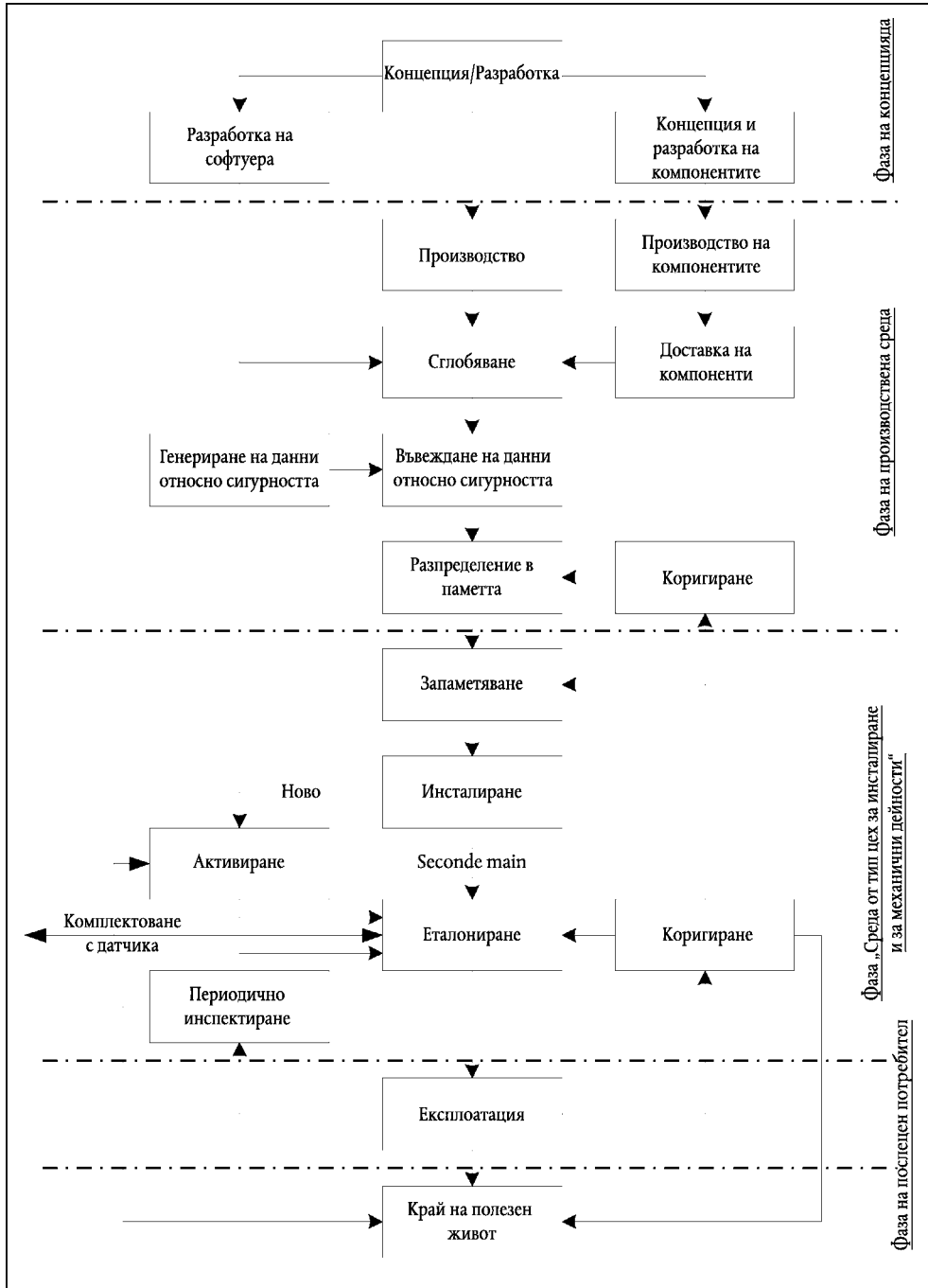
Трябва да се отбележи, че въпреки принадлежността на печатащото устройство към зададено състояние за оценка на системата, отпечатаният върху хартия документ престава да бъде такъв след отпечатването.

3.2. Цикъл на живот на блока, монтиран върху превозното средство

Следващата фигура показва характерния цикъл на живот на UEV:

Фигура 3

Цикъл на живот, характерен за UEV



3.3. Заплахи

Този параграф представя описание на заплахите, които представляват опасност за UEV.

3.3.1. Заплахи, които съществуват относно политиките за идентифициране и за контрол на достъпа

3.Достъп Някои потребители могат да се опитат да получат достъп до функции, които са им забранени (например водачи, които получават достъп до функции по еталониране)

3.Идентифициране Някои потребители могат да се опитат да си послужат с няколко идентификации или да не използват никаква.

3.3.2. Заплахи, произтичащи от концепцията

3.Неизправности	Някои аномалии, които засягат оборудването, софтуера и процедурите по свързване, могат да поставят UEV в непредвидено положение, което може да наруши сигурността
3.Изпитания	Прибягването до неактивирани режими на изпитания или до скрити вентилни схеми могат да нарушат сигурността на UEV
3.Концепция	Някои потребители могат да се опитат да получат по незаконен начин конфиденциални данни, свързани с концепцията на въпросния UEV, като ги извлекат от оборудването, с което разполага производителят (кражба, подкуп и т. н.) или чрез извършване на инженерно-проучвателна работа по обратен път

3.3.3. Заплахи, произтичащи от експлоатацията

3.Параметри_еталониране	Някои потребители могат да се опитат да използват оборудване с погрешно еталониране (чрез внасяне на промени в данните за еталониране или поради структурни слабости)
3.Обмен_данни_карта	Някои потребители могат да се опитат да внесат промени в данните по време на обмена на данни между UEV и тахографските карти (добавки, изменения, изтривания, възстановяване на сигнала)
3.Часовник	Някои потребители могат да се опитат да внесат промени във вътрешния часовник
3.Околна среда	Някои потребители могат да нарушат сигурността на UEV чрез агресивни въздействия, свързани с околната среда (термични въздействия, електромагнитни, оптически, химически, механични и др.)
3.Фиктивни_периферни устройства	Някои потребители могат да се опитат да свържат фиктивни периферни устройства (датчик за движение, карти с памет) към UEV
3.Оборудване	Някои потребители могат да се опитат да повредят съставни части на оборудването на UEV
3.Данни_движение	Някои потребители могат да се опитат да внесат промени в данните за движение на превозното средство (добавки, изменения, изтривания, възстановяване на сигнала)
3.Не_активиране	Някои потребители могат да се опитат да си послужат с неактивирани устройства
3.Извеждане_данни	Някои потребители могат да се опитат да променят извеждането на данни (отпечатване, изобразяване или прехвърляне)
3.Захранване	Някои потребители могат да се опитат, в разрез с целите, свързани със сигурността на UEV, да извършат промяна в неговото захранване (прекъсване, намаляване, усилване на електрическия ток)
3.Данни_сигурност	Някои потребители могат да се опитат да се добият по незаконен начин с конфиденциални данни, свързани със сигурността, по време на тяхното генериране, на тяхното прехвърляне или на тяхното записване вътре в оборудването
3.Софтуер	Някои потребители могат да се опитат да направят промени в софтуера на UEV
3.Запометени_данни	Някои потребители могат да се опитат да променят запометените данни (данните на потребителя или данните, свързани със сигурността).

3.4. Цели, свързани със сигурността

Главната цел, свързана със сигурността на тахографската цифрова система, има следния вид:

Ц.Главна	Данните, които контролните служби проверяват, трябва да бъдат на разположение и да отразяват точно и с изискваната прецизност дейностите на проверяваните водачи и на техните превозни средства както по отношение на скоростта на даденото превозно средство, така и по отношение на периодите на кормуване, на работа, на разположение и на почивка.
----------	--

Следователно целите, свързани със сигурността на UEV, които спомагат за постигане на общата цел относно сигурността, имат следния вид:

Ц.Главна_UEV	Данните, които UEV трябва да измерва и записва, за да могат контролните служби да извършват необходимите проверки, трябва да бъдат на разположение и да отразяват точно и с изискваната прецизност дейностите на проверяваните водачи и на техните превозни средства както по отношение на скоростта на даденото превозно средство, така и по отношение на периодите на кормуване, на работа, на разположение и на почивка
Ц.Експлоатация_UEV	UEV трябва да бъде в състояние сам да извежда данни към външните запамятаващи устройства, за да се позволи на правоимащите да проверяват целостта и автентичността им.

3.5. Цели, свързани с информационната сигурност

Целите, свързани с информационната сигурност, специфични за UEV, които допринасят за неговите глобални цели относно сигурността, имат следния вид:

Ц.Достъп	UEV трябва да контролира достъпа на потребителите до функциите и данните
Ц.Отговорност	UEV трябва да събира точните данни за дейностите
Ц.Анализ	UEV трябва да следи опитите за отслабване на сигурността на системата и да достига до потребителите, които участват в тези операции
Ц.Удостоверяване	UEV трябва да удостоверява потребителите и свързаните устройства (когато трябва да се установи връзка за предаване на конфиденциални данни между различните устройства)
Ц.Цялост	UEV трябва да предпазва целостта на записаните данни
Ц.Извеждане на данни	UEV трябва да гарантира, че извежданата информация отразява с необходимата точност измерените или записани данни
Ц.Обработка	UEV трябва да се увери, че обработката на входящите данни, част от които са данните на потребителя, се извършва с необходимата прецизност
Ц.Надеждност	UEV трябва да осигури услуга с достатъчна надеждност
Ц.ОбменЗащита_данни	UEV трябва да осигурява защита на обмена на данни с датчика за движение и тахографските карти.

3.6. Ресурси, свързани с материалите, процедурите и личния състав

Този параграф представя описание на ресурсите, свързани с материалите, процедурите и личния състав, които допринасят за сигурността на UEV.

3.6.1. Концепция на оборудването

Р.Разработка	Конструкторите на UEV трябва да следят при разпределението на отговорностите по време на фазата на неговата разработка да не се изложи на опасност информационната сигурност на проекта
Р.Производство	Производителите на UEV трябва да следят да не се изложи на опасност информационната сигурност на проекта при разпределението на отговорностите по време на фазата на неговото производство, както и UEV да бъде защитен срещу риск от физически въздействия, които могат да нарушат информационната му сигурност по време на производствения процес.

3.6.2. Доставка и активиране на оборудването

Р.Доставка	Производителите на UEV, производителите на автомобили, както и цеховете за инсталиране или за механичен монтаж, трябва да следят да не се допусне никакво действие върху неактивирани UEV, което може да наруши тяхната информационна сигурност
Р.Активиране	Производителите на автомобили, както и цеховете за инсталиране или за механичен монтаж, трябва да активират разглежданите UEV след тяхното инсталиране, но преди разглежданите превозни средства да са напуснали помещенията, където това инсталиране е било извършено.

3.6.3. Генериране и доставка на данни, свързани със сигурността

Р.Генериране_данни_сигурност	Алгоритмите за генериране на данни, свързани със сигурността, трябва да бъдат достъпни само за упълномощени лица и на такива, на които може да се има доверие
Р.Транспорт_данни_сигурност	Данните, свързани със сигурността, трябва да бъдат генерирани, отправени и въведени в UEV по такъв начин, че да бъде съхранена тяхната конфиденциалност и тяхната цялост.

3.6.4. Доставка на картите

Р.Карты_на разположение	Тахографските карти трябва да бъдат на разположение и да се доставят само на надлежно упълномощени лица
Р.Уникулност_карта_водач	Водачите трябва да притежават по една-единствена валидна карта
Р.Проследяване_карта	Доставката на карти трябва да бъде лесно проследявана (бели и черни списъци — на изправни и неизправни карти), а черните списъци да се използват по време на анализите, свързани със сигурността.

3.6.5. Монтиране, еталониране и инспектиране на оборудването за запис

Р.Одобрени_цехове	Инсталирането, еталонирането и ремонтването на оборудването за запис трябва да бъдат поверени на одобрени цехове за инсталиране или монтаж, на които може да се има доверие
Р.Редовни_инспекции	Оборудването за запис трябва да бъде обект на периодични инспекции и еталонирания
Р.Прецизно_еталониране	Одобрените цехове за инсталиране и механичен монтаж са длъжни да въведат съответните параметри на превозното средство в оборудването за запис по време на еталонирането.

3.6.6. Експлоатация на оборудването

Р.Надеждност_водачи	Водачите трябва да спазват правилата за ползване на оборудването и да доказват, че имат отговорно отношение (например да си служат със своите карти на водач, да избират правилно дейността си, когато избирането им се извършва ръчно, и т. н.).
---------------------	---

3.6.7. Контрол по прилагането на закона

Р.Контролни проверки	Оборудването трябва да бъде подлагано редовно и инцидентно на контролни проверки относно прилагането на закона. Тези контролни проверки трябва да са придружавани от анализи, свързани със сигурността.
----------------------	---

3.6.8. Ъпгрейдване на софтуера

Р. Актуализация_софтуер	При всяко ъпгрейдване на софтуера трябва да се издава сертификат за сигурност преди пускането му в действие в UEV.
-------------------------	--

4. Функции, свързани със сигурността

4.1. Идентифициране и удостоверяване

4.1.1. Идентифициране и удостоверяване на датчика за движение

UIA_201 UEV е в състояние да установи по време на всяко взаимодействие идентичността на датчика за движение, към който той е свързан.

UIA_202 Идентичността на датчика за движение се състои от сертификационния номер и серийния номер на датчика.

UIA_203 UEV удостоверява датчика за движение, към който той е свързан:

- по време на свързването на датчика за движение,
- по време на всяко еталониране на оборудването за запис,
- по време на всяко възстановяване на захранването.

Този процес по взаимно удостоверяване трябва да се задейства от UEV.

UIA_204 UEV трябва да извършва периодично (този период се определя от производителя, но във всеки случай той трябва да бъде по-малък от 1 час) процедура по ново идентифициране и удостоверяване на датчика за движение, към който той е свързан. UEV трябва да се увери, че никой не е заменил датчика за движение, идентифициран по време на последното еталониране на оборудването за запис, с друго устройство.

UIA_205 UEV открива и предупреждава за всеки опит за използване на копирани или възстановени данни за удостоверяване.

UIA_206 След откриване на X последователни, но безрезултатни опити за удостоверяване (производителят е този, който трябва да определи техния брой, но този брой не трябва да надвишава 20), и след откриване на непозволена смяна на идентичност (казано по друг начин, когато оборудването за запис не е в процес по еталониране) на датчика за движение, функцията, която е свързана със сигурността (SEF) трябва:

- да генерира отчет за анализ на събитието,
- да предупреди потребителя,
- да продължи да приема и да използва незащитените от неотризиран достъп данни за движение, които му изпраща датчикът за движение.

4.1.2. Идентифициране и удостоверяване на потребителя

UIA_207 UEV трябва да осигурява постоянно и избиращо проследяване на самоличността на двамата потребители, като следи тахографските карти, които са вкарани съответно в четящите устройства на водача и помощник-водача.

UIA_208 Самоличността на всеки потребител трябва да се състои от следните елементи:

- група от потребители:
 - ВОДАЧ (карта на водач),
 - КОНТРОЛЪОР (карта на контрол),
 - ЦЕХ (цехова карта),
 - ПРЕДПРИЯТИЕ (карта на предприятие),
 - НЯМА ДАННИ (няма поставена карта),
- всеки идентификатор на потребител трябва да се състои от следните елементи:
 - код на държавата-членка, която е издала картата и картовия номер,
 - НЯМА ДАННИ, ако групата потребители е НЕИЗВЕСТНА.

Самоличностите, за които НЯМА ДАННИ, могат да бъдат имплицитно или експлицитно известни.

UIA_209 UEV трябва да извършва удостоверяване на своите потребители по време на всяко поставяне на карта.

UIA_210 UEV трябва да извършва ново удостоверяване на своите потребители:

- по време всяко възстановяване на захранването,
- периодично или след появяване на някои събития (периодът се определя от производителя, но във всеки случай той трябва да бъде по-малък от 24 часа).

UIA_211 Процедурата по удостоверяване трябва да докаже, че поставената карта е валидна тахографска карта, в която са записани данни, свързани със сигурността, които произлизат задължително от разглежданата система. Този процес по взаимно удостоверяване трябва да се задейства от UEV.

UIA_212 Освен изложените по-горе предписания, цеховете също се удостоверяват чрез проверка на техния персонален идентификационен номер. Тези идентификационни номера трябва да съдържат най-малко 4 символа.

Забележка: ако този персонален идентификационен номер се съобщава на UEV с помощта на външно устройство, разположено в близост до него, конфиденциалността на дадения номер не трябва задължително да представлява обект на особена защита по време на операцията по трансфер.

UIA_213 UEV трябва да открива и предупреждава при всеки опит за използване на копирани или възстановени данни за удостоверяване.

UIA_214 След откриването на 5 последователни неуспешни опита за удостоверяване функцията, свързана с обезпечаване на сигурността (SEF), трябва:

- да генерира отчет за анализ на събитието,
- да предупреди потребителя,
- да определи потребителя като НЕИЗВЕСТЕН, а картата като невалидна [(дефиниция z) и изискване 007].

4.1.3. Идентифициране и удостоверяване на предприятието, което е свързано дистанционно

Инсталирането на възможност за дистанционна връзка е по избор. Следователно следващият параграф се прилага само при условие, че тази функция е инсталирана.

- UIA_215 По време на всяко взаимодействие с предприятието, което се е свързало дистанционно, UEV трябва да бъде в състояние да установи идентичността на това предприятие.
- UIA_216 Идентичността на предприятието, което се е свързало дистанционно, трябва да се състои от следните елементи: — код на държавата-членка, която е издала картата, и картовия номер на предприятието.
- UIA_217 UEV трябва да извърши убедително удостоверяване на предприятието, което е свързано дистанционно, преди да разреши извеждането на данни към него.
- UIA_218 Процедурата по удостоверяване трябва да докаже, че въпросното предприятие притежава валидна карта за предприятие, върху която са записани данни, свързани със сигурността, които произлизат задължително от разглежданата система.
- UIA_219 UEV трябва да открива и предупреждава при всеки опит за използване на копирани или възстановени данни за удостоверяване.
- UIA_220 След откриването на 5 последователни, но неуспешни опита за удостоверяване, функцията, свързана със сигурността (SEF), трябва:
- да предупреди предприятието, което е свързано дистанционно.

4.1.4. Идентифициране и удостоверяване на блока за управление

Производителите на UEV трябва да предвидят разработването и производството на специализирани периферни устройства, които позволяват изпълнението на допълнителни функции по управление на UEV (например ъпгрейждане на софтуерите, презареждане на данните, свързани със сигурността, и т. н.). Следователно следващият параграф се прилага само при условие, че тази функция е инсталирана.

- UIA_221 По време на всяко взаимодействие с блок за управление, UEV трябва да бъде в състояние да установи идентичността на този блок.
- UIA_222 UEV трябва да извършва убедително удостоверяване на разглеждания блок за управление, преди да разреши всяко последващо взаимодействие с него.
- UIA_223 UEV трябва да открива и предупреждава при всеки опит за използване на копирани или възстановени данни за удостоверяване.

4.2. Контрол на достъпа

Контролът на достъпа гарантира, че извличането на информации от запазеното състояние за оценка на системата, създаването на такава информация вътре в него или внасянето на промени в тези данни са операции, които могат да бъдат извършвани единствено от надлежно упълномощени лица.

Уместно е да се отбележи, че противно на търговския интерес или на частния характер на някои потребителски данни, записани от UEV, те нямат поверителен характер. Следователно функционалното изискване относно правата за достъп до четене на данните (изискване 011) не е обект на никаква функция, свързана с обезпечаването на сигурността.

4.2.1. Политика на контрола на достъпа

- ACC_201 UEV трябва да управлява и контролира правата за достъп до функциите и данните.

4.2.2. Права на достъп до функциите

- ACC_202 UEV трябва да прилага правилата за избор на експлоатационния режим (изисквания от 006 до 009).
- ACC_203 UEV трябва да прибегва да необходимия експлоатационен режим за прилагане на правилата за контрол на достъпа до функциите (изискване 010).

4.2.3. Права за достъп до данните

- ACC_204 UEV трябва да прилага правилата за достъп до функцията за писане спрямо идентификационните данни на UEV (изискване 076).
- ACC_205 UEV трябва да прилага правилата за достъп до функцията за писане спрямо идентификационните данни на свързания с него датчик за движение (изисквания 076 и 155).
- ACC_206 След активирането си UEV трябва да следи извеждането на данни за еталониране и записването им в паметта за данни да бъде възможно само в режим на еталониране (изисквания 154 и 156).
- ACC_207 След своето активиране UEV трябва да прилага правилата за достъп до функцията за писане и за изтриване спрямо данните за еталониране (изискване 097).

- ACC_208 След активирането си UEV трябва да следи въвеждането на данни за сверяването на часовника и записването им в паметта му за данни да бъде възможно само в режим на еталониране (това изискване не се прилага към незначителните настройки на часовника, които са разрешени от изисквания 157 и 158).
- ACC_209 След своето активиране UEV трябва да прилага правилата за достъп до функцията за писане и за изтриване спрямо данните за сверяването на часовника (изискване 100).
- ACC_210 UEV трябва да прилага към данните, свързани със сигурността, необходимите права за достъп до функцията за четене и писане (изискване 080).

4.2.4. Структура на файловете и условия за достъп

- ACC_211 Структурата на файловете на приложението и на файловете за данни, както и условията за достъп до тези файлове, трябва да се определят в процеса на производството, след което да се блокират, за да се попречи на всякакъв опит да извършване на промяна или изтриване.

4.3. Отговорност

- ACT_201 UEV трябва да следи водачите да носят отговорност за своите дейности (изисквания 081, 084, 087, 105а, 105б, 109 и 109а).
- ACT_202 UEV трябва да съхранява в паметта си постоянните данни за идентифициране (изискване 075).
- ACT_203 UEV трябва да следи цеховете да носят отговорност за своите дейности (изисквания 098, 101 et 109).
- ACT_204 UEV трябва да следи контрольорите да носят отговорност за техните дейности (изисквания 102, 103 и 109).
- ACT_205 UEV трябва да записва данните относно километража (изискване 090), както и подробни данни относно скоростта (изискване 093).
- ACT_206 UEV трябва да следи данните на потребителя, свързани с изискванията от 081 до 093 и от 102 до 105б включително, да не претърпяват никакво изменение след тяхното записване, освен когато станат най-старите запазени данни и трябва да се заместят от по-нови данни.
- ACT_207 UEV трябва да се въздържа от промяна на вече запазени данни върху тахографска карта (изисквания 109 и 109а) освен за заместване на най-старите данни от нови данни (изискване 110) или ако системата се намира в случая, описан в бележката на параграф 2.1 на Допълнение 1.

4.4. Анализ

Функциите за анализ трябва да се прилагат само за събития, които могат да покажат опит за неотризирана промяна или нарушаване на сигурността. Тяхното прилагане е излишно в рамките на нормалното упражняване на правата, дори когато те имат връзка със сигурността.

- AUD_201 UEV трябва да записва събитията, които нарушават сигурността му, като придружава тяхното записване с данните относно това събитие (изисквания 094, 096 и 109).
- AUD_202 Събитията, които засягат сигурността на UEV, са следните:

- опити за нарушаване на сигурността:
 - неуспех на процедурата по удостоверяване на датчика за движение,
 - неуспех на процедурата по удостоверяване на тахографските карти,
 - неправомерно заменяне на датчика за движение,
 - нарушение на целостта на входящите данни, записани на дадена карта,
 - нарушение на целостта на записаните данни на потребител,
 - грешка при трансфер на вътрешни данни,
 - неправомерно отваряне на корпуса,
 - саботиране на оборудването,

- неправилно приключване на последната сесия на картата,
- събитие за грешка, засягащо данните за движение,
- събитие за грешка, засягащо хранването,
- вътрешна неизправност в UEV.

AUD_203 UEV трябва да прилага правилата за архивиране на отчетите за анализ (изисквания 094 и 096).

AUD_204 UEV трябва да записва в паметта си за данни отчетите за анализ, генерирани от датчика за движение.

AUD_205 Системата трябва да позволява отпечатването, изобразяването и прехвърлянето на отчетите за анализ.

4.5. **Повторна употреба на информационни обекти**

REU_201 UEV трябва да позволява повторната употреба на временно съхранените информационни обекти, без това да се изразява в генериране на неприемливи информационни потоци.

4.6. **Прецизност**

4.6.1. *Политика на контрол на информационните потоци*

ACR_201 UEV трябва да следи данните на потребителя, определени в изисквания 081, 084, 087, 090, 093, 102, 104, 105, 105a и 109, да бъдат обработвани само при получаването им от съответните източници на входяща информация:

- данни за движение на превозното средство,
- часовник в реално време на UEV,
- параметри за еталониране на оборудването за запис,
- тахографски карти,
- данни, въведени от потребителя.

ACR_201a UEV трябва да следи данните на потребителя, определени в изискване 109a, да бъдат въведени само за периода между последното изваждане на картата и настоящото поставяне на карта (изискване 050a).

4.6.2. *Трансфер на вътрешни данни*

Изискванията, изложени в този параграф, се прилагат само ако UEV използва устройства, които са разделени физически.

ACR_202 Ако трябва да бъдат прехвърлени данни между физически разделените устройства на UEV, тогава е необходимо те да бъдат подсиурени срещу всякакъв опит за неотризирана промяна.

ACR_203 В случай на засичане на грешка при трансфера на данни по време на вътрешен трансфер, UEV трябва да извърши ново прехвърляне, а функцията, свързана с обезпечаване на сигурността, трябва да генерира отчет за анализ на събитието.

4.6.3. *Цялост на записаните данни*

ACR_204 UEV трябва да проверява данните на потребителя, записани в паметта му за данни, за да открие всяко евентуално нарушаване на целостта им.

ACR_205 В случай на откриване на нарушаване на целостта на запаменените данни на потребителя функцията, свързана с обезпечаване на сигурността, трябва да генерира отчет за анализ.

4.7. **Надеждност на услугата**

4.7.1. *Изпитания*

RLB_201 Всички команди, действия или точки за извършване на изпитания, необходими за нуждите на изпитанията във фазата на производство на UEV, се деактивират или изтриват преди активирането на UEV. Не трябва да бъде възможно тяхното възстановяване с цел на използването им по-късно.

RLB_202 UEV трябва да изпълнява процедура по автоматични тествания по време на началната фаза на пускане в действие, както и по време на нормалната му експлоатация, с цел да се потвърди правилното му функциониране. Автоматичните тествания на UEV трябва да включват проверка на целостта на данните относно сигурността, както и проверка на целостта на записания изпълним код (при положение, че той не е записан в постоянната памет).

RLB_203 В случай на откриване на вътрешна аномалия по време на автоматично тестване функцията, свързана с обезпечаване на сигурността, трябва:

- да генерира отчет за анализ (освен ако е в режим на еталониране) (вътрешна аномалия на UEV),
- да защити целостта на записаните данни.

4.7.2. Софтуер

- RLB_204 След активиране на UEV е невъзможно операционната му система да бъде анализирана или коригирана по местоработата на потребителя.
- RLB_205 Входящите данни, произхождащи от външни източници, не трябва в никакъв случай да се възприемат като изпълними кодове.

4.7.3. Хардуерна защита

- RLB_206 Ако корпусът на UEV е разработен да се отваря, UEV трябва да бъде в състояние, освен ако е в режим на еталониране, да открие всяко отваряне на този корпус, извършено в период от минимум 6 месеца, даже и в случай, когато той няма външно захранване. В такъв случай функцията, свързана с обезпечаването на сигурността, трябва да генерира отчет за анализ (приема се отчетите за анализ от този характер да се генерират и запамяват след евентуалното възстановяване на електрическото захранване).

Ако корпусът на UEV е разработен да не се отваря, UEV трябва да бъде разработен така, че всеки опит за неоторизиран достъп да бъде лесно откриван (например чрез визуална проверка).

- RLB_207 След своето активиране UEV трябва да е в състояние да засича определени опити за саботиране на оборудването (те се определят от производителя).
- RLB_208 При евентуален опит за саботиране функцията, свързана със сигурността, трябва да генерира отчет за анализ, а UEV трябва да извърши следното: (определя се от производителя).

4.7.4. Прекъсвания в захранването

- RLB_209 UEV трябва да засича всяко отклонение от предписаните стойности, включително прекъсванията на захранването.
- RLB_210 В такива случаи функцията, свързана с обезпечаване на сигурността, трябва:

- да генерира отчет за анализ (осен ако е в режим на еталониране),
- да запази състоянието на защита срещу неоторизиран достъп до UEV,
- да осигури поддръжането на функциите, свързани със сигурността, които се прилагат към все още оперативните компоненти или процеси,
- да запази целостта на записаните данни.

4.7.5. Условия за реинициализиране

- RLB_211 В случай на прекъсване на захранването, на преждевременното прекъсване на определена операция или при всяко друго положение, което налага неговото реинициализиране, UEV трябва да се рестартира безконфликтно.

4.7.6. Наличност на данните

- RLB_212 UEV трябва да гарантира достъпа до източниците на данни, когато това се наложи, без те да се изискват или задръжат излишно.
- RLB_213 UEV трябва да забранява всяко освобождаване на картите, преди да е извършил записването на необходимите данни на тях (изисквания 015, и 016).
- RLB_214 В такъв случай функцията, свързана със сигурността, трябва да генерира отчет за анализ относно събитието.

4.7.7. Наличие на няколко приложения

- RLB_215 Ако UEV съдържа приложения, които са различни от тахографското приложение, всички тези приложения трябва да бъдат отделени едни от други на физическо и/или логическо ниво. Тези приложения не трябва да използват съвместно никакви данни, свързани със сигурността. Едновременно може да бъде активирана една-единствена задача.

4.8. Обмен на данни

Този параграф разглежда обмена на данни между UEV и свързаните с него периферни устройства.

4.8.1. Обмен на данни с датчика за движение

- DEX_201 UEV трябва да извършва проверка на целостта и автентичността на данните за движение, въведени от датчика за движение.

DEX_202 В случай, че се открие нарушение на целостта или на автентичността, която засяга определени данни за движение, функцията, свързана с обезпечаване на сигурността, трябва:

- да генерира отчет за анализ,
- да продължи да използва въведените данни.

4.8.2. Обмен на данни с тахографските карти

DEX_203 UEV трябва да извърши проверка на целостта и автентичността на данните за движение, въведени от тахографските карти.

DEX_204 В случай, че се открие нарушена цялост или автентичност, която засяга определени данни, записани върху карта, UEV трябва:

- да генерира отчет за анализ,
- да се въздържа от използване на съответните данни.

DEX_205 UEV трябва да изпраща данните към тахографските карти, като ги придружава със съответните им атрибути за сигурност така, че съответната или съответните карта/и да са в състояние да проверят тяхната цялост и автентичност.

4.8.3. Обмен на данни с външни запазващи устройства (функция за прехвърляне на данни)

DEX_206 UEV трябва да генерира доказателство за произход на данните, прехвърляни към външни запазващи устройства.

DEX_207 UEV трябва да достави на получателя средство за проверка на автентичността на доказателството за произход на прехвърляните данни.

DEX_208 UEV трябва да извърши прехвърляне на данни към външните запазващи устройства, като ги придружава със съответните им атрибути за сигурност така, че съответното или съответните запазващо/и устройство/а да са в състояние да проверят целостта и автентичност на прехвърляните данни.

4.9. Криптографска поддръжка

Изискванията, които са изложени в този параграф, се прилагат само при положение, че тяхната употреба се налага, в зависимост от използваните механизми за сигурност и от решенията, приети от производителя.

CSP_201 Всяка криптографска операция, изпълнена от UEV, трябва да съответства на точен алгоритъм и на определен формат на криптографски ключ.

CSP_202 Ако UEV генерира криптографски ключове, той трябва да изпълнява тази задача, като спазва определени формати и алгоритми за генериране на криптографски ключове.

CSP_203 Ако UEV разпределя криптографски ключове, той трябва да изпълнява тази задача, като спазва определени методи на разпределение на криптографските ключове.

CSP_204 Ако UEV получава достъп до криптографски ключове, той трябва да изпълнява тази задача, като спазва определени методи за достъп до криптографските ключове.

CSP_205 Ако UEV унищожава криптографски ключове, той трябва да изпълнява тази задача, като спазва определени методи за унищожаване на криптографските ключове.

5. Определяне на механизмите за сигурност

Изискваните механизми за сигурност са обект на точно описание в допълнение 11.

Другите механизми за сигурност трябва да бъдат определени от производителите.

6. Минимална мощност на механизмите за сигурност

Изискваната минимална мощност на механизмите на сигурност на блока, монтиран на превозното средство, е висока, в съответствие с критериите, които са определени в референтния документ на ITSEC.

7. Степен на гаранция

Степента на гаранция, предвидена за блока, монтиран на превозното средство, отговаря на степен Е3, в съответствие с критериите, които са определени в референтния документ на ITSEC.

	Заплахи																	Цели на информационната сигурност											
	Достъп	Идентифициране	Неизправности	Изпитания	Концепция	Параметри_Еталониране	Обмен_Данни_Карта	Часовник	Околна среда	Фиктивни_Периф.устр.	Харлуер	Данни_Движение	Деактивирване	Изхошли_Данни	Захранване	Загръстване с ланни	Данни_Сигурност	Софтуер	Замаетени_Данни	Достъп	Отговорност	Анализ	Удостоверяване	Цялост	Извеждане на ланни	Обработка	Населност	Обмен_Защитени_Данни	
UIA_214 Неуспешно удостоверяване	x	x							x												x								
UIA_215 Удостоверяване на отдалечен потребител	x	x																	x			x						x	
UIA_216 Самоличност на отдалечен потребител	x	x																	x			x							
UIA_217 Удостоверяване на отдалечен потребител	x	x																	x			x						x	
UIA_218 Средства за удостоверяване	x	x																	x			x							
UIA_219 Нефалшифицируемо удостоверяване	x	x																	x			x							
UIA_220 Неуспешно удостоверяване	x	x																											
UIA_221 Идентифициране на периферно устройство за управление	x	x																	x			x							
UIA_222 Удостоверяване на периферно устройство за управление	x	x																	x			x							
UIA_223 Нефалшифицируемо удостоверяване	x	x																	x			x							
Управление на достъпа																													
ACC_201 Политика на контрол на достъпа	x					x	x										x	x	x										
ACC_202 Права за достъп до функциите	x					x	x													x									
ACC_203 Права за достъп до функциите	x					x	x													x									
ACC_204 Идентификатор на UEV																			x	x									
ACC_205 Идентификатор на свързания датчик									x										x	x									
ACC_206 Данни от еталониране	x					x													x	x									
ACC_207 Данни от еталониране						x													x	x									
ACC_208 Данни от сверяване на часовника							x												x	x									
ACC_209 Данни от сверяване на часовника							x												x	x									
ACC_210 Данни относно сигурността																	x	x	x										
ACC_211 Структура на файловете и условия за достъп	x					x											x	x	x										
Отговорност																													
ACT_201 Отговорност на водачите																				x									
ACT_202 Данни за идентификатора на UEV																				x	x								
ACT_203 Отговорност на цеховете																				x									
ACT_204 Отговорност на контрольорите																				x									
ACT_205 Подробна информация относно движението на превозното средство																				x									
ACT_206 Промяна на данните относно дейността																			x				x				x		
ACT_207 Промяна на данните относно дейността																			x				x				x		

ОБЩИ ЦЕЛИ ОТНОСНО СИГУРНОСТТА НА ТАХОГРАФСКИТЕ КАРТИ

1. Въведение

Настоящият документ съдържа описание на тахографска карта, на заплахите, които тя трябва да е в състояние да неутрализира, и на целите, свързани със сигурността, на които трябва да отговаря. Той уточнява характера на функциите по обезпечаване на сигурността, които системата изисква. Освен това той уточнява минималната мощност на механизмите за сигурност, както и изискваната степен на сигурност както по отношение на разработката им, така и по отношение на оценката на качествата на разглежданото оборудване.

Изискванията, които са изложени в настоящия документ, присъстват като съставна част на приложение I Б. Изискванията, представени за по-голяма яснота в текста на приложение I Б, понякога се припокриват с изискванията, свързани с целите относно сигурността. В случай на разминаване в смисъла между някои от необходимите изисквания, свързани с целите относно сигурността, и някои от изискванията от приложение I Б, към което първото препраща, за меродавно се приема изискването, което е изложено в приложение I Б.

Изискванията, изложени в приложение I Б, към които целите относно сигурността не правят никакво препращане, нямат отношение към функциите, свързани с обезпечаване на сигурността.

Тахографската карта представлява стандартна карта с чип, на която е записано специализирано тахографско приложение. Тя трябва да отговаря на изискванията, които се прилагат за картите от такъв характер, както по отношение на функционалността си, така и по отношение на степента на гаранция и на сигурност. Следователно тази цел, свързана със сигурността, включва само допълнителните изисквания за сигурност, необходими за тахографското приложение.

За целите на проследяването са въведени индивидуални маркери за заплахите, целите, свързаните с процедурите ресурси и спецификациите на функциите, свързани с обезпечаване на сигурността, поместени в документацията по тяхното разработване и оценяване.

2. Съкращения, определения и изходна база**2.1. Съкращения**

IC	Карта с вграден чип (електронен компонент, разработен да изпълнява функции по обработка и/или запамятване)
OS	Операционна система
PIN	Индивидуален идентификационен номер
ROM	Постоянна памет
SFP	Политика по определяне на функциите, свързани с обезпечаване на сигурността
TBD	За определяне
TOE	Зададено състояние за оценка на системата
TSF	Функция относно сигурността на зададеното състояние за оценка на системата
UEV	Блок, монтиран на превозното средство.

2.2. Определения

Цифров тахограф	Апаратура за записване.
Поверителни данни	Данните, които са записани върху тахографската карта, на които е необходимо да се запази целостта и поверителността (когато такива мерки се прилагат към данните, свързани със сигурността), като в същото време се забранява внасянето на незаконни изменения. Данните, свързани със сигурността, и данните на потребителя се считат за конфиденциални данни.
Данни за обезпечаване на сигурността	Особени данни, необходими за изпълнението на функциите, свързани с обезпечаване на сигурността (например криптографски ключове).
Система	Оборудване, личен състав или предприятия, които поддържат определена връзка с уредите за регистриране на данните за движение.
Потребител	Всяка единица (човек или външно компютърно устройство), независимо от зададеното състояние за оценка на системата, която влиза във взаимодействие с него (когато този термин не влиза в състава на израза „данни на потребител“).

Данни на потребител	Конфиденциални данни (различни от данните, свързани със сигурността), записани на разглежданата тахографска карта. Данните за идентифициране и за дейност са съставна част от данните на потребителя.
Данни за идентифициране	Данните за идентифициране, които обхващат данните за идентифицирането на карта и за идентифициране на титулярите на карта.
Данни за идентифициране на карта	Данни на потребителя, имащи отношение към идентифицирането на карта според изисквания 190, 191, 192, 194, 215, 231 и 235.
Данни за идентифициране на титулярите	Данни на потребителя, имащи отношение към идентифицирането на титулярите според изисквания 195, 196, 216, 232 и 236.
Данни относно дейността	Данните относно дейността обхващат данните за дейност на титуляра на картата, данните за събития и за аномалии, както и данните за контролните дейности.
Данни за дейностите на титулярите	Данните на потребителя, имащи отношение към дейностите, извършвани от титуляра на картата според изисквания 197, 199, 202, 212, 212a, 217, 219, 221, 226, 227, 229, 230a, 233 и 237.
Данни за събития и за аномалии	Данните на потребителя, имащи отношение към събитията или аномалиите според изисквания 204, 205, 207, 208 и 223.
Данни за контролните дейности	Данните на потребителя, имащи отношение към контрола за прилагането на закона според изисквания 210 и 225.

2.3. *Изходна база*

ITSEC	ITSEC Information Technology Security Evaluation Criteria 1991 [Критерии за оценка на информационната сигурност]
IC PP	Smartcard Integrated Circuit Protection Profile — Версия 2.0 — септември 1998 г. Депозиран във Френската национална организация по сертифициране под вх. № PP/9806
ES PP	Smart Card Integrated Circuit With Embedded Software Protection Profile — Версия 2.0 — юни 1999 г. Депозиран във Френската национална организация по сертифициране под вх. № PP/9911

3. *Аргументация на продукта*

3.1. *Описание на тахографска карта и метод на използване*

Тахографската карта е карта с вграден чип, която отговаря на критериите, указани в референтните документи IC PP и ES PP. Освен това на тази карта трябва да има записано приложение, което е разработено да се използва с оборудването за запис.

Елементарните функции на една тахографска карта имат следния вид:

- запаметяване на данните за идентифициране на картата и на нейния титуляр. Блокът, монтиран на превозното средство, използва тези данни, за да идентифицира титуляра на картата, вследствие на което да дава права за достъп до функциите и данните и да следи титуляра на картата по отношение на отговорното изпълнение на дейностите, които той извършва,
- записване на данните за дейностите на титуляра на картата, данните за събитията и за аномалиите, както и данните за контролните дейности, които се отнасят до титуляра на картата.

Следователно тахографската карта е разработена за използване във взаимовръзка с интерфейсното картово устройство на блок, монтиран на превозното средство. Тя трябва да може също да се използва с всяко четящо устройство на карти (с каквото е снабден например един персонален компютър) при положение, че това оборудване има правата за достъп до четене на всички данни на потребителя.

По време на крайната фаза на използване от цикъла на живот на една тахографска карта (фаза 7 от цикъла на живот според референтния документ ES PP), единствено блоковете, които са монтирани на превозните средства, могат да записват данни на потребителя върху съответната карта.

Функционалните изисквания, на които трябва да отговаря една тахографска карта, са указани в текста на приложение I Б и в Допълнение 2.

3.2. *Цикъл на живот на тахографската карта*

Цикълът на живот на една тахографска карта отговаря на цикъла на живот на карта с вграден чип, описан в референтния документ ES PP.

3.3. **Заплахи**

Освен общите заплахи, които застрашават картите с чип и които са описани в референтните документи ES PP и IC PP, съществува опасност от следните заплахи за една тахографска карта:

3.3.1. *Крайни цели*

Крайната цел на лицата, искащи да получат неоторизиран достъп, е внасяне на промени в данните на потребителя, записани в зададеното състояние за оценка на системата.

3.Идентифициране_Данни Внасянето на промени в данните за идентифициране, които са записани в зададеното състояние за оценка на системата (например свързани с типа карта, с датата на изтичане на валидността на картата или с данните за идентифициране на титуляра) може да позволи неправомерно използване на зададеното състояние за оценка на системата и може да представлява сериозна заплаха за глобалната цел относно сигурността на системата

3.Данни_Дейност Внасянето на промени в данните относно дейността, които са записани в зададеното състояние за оценка на системата, може да представлява сериозна заплаха за нейната сигурност

3.Обмен_Данни Внасянето на промени в данните относно дейността (добавки, изтриване, промени) по време на тяхното импортиране или експортиране може да представлява сериозна заплаха за сигурността на зададеното състояние за оценка на системата.

3.3.2. *Начини на проникване*

Съставните елементи на зададеното състояние за оценка на системата могат да бъдат атакувани по различни начини:

- опити за незаконно получаване на конфиденциални данни, свързани с концепцията на хардуера и софтуера на зададеното състояние за оценка на системата и на нейните функции или по-специално данните, свързани със сигурността. За незаконното получаване на тези информации лицата, желаещи да получат неоторизиран достъп, могат да използват начини да се доберат направо до разработеното от проектантите или производителите оборудване (чрез кражба, подкуп и т. н.) или да извършат пряко проучване на зададеното състояние за оценка на системата (проучвания на структурата, логически анализ, и т. н.),
- използване на евентуални слабости, каквито биха могли да се появят в концепцията или реализацията на зададеното състояние за оценка на системата (използване на грешки в хардуера, грешки в софтуера, нарушения при предаването на данни, грешки, причинени в зададеното състояние за оценка на системата чрез различни агресивни въздействия или използване на слабости, каквито биха показали някои функции, свързани със сигурността, като процедурите по удостоверяване, контрола на достъпа до данните, криптографските операции, и т. н.),
- внасяне на промени в състоянието за оценка на системата или в нейните функции, свързани със сигурността посредством физически, електрически или логически въздействия, които могат да са съчетани или не.

3.4. **Цели, свързани със сигурността**

Главната цел, свързана със сигурността на цялата тахографската цифрова система, има следния вид:

Ц.Главна Данните, които контролните служби проверяват, трябва да бъдат на разположение и да отразяват точно и с изискваната прецизност дейностите на проверяваните водачи и на техните превозни средства, както по отношение на скоростта на даденото превозно средство, така и по отношение на периодите на кормуване, на работа, на разположение и на почивка.

Следователно главните цели на зададеното състояние за оценка на системата, които допринасят за тази цел, свързана с общата сигурност, имат следния вид:

Ц.Данни_Идентиф_Карта Зададеното състояние за оценка на системата трябва да защитава данните за идентифициране на картата и на нейния титуляр, записани по време на операцията по персонализирането на картата.

Ц. Запис_Дейност_Карта Зададеното състояние за оценка на системата трябва да защитава данните, записани на картата от блоковете, монтирани на превозното средство.

3.5. **Цели, свързани с информационната сигурност**

Освен общите цели за сигурност, описани в референтните документи ES PP и IC PP, специфичните цели относно информационната сигурност на зададеното състояние за оценка на системата, които допринасят за нейните глобални цели, свързани със сигурността по време на финалната фаза на използване по време на нейния цикъл на живот, имат следния вид:

Ц.Достъп_Данни Зададеното състояние за оценка на системата трябва да ограничи даването на права на достъп за записване на данни на потребител само на удостоверените блокове, монтирани на превозните средства

Ц.Връзка_Защитена срещу неоторизиран достъп Зададеното състояние за оценка на системата трябва да бъде в състояние да осигури прилагането на процедури и протоколи за връзка, защитени срещу неоторизиран достъп, между картата и интерфейсното устройство, когато приложението налага това.

3.6. **Ресурси свързани с материалите, процедурите и личния състав**

Референтните документи ES PP и IC PP описват ресурсите, свързани с материалите, процедурите и личния състав, които допринасят за сигурността на зададеното състояние за оценка на системата (раздели, които са посветени на целите, свързани със сигурността по отношение на околната среда).

4. Функции, свързани с обезпечаване на сигурността

Този параграф разглежда по-задълбочено някои от разрешените операции, като например предназначението или избора на референтните ES PP, и указва допълнителните изисквания за функциониране, на които трябва да отговарят функциите, свързани с обезпечаване на сигурността.

4.1. Съответствие с профилите на защита

- CPP_301 Зададеното състояние за оценка на системата трябва да отговаря на изискванията, указани в референтния документ IC PP.
- CPP_302 Зададеното състояние за оценка на системата трябва да отговаря на изискванията, указани в референтния документ ES PP, след извършване на определени подобрения по-късно.

4.2. Идентифициране и удостоверяване на потребителя

Картата трябва да бъде в състояние да идентифицира устройството, в което е поставена, и да провери дали това е удостоверен блок, монтиран на превозното средство, или не. Картата е в състояние да извърши експортиране на данните на потребителя независимо от устройството, към което тя се свързва, с изключение на картата на контролор, която може да експортира данни за идентифициране на титуляра на картата само към удостоверен блок, монтиран на превозното средство, (по този начин даденият контролор може да се увери, че съответният блок, монтиран на превозното средство, не е фиктивен, тъй като неговите координати се изобразяват на екрана или на контролните разпечатки).

4.2.1. Идентифициране на потребителя

Задание (FIA_UID.1.1) Списък на действията, променени до известна степен от функциите, свързани с обезпечаването на сигурността на зададеното състояние за оценка на системата: няма.

Задание (FIA_ATD.1.1) Списък на атрибутите, свързани със сигурността:

- ГРУПА_ПОТРЕБИТЕЛ: БЛОК_НА_ПРЕВОЗНО СРЕДСТВО, БЛОК_БЕЗ_ПРЕВОЗНО СРЕДСТВО,
- ИДЕНТИФИКАТОР_ПОТРЕБИТЕЛ: Регистрационен номер на превозното средство (NIV) и код на държавата-членка, в която то е регистрирано (ИДЕНТИФИКАТОР_ПОТРЕБИТЕЛ известен само на ГРУПА_ПОТРЕБИТЕЛ = БЛОК_ПРЕВОЗНО СРЕДСТВО).

4.2.2. Удостоверяване на потребителя

Задание (FIA_UAU.1.1) Списък на действията, променени до известна степен от функциите, свързани с обезпечаването на сигурността на зададеното състояние за оценка на системата:

- карта на водача и цехова карта: експортиране на данните на потребителя, придружени от съответните атрибути, свързани с обезпечаване на сигурността (функция за прехвърляне на данни, които са записани на картата),
- карта на контролор: експортиране на данните на потребителя без атрибути, свързани с обезпечаване на сигурността, с изключение на данните за идентифициране на титуляра на съответната карта.

- UIA_301 Процедурата по удостоверяване на даден блок, монтиран на превозното средство, трябва да се състои в доказване, че той съдържа данни относно сигурността, които произлизат задължително от разглежданата система.

Селектиране (FIA_UAU.3.1 и FIA_UAU.3.2): превенция.

Задание (FIA_UAU.4.1) Идентифициран/и механизъм/и за удостоверяване: всеки механизъм за удостоверяване.

- UIA_302 Цеховата карта трябва да притежава допълнителен механизъм за удостоверяване, който да ѝ позволи извършване на проверка на личния идентификационен номер (този механизъм позволява на блока, монтиран на превозното средство, да се увери в самоличността на притежателя на картата; той не е разработен за защита на съдържанието на цеховата карта).

4.2.3. Неуспех на процедурата по удостоверяване

Следващите задания описват реагирането на дадена карта по време на всяка неуспешна процедура по удостоверяване на определен потребител.

Задание (FIA_AFL.1.1) Номер: 1, списък на събития за удостоверяване: удостоверяване на интерфейсно устройство.

Задание (FIA_AFL.1.2) Списък на действията:

- предупреждава се свързаното устройство,
- приемане на потребителя като БЛОК_БЕЗ_ПРЕВОЗНО СРЕДСТВО.

Следващите задания описват реагирането на дадена карта по време на неуспех на допълнителния механизъм за удостоверяване, посочен в точка UIA_302.

Задание (FIA_AFL.1.1) Номер: 5, списък на събития, свързани с удостоверяването: контрол на идентификационните персонални номера (на цехова карта).

Задание (FIA_AFL.1.2) *Списък на действията:*

- предупреждава се свързаното устройство,
- блокира се процедурата за контрол на индивидуалния идентификационен номер по такъв начин, че всеки последващ опит за проверка да бъде неуспешен,
- трябва да има възможност да се указва на следващите потребители причината за наложената блокировка.

4.3. **Управление на достъпа**

4.3.1. *Политика на контрол на достъпа*

По време на крайната фаза на използване от цикъла си на живот тахографската карта работи при прилагане на само една политика относно контрола на достъпа, която се обуславя от функциите, свързани с обезпечаване на сигурността (SFP) и се нарича AC_SFP.

Задание (FDP_ACC.2.1) *Контрол на достъпа SFP: AC_SFP.*

4.3.2. *Функции на контрола на достъпа*

Задание (FDP_ACF.1.1) *Контрол на достъпа SFP: AC_SFP.*

Задание (FDP_ACF.1.1) *Наименована група от атрибути, свързани със сигурността: ГРУПА_ПОТРЕБИТЕЛ.*

Задание (FDP_ACF.1.2) *Правила, които управляват достъпа до контролирани субекти и обекти посредством контролирани операции:*

- ОБЩО_ЧЕТЕНЕ: Данните на потребителя могат да се извлекат от зададеното състояние за оценка на системата от всеки потребител с изключение на данните за идентифициране на титуляра на съответната карта, четенето на които при картите на контролор е запазено за БЛОКОВЕ_НА_ПРЕВОЗНО_СРЕДСТВО,
- ЗАПИСВАНЕ_ИДЕНТИФ: Идентификационните данни могат да се записват само веднъж, и то преди края на фаза 6 от цикъла на живот на картата. Никой потребител няма право да записва или да променя идентификационни данни по време на финалната фаза на ползване от цикъла на живот на дадената карта,
- ЗАПИСВАНЕ_ДЕЙНОСТИ: Единствено БЛОКОВЕ_НА_ПРЕВОЗНО_СРЕДСТВО имат право да записват данните относно дейностите в зададеното състояние за оценка на системата,
- АКТУАЛИЗИРАНЕ_СОФТУЕР: Никой потребител няма право да извършва каквото и да е актуализиране на софтуера на зададеното състояние за оценка на системата,
- СТРУКТУРА_ФАЙЛОВЕ: Структурата на файловете, както и условията за достъп, трябва да бъдат определени преди края на фаза 6 от цикъла на живот на зададеното състояние за оценка на системата, след което трябва да се блокират, за да се предотврати всеки опит за промяна или за изтриване от даден потребител.

4.4. **Отговорност**

АСТ_301 Зададеното състояние за оценка на системата трябва да съхрани в паметта си постоянните данни за идентифициране.

АСТ_302 Часът и датата на персонализация на зададеното състояние за оценка на системата трябва да бъдат указани така, че тя да не може да се променя.

4.5. **Анализ**

Зададеното състояние за оценка на системата трябва да следи събитията, които посочват потенциално нарушаване на сигурността му.

Задание (FAU_SAA.1.2) *Определена подгрупа от събития за анализирани:*

- неуспех на процедурата по удостоверяване на титуляра на картата (5 последователни неуспешни проверки на персоналния идентификационен номер на титуляра),
- грешка при автоматично тестване,
- грешка, свързана с целостта на записаните данни,
- грешка, свързана с целостта, открита при въвеждането на данни относно дейностите.

4.6. **Прецизност**

4.6.1. *Цялост на записаните данни*

Задание (FDP_SDI.2.2) *Действия, които трябва да се предприемат:* предупреждава се свързаното устройство.

4.6.2. *Удостоверяване на базовите данни*

Задание (FDP_DAU.1.1) *Списък на обекти или типове информация:* Данни относно дейностите.

Задание (FDP_DAU.1.2) *Списък на субектите:* Всеки субект.

4.7. Надеждност на услугата

4.7.1. Изпитания Селектиране

(FPT_TST.1.1): по време на първоначалното пускане в действие и редовно по време на нормална експлоатация.

Забележка: в настоящия случай изразът „по време на първоначалното пускане в действие“ означава преди изпълнението на кода [а не задължително по време на процедурата Answer To Reset (отговор на реинициализиране)].

- RLB_301 Автоматичните тествания на зададеното състояние за оценка на системата трябва да включват проверка на целостта на всеки софтуерен код, който не е записан в постоянната памет.
- RLB_302 В случай на откриване на грешка при автоматичното тестване функцията по обезпечаване на сигурността на зададеното състояние за оценка на системата трябва да изпрати предупреждение до свързаното устройство.
- RLB_303 Според изискванията на изпитанията, на които операционната система трябва да се подложи, всички команди и действия, свързани с тяхното изпълнение, трябва да бъдат деактивирани или премахнати. Не трябва да има възможност за тяхната замяна или възстановяване с цел по-късното им използване. Командите, които са свързани изключително с определена фаза от цикъла на живот, трябва да останат недостъпни през следващите фази на този цикъл.

4.7.2. Софтуер

- RLB_304 Трябва да бъде невъзможно извършването на анализ, изменение или коригиране по месторабота на потребителя на операционната система на зададеното състояние за оценка на системата.
- RLB_305 Данните, въведени от външни източници, по никакъв начин не трябва да бъдат приемани като изпълними кодове.

4.7.3. Захранване

- RLB_306 По време на прекъсвания или колебания в захранването зададеното състояние за оценка на системата трябва да се намира в задоволителна степен на защита срещу неоторизиран достъп.

4.7.4. Условия за реинициализиране

- RLB_307 В случай на прекъсване на захранването (или на колебания в захранващото напрежение), което засяга зададеното състояние за оценка на системата, в случай на преждевременно прекъсване на определена операция или при всяко друго положение, което налага неговото реинициализиране, зададеното състояние за оценка на системата трябва да се рестартира безконфликтно.

4.8. Обмен на данни

4.8.1. Обмен на данни с блок, монтиран на превозното средство

- DEX_301 Зададеното състояние на системата трябва да извърши проверка на целостта и автентичността на данните, импортирани от блока, монтиран на превозното средство.
- DEX_302 В случай че се открие нарушена цялост на импортираните данни, зададеното състояние за оценка на системата трябва:
— да предупреди устройството, изпращащо данните,
— да се въздържа от използване на разглежданите данни.
- DEX_303 Зададеното състояние за оценка на системата трябва да извършва експортиране на данните на потребителя към блока, монтиран на превозното средство, като ги придружава със съответните им атрибути за сигурност така, че този блок, монтиран на превозното средство, да бъде в състояние да провери целостта и автентичността на получените данни.

4.8.2. Експортиране на данни към дадено независимо устройство (функция по прехвърляне на данни)

- DEX_304 Зададеното състояние за оценка на системата трябва да може да генерира доказателство за произхода относно данните, прехвърляни към външни запамятаващи устройства.
- DEX_305 Зададеното състояние за оценка на системата трябва да може да предостави на получателя средство за проверка на автентичността на доказателството за произход на прехвърляните данни.
- DEX_306 Зададеното състояние за оценка на системата трябва да може да извърши прехвърляне на данни към външни запамятаващи устройства, като ги придружава със съответните им атрибути за сигурност така, че съответното или съответните запамятаващо/и устройство/а да са в състояние да проверят тяхната цялост и автентичност.

4.9. Криптографска поддръжка

- CSP_301 Ако функцията по обезпечаване на сигурността на зададеното състояние на системата генерира криптографски ключове, тя трябва да изпълнява тази задача, като спазва определени формати и алгоритми за генериране на криптографски ключове. Генерираните криптографски ключове за определени сесии трябва да се характеризират с ограничен брой на употреба (този брой се определя от производителя, но той трябва да бъде под 240).
- DEX_302 Ако функцията по обезпечаване на сигурността на зададеното състояние на системата разпределя криптографски ключове, тя трябва да изпълнява тази задача, като спазва определени методи на разпределение на криптографски ключове.

5. Определяне на механизмите за сигурност

Изискваните механизми за сигурност са предмет на точно описание в Допълнение 11.

Другите механизми за сигурност трябва да бъдат определени от производителя на зададеното състояние за оценка на системата.

Допълнение 11

ОБЩИ МЕХАНИЗМИ ОТНОСНО СИГУРНОСТТА

СЪДЪРЖАНИЕ

1.	Общи положения	240
1.1.	Изходна база	240
1.2.	Начини на записване и съкращения	241
2.	Криптографски системи и алгоритми	242
2.1.	Криптографски системи	242
2.2.	Криптографски алгоритми	242
2.2.1.	Алгоритъм RSA	242
2.2.2.	Алгоритъм за сегментиране	242
2.2.3.	Алгоритъм за криптиране на данни	242
3.	Ключове и сертификати	242
3.1.	Генериране и разпределение на ключове	242
3.1.1.	Генериране и разпределение на ключове RSA	242
3.1.2.	Ключове за контрол RSA	244
3.1.3.	Ключове на датчика за движение	244
3.1.4.	Генериране и разпределение на ключове за сесия T-DES	244
3.2.	Ключове	244
3.3.	Сертификати	244
3.3.1.	Съдържание на сертификатите	245
3.3.2.	Издадени сертификати	246
3.3.3.	Проверка и разкриване съдържанието на сертификатите	247
4.	Механизъм на взаимно удостоверяване	247
5.	Конфиденциалност, цялост и механизми за удостоверяване на данните, прехвърляни между блоковете, монтирани на превозни средства, и картите	250
5.1.	Защитен от неотризиран достъп обмен на съобщения	250
5.2.	Обработка на грешки при защитения от неотризиран достъп обмен на съобщения	251
5.3.	Алгоритъм за изчисляване на сумите за криптографски контрол	252
5.4.	Алгоритъм за изчисляване на криптограмите, предназначени за инструкциите DO за конфиденциалност	252
6.	Механизми за поставяне на цифров подпис на прехвърлянията на данни	253
6.1.	Генериране на подписи	253
6.2.	Проверка на подписите	253

1. ОБЩИ ПОЛОЖЕНИЯ

Настоящото допълнение указва механизмите за сигурност, които гарантират:

- взаимното удостоверяване между блоковете UEV и тахографските карти, включително съгласуването на ключовете за сесия,
- конфиденциалността, целостта и удостоверяването на данните, прехвърляни между блоковете UEV и тахографските карти,
- цялостта и удостоверяването на данните, прехвърляни от блоковете UEV към външни запамятаващи устройства,
- целостта и удостоверяването на данните, прехвърляни от тахографските карти към външните запамятаващи устройства.

1.1. Изходна база

В настоящото допълнение се използва следната изходна база:

SHA-1	National Institute of Standards and Technology (NIST). FIPS Публикация 180-1: Secure Hash Standard. Април 1995 г.
PKCS1	RSA Laboratories. PKCS 1: RSA Encryption Standard. Версия 2.0. Октомври 1998 г.
TDES	National Institute of Standards and Technology (NIST). FIPS Публикация 46-3: RSA Encryption Standard. Проект за стандарт 1999 г.
TDES-OP	ANSI X9.52, Triple Data Encryption Algorithm Modes of Operation. 1998 г.
ISO/CEI 7816-4	IT — Идентификационни карти — Карти с вградена/и интегрална/и схема/и с контакти — Част 4: междумодулни команди за обмен на данни. Първо издание: 1995 г.+ изменение и допълнение 1: 1997 г.
ISO/CEI 7816-6	IT — Идентификационни карти — Карти с вградена/и интегрална/и схема/и с контакти — Част 6: елементи, свързани с междумодулни данни. Първо издание: 1996 г. + Cor 1: 1998 г.
ISO/CEI 7816-8	IT — Идентификационни карти — Карти с вградена/и интегрална/и схема/и с контакти — Част 8: междумодулни команди, свързани със сигурността. Първо издание: 1999 г.
ISO/CEI 9796-2	IT — Техники, свързани със сигурността — Схеми на цифров подпис с възстановяване на съобщението — Част 2: механизми, които използват функция за сегментиране. Първо издание: 1997 г.
ISO/CEI 9798-3	IT — Техники, свързани със сигурността — Механизми за удостоверяване на устройства — Част 3: удостоверяване на устройство, което използва алгоритъм с публичен ключ. Второ издание: 1998 г.
ISO 16844-3	Пътни превозни средства — Тахографски системи — Част 3: Интерфейс за откриване на движение.

1.2. Начини на записване и съкращения

Следващите съкращения и начини на записване се използват в настоящото допълнение:

(K_a , K_b , K_c)	Група от ключове, предназначени за тройния алгоритъм за криптиране на данни
CA	Сертифициращ орган
CAR	Референтни данни на сертифициращия орган
CC	Сума за криптографски контрол
CG	Криптограма
CH	Заглавна част на команда
CHA	Разрешение на притежател на сертификат
CHR	Референтни данни за притежателя на сертификат
D()	Декриптиране с DES (/Data Encryption Standard)
DE	Елемент на данни
DO	Обект за данни
d	Частен ключ — Степенен показател на частния ключ RSA
e	Публичен ключ — Степенен показател на публичен ключ RSA
E()	Криптиране с DES
EQT	Оборудване
Hash()	Стойност на сегментиране в качеството й на изходна стойност от <i>hash</i>
Hash	Функция Hash
KID	Идентификатор на ключ
K_m	Ключ TDES. Главен ключ, определен в стандарт ISO 16844 -3
$K_{m_{VU}}$	Ключ TDES, записан в блоковете, монтирани на превозното средство
$K_{m_{WC}}$	Ключ TDES, записан в цеховите карти
m	Указател за представяне на съобщение, цяло число между 0 и $n-1$
n	Ключове RSA, по модул
PB	Байтове за запълване
PI	Байт за указване на запълване (използван в криптограмите, предназначени за инструкциите за конфиденциалност DO)
PV	Обикновена стойност
s	Указател за представяне на подписа, цяло число между 0 и $n-1$
SSC	Брояч на изпратени последователности
SM	Защитен от неотризиран достъп обмен на съобщения
TCBC	Режим на работа чрез свързване на блокове от кодирани данни TDEA
TDEA	Троен алгоритъм за криптиране на данни
TLV	Дължина на маркерите
VU	Блок, монтиран на превозното средство
X.C	Сертификат на потребителя X, издаден от сертифициращия орган
X.CA	Сертифициращ орган на потребителя X
X.CA.PK ₀ X.C	Операция по разкриване съдържанието на сертификат с цел извличане на публичен ключ от него. Става дума за непостоянен оператор, операндът отляво на който отговаря на публичния ключ на даден сертифициращ орган, а операндът отдясно отговаря на сертификата, издаден от същия орган. Като резултат се получава публичният ключ на потребителя X, чийто сертификат представлява операндът отдясно.

X.PK	Публичен ключ RSA на потребителя X
X.PK[I]	Криптиране RSA на някои информации I с помощта на публичния ключ на потребителя X
X.SK	Частен ключ RSA на потребителя X
X.SK[I]	Криптиране RSA на някои информации I с помощта на частния ключ на потребителя X
'xx'	Стойност в шестнадесетичен формат
	Оператор за конкатенация.

2. КРИПТОГРАФСКИ СИСТЕМИ И АЛГОРИТМИ

2.1. Криптографски системи

CSM_001 Блоковете, монтирани на превозните средства и тахографските карти, трябва да използват класическа криптографска система с публичен ключ RSA за осигуряване на следните механизми за сигурност:

- взаимно удостоверяване между блоковете, монтирани на превозните средства, и тахографските карти,
- маршрутизация на тройните ключове за сесия DES (Data Encryption Standard) между блоковете, монтирани на превозните средства, и тахографските карти,
- цифров подпис на данните, прехвърляни върху външните запаметяващи устройства от блоковете, монтирани на превозните средства, или от тахографските карти.

CSM_002 Блоковете, монтирани на превозните средства, и тахографските карти трябва да използват симетрична криптографска система троен DES за осигуряване на механизъм, който да гарантира целостта на данните по време на обмена на данни на потребител между блоковете, монтирани на превозните средства и тахографските карти и за да осигури, при необходимост, конфиденциалността на обменените данни между блоковете, монтирани на превозните средства, и тахографските карти.

2.2. Криптографски алгоритми

2.2.1. Алгоритъм RSA

CSM_003 Алгоритъмът RSA се определя най-пълно чрез следните отношения:

$$X.SK[m] = s = m^d \text{ mod } n$$

$$X.PK[s] = m = s^e \text{ mod } n$$

За по-подробно описание на функцията RSA, потърсете информация в референтния документ PKCS1.

Степенният публичен показател „e“ за изчисляването на RSA трябва да бъде различен от 2 във всички ключове, генерирани с RSA.

2.2.2. Алгоритъм за сегментиране

CSM_004 Механизмите за цифровия подпис трябва да използват алгоритъма за сегментиране SHA-1 така, както е определен в референтния документ SHA-1.

2.2.3. Алгоритъм за криптиране на данни

CSM_005 Алгоритми DES трябва да се използват при режим на свързване на кодирани блокове.

3. КЛЮЧОВЕ И СЕРТИФИКАТИ

3.1. Генериране и разпределение на ключове

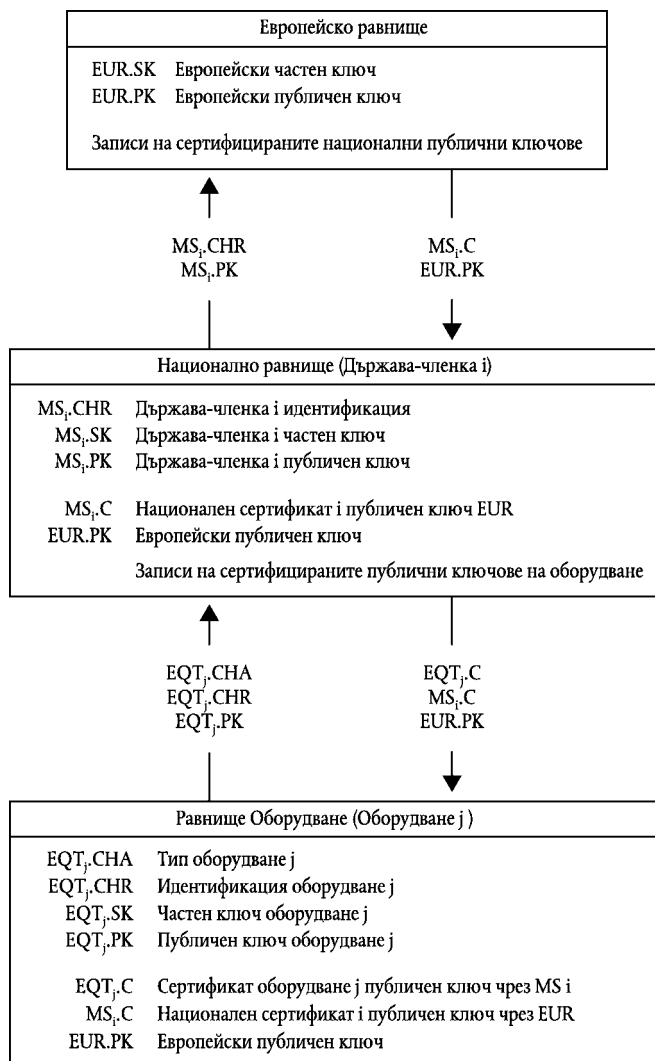
3.1.1. Генериране и разпределение на ключове RSA

CSM_006 Ключовете RSA трябва да се генерират на три йерархични функционални равнища:

- европейско равнище,
- равнище на държавата-членка,
- равнище на оборудване.

- CSM_007 На европейско равнище трябва да се генерира само една двойка европейски ключове (EUR.SK и EUR.PK). Европейският частен ключ трябва да позволи сертифицирането на публичните ключове на държавите-членки. Трябва се съхраняват записите на всички сертифицирани ключове. Тези задачи трябва да се изпълняват от европейски сертифициращ орган, поставен под контрола и отговорността на Европейската комисия.
- CSM_008 На равнище на държава-членка трябва да се генерира само една двойка ключове за държава-членка (MS.SK и MS.PK). Публичните ключове на държавите-членки трябва да бъдат сертифицирани от европейския сертифициращ орган. Частният ключ на държавата-членка трябва да позволи сертифицирането на частните ключове, които се въвеждат в оборудването (блок, монтиран на превозното средство, или тахографска карта). Записи на всички сертифицирани публични ключове трябва да бъдат съхранявани с данните за идентифициране на оборудването, за което те са предназначени. Тези задачи трябва да се изпълняват от национален сертифициращ орган. Всяка държава-членка има право да сменя периодично двойките ключове.
- CSM_009 На равнището на оборудването трябва да се генерира и въвежда само една двойка ключове във всяко оборудване (EQT.SK и EQT.PK). Публичните ключове на оборудването трябва да бъдат сертифицирани от националния сертифициращ орган. Тези задачи трябва да се изпълняват от производителите на оборудването, персонализаторите на оборудването или от компетентните власти в национален мащаб. Тази двойка ключове трябва да се използва от услугите по удостоверяване, по цифровия подпис и по криптирането.
- CSM_010 Конфиденциалността на частните ключове трябва да се запази през периода на тяхното генериране, тяхното (евентуално) маршрутизиране и тяхното архивиране.

Функционалната схема, която следва, представя синтез на движението на данните, характеризиращо този процес:



3.1.2. Ключове за контрол RSA

CSM_011 За целите на изпитанията на оборудване (включително изпитания за възможност за взаимна работа), сертифициращият европейски орган трябва да генерира най-малко една различна европейска двойка ключове за контрол и две двойки национални ключове за контрол, публичните ключове на които трябва да се сертифицират съвместно с европейския частен ключ за контрол. Производителите трябва да въведат в оборудването, което е в процес на типово сертифициране, ключове за тестване, които са сертифицирани от един от националните ключове за тестване.

3.1.3. Ключове на датчика за движение

Конфиденциалността на трите ключа TDES, описани по-долу, трябва да бъде защитена по подходящ начин по време на генерирането, на транспортирането (ако е необходимо) и на съхранението.

За да се позволи използването на апаратури за контрол, които отговарят на стандарта ISO 16844, европейският сертифициращ орган и сертифициращите власти на държавата-членка трябва също да съблюдават следните аспекти:

CSM_036 Европейският сертифициращ орган генерира ключовете $K_{m_{VU}}$ и $K_{m_{WC}}$, два тройни ключа DES, които са уникални и независими, както и ключа K_m по формулата:

$$K_m = K_{m_{VU}} \text{ XOR } K_{m_{WC}}$$

Европейският сертифициращ орган предава тези ключове при съблюдаване на съответни процедури, осигуряващи защита срещу неоторизиран достъп, на властите на държавите-членки, компетентни относно сертифицирането, които са направили искане за тях.

CSM_037 Сертифициращите органи на държавите-членки:

- използват ключа K_m за криптирането на данните на датчика за движение, поискани от производителите на датчиците за движение (данните за криптиране с ключа K_m са определени в стандарт ISO 16844-3),
- предават ключа $K_{m_{VU}}$ на производителите на блокове за монтиране на превозните средства при съблюдаване на съответните процедури, осигуряващи защита срещу неоторизиран достъп, за да бъдат инсталирани в тези UEV,
- следят ключ $K_{m_{WC}}$ да бъде инсталиран във всички цехови карти `SensorInstallationSecData` в елементарния файл `Sensor_Installation_Data` по време на персонализацията на картата.

3.1.4. Генериране и разпределение на ключове за сесия T-DES

CSM_012 По време на процеса по взаимното удостоверяване блоковете, монтирани на превозните средства, и тахографските карти трябва да генерират и обменят необходимите данни за изработването на общ ключ за сесия T-DES. Конфиденциалността на този обмен на данни трябва да бъде защитена от механизъм за криптиране RSA.

CSM_013 Този ключ трябва да се използва по време на всички последващи операции, които са свързани със защитен срещу неоторизиран достъп обмен на съобщения. Неговата валидност трябва да изтече в края на сесията (изваждане или реинициализиране на картата) и/или след 240 употреби (определение за употребата на ключа: изпращане на команда, която използва защитен срещу неоторизиран достъп обмен на съобщения към съответната карта и свързаният с това изпращане отговор).

3.2. Ключове

CSM_014 Ключовете RSA трябва да имат (независимо от нивото им) следните дължини: модули n 1024 бита, публичен степенен показател e максимум 64 бита, частен степенен показател d 1024 бита.

CSM_015 Ключовете T-DES трябва да имат формата (K_a, K_b, K_a) , където K_a и K_b са независими ключове с дължина 64 бита. Никакъв бит за откриване на грешка в четността не трябва да бъде със стойност 1.

3.3. Сертификати

CSM_016 Сертификатите, свързани с публичните ключове RSA, трябва да бъдат от типа „non self-descriptive“ и „card verifiable“ (Справка: стандарт ISO/CEI 7816-8)

3.3.1. Съдържание на сертификатите

CSM_017 Сертификатите, свързани с публичните ключове RSA, трябва да съдържат следните данни в следващия ред:

Данни	Формат	Байтове	Наблюдения
CPI	ЦЯЛО ЧИСЛО	1	Идентификатор на профил на сертификата ('01' за тази версия)
CAR	НИЗ ОТ БАЙТОВЕ	8	Референтни данни за сертифициращия орган
CNA	НИЗ ОТ БАЙТОВЕ	7	Разрешение на притежателя на сертификата
EOV	Реално време	4	Изтичане на валидността на сертификата. Опционално, 'FF', попълнен с байтовете за запълване в случай на неизползване
CHR	НИЗ ОТ БАЙТОВЕ	8	Референтни данни за притежателя на сертификата
n	НИЗ ОТ БАЙТОВЕ	128	Публичен ключ (модул)
e	НИЗ ОТ БАЙТОВЕ	8	Публичен ключ (публичен степенен показател)
		164	

Забележки:

1. „Идентификатор за профил на сертификата“ (CPI) определя точната структура на даден сертификат за удостоверяване. Той изпълнява функция на вътрешен идентификатор на оборудване в съответен заглавен списък, който описва конкатенацията на елементите на информация, съдържащи се в сертификата.

Заглавният списък, свързан със съдържанието на този сертификат, има следния вид:

„4D“	„16“	„5F 29“	„01“	„42“	„08“	„5F 4B“	„07“	„5F 24“	„04“	„5F 20“	„08“	„7F 49“	„05“	„81“	„81 80“	„82“	„08“
Tag на разширения заглавен списък	Дължина на заглавния списък	Tag CPI	Дължина CPI	Tag CAR	Дължина CAR	Tag CNA	Дължина CNA	Tag EOV	Дължина EOV	Tag CHR	Дължина CHR	Tag на публичен ключ (Конструиран)	Дължина на последващите DO	Модул	Дължина на модула	Степенен публичен показател	Дължина на степенния публичен показател

2. „Референтните данни за сертифициращия орган“ (CAR) позволяват идентифицирането на ОН, който издава сертификата, по такъв начин, че елементът на информация да може да извършва едновременно функцията на идентификатор на ключ, на който може да се има доверие, отправящ към публичния ключ на сертифициращия орган (за повече информация относно кодирането трябва да се види „Идентификатор на ключ“, описан по-долу).
3. „Разрешението на притежателя на сертификата“ (CNA) позволява идентифицирането на правата на притежателя на сертификата. Той се състои от идентификатор на тахографско приложение и на типа на оборудването, за което е предназначен съответният сертификат (в зависимост от елемента на информация EquipmentType, „00“ за дадена държава-членка).
4. „Референтните данни за притежателя на сертификата“ (CHR) позволяват уникалното идентифициране на притежателя на сертификата по такъв начин, че елементът на информация да може да извършва едновременно функцията на идентификатор на ключ на субект, отправящ към публичния ключ на притежателя на сертификата.
5. Идентификаторите на ключ идентифицират единствено притежателите на сертификат или сертифициращите органи. Те се кодират, както следва:

5.1. Оборудване (UEV или карта):

Данни	Сериен номер на оборудването	Дата	Тип	Производител
Дължина	4 байта	2 байта	1 байт	1 байт
Стойност	Цяло число	Кодиране DCB мм	Фабрични характеристики	Код на производителя

Ако се отнася до определен UEV, производителят трябва, по време на заявката за сертификати, да знае или не идентификационните данни на оборудването, в което ще бъдат инсталирани ключовете.

В първия случай производителят трябва да изпрати идентификационните данни на оборудването, придружени от публичния ключ на националния орган, компетентен относно сертифицирането. Сертификатът в такъв случай трябва да съдържа идентификационните данни на разглежданото оборудване. Производителят трябва да следи съответните ключове и сертификат да бъдат въведени в разглежданото оборудване. Идентификаторът на ключ има формата, указана по-горе.

Във втория случай производителят трябва да идентифицира индивидуално всяко искане за сертификат и да изпрати съответните идентификационни данни, придружени от публичния ключ на националния орган, компетентен относно сертифицирането. Сертификатът в такъв случай трябва да съдържа идентификационните данни на съответната заявка за сертификат. Производителят трябва да съобщи на свой ред на националния орган, компетентен относно сертифицирането, данните относно предназначението на ключовете във връзка с разглежданото оборудване (тоест идентификационните данни на заявката за сертификат и идентификационните данни на визираното оборудване) след тяхното инсталиране на това оборудване. Идентификаторът на ключ има формата, указана по-долу.

Данни	Сериен номер на искането за сертификат	Дата	Тип	Производител
Дължина	4 байта	2 байта	1 байт	1 байт
Стойност	Кодиране DCB	Кодиране DCB мм дд	'FF'	Код на производителя

5.2. Сертифициращ орган:

Данни	Идентификация на органа	Сериен номер на ключа	Допълнителна информация	Идентификатор
Дължина	4 байта	1 байт	2 байта	1 байт
Стойност	1 байт цифров код за националността 3 байта буквено-цифров код за националността	Цяло число	Допълнително кодиране (зависи от ОН) 'FF FF' в случай на неизползване	'01'

Сериенният номер на даден ключ позволява да се прави разлика между различните ключове на определена държава-членка в случай, че някои от тях бъдат променени.

6. Проверителите на сертификатите трябва да знаят по подразбиране, че сертифицираният публичен ключ е от тип RSA, който се използва за удостоверяване, проверка и криптиране на цифровите подписи с цел осигуряване на конфиденциалност (сертификатът не съдържа никакъв „Обектен идентификатор“, позволяващ неговото прецизиране).

3.3.2. Издадени сертификати

CSM_018 Издаденият сертификат има формата на цифров подпис, придружен от частично възстановяване на съдържанието на сертификата съгласно стандарт ISO/CEI 9796-2, като „Референтните данни относно сертифициращия орган“ затварят сертификата.

$$X.C = X.CA.SK[6A] || C_r || Hash(Cc) || BC || C_n || X.CAR$$

$$\text{Съдържание на сертификата} = C_c = \begin{matrix} C_r & || & C_n \\ 106 \text{ Bytes} & & 58 \text{ Bytes} \end{matrix}$$

Забележки:

1. Този сертификат съдържа 194 байта.
2. CAR, които са маскирани от подписа, се добавят също така към него, за да може публичният ключ на сертификационния орган да бъде избран за извършване на проверката на сертификата.
3. Проверителят на сертификата трябва да познава по подразбиране алгоритъма, използван от сертифициращия орган за подписване на сертификата.

4. Заглавният списък, свързан с този издаден сертификат, има следния вид:

„7F 21“	„09“	„5F 37“	„81 80“	„5F 38“	„3A“	„42“	„08“
Таг на сертификата CV (конструиран)	Дължина на последващите DO	Таг на подписа	Дължина на подписа	Таг на останалата част	Дължина на останалата част	Таг CAR	Дължина CAR

3.3.3. Проверка и разкриване съдържанието на сертификатите

Проверката и разкриването на съдържанието на сертификатите се състои в проверка на подписа съгласно стандарт ISO/CEI 9796-2, и в извличане на съдържанието на сертификата и на публичния ключ, който той съдържа: X.PK = X.CA.PK₀X.C, комплект, използван за проверка на валидността на сертификата.

CSM_019 Тази процедура съдържа следните операции:

Проверка на подписа и извличане на съдържанието:

- $X.C = \text{Sign}_{128 \text{ Bytes}} \parallel C_n'_{58 \text{ Bytes}} \parallel \text{CAR}'_{8 \text{ Bytes}}$
- $\text{ft CAR}'$ се избира публичният ключ на съответния сертифициращ орган (при положение че тази операция не е била извършена с други средства),
- Отваря се Sign . с публичния ключ на ОН: $Sr' = X.CA.PK [\text{Sign}]$,
- проверява се дали Sr' започва с '6A' и завършва с 'BC'
- изчислява се Cr' и H' въз основа на: $Sr' = '6A' \parallel C_r'_{106 \text{ Bytes}} \parallel H'_{20 \text{ Bytes}} \parallel 'BC'$
- възстановява се съдържанието на сертификата $C' = Cr' \parallel Cn'$,
- проверява се *Сегментирането* ($C' = H'$).

Ако резултатите от проверките са удовлетворителни, сертификатът е оригинален и съдържанието му е C' .

Проверява се валидността. От C' :

- контролира се, при необходимост, датата на изтичане на валидността.

От сертификата C' се извлича и се запамятава публичният ключ, идентификаторът на ключа, разрешението на притежателя на сертификата и датата на изтичане на валидността на сертификата:

- $X.PK = n \parallel e$,
- $X.KID = CHR$,
- $X.CHA = CHA$,
- $X.EOV = EOV$.

4. МЕХАНИЗЪМ ЗА ВЗАИМНО УДОСТОВЕРЯВАНЕ

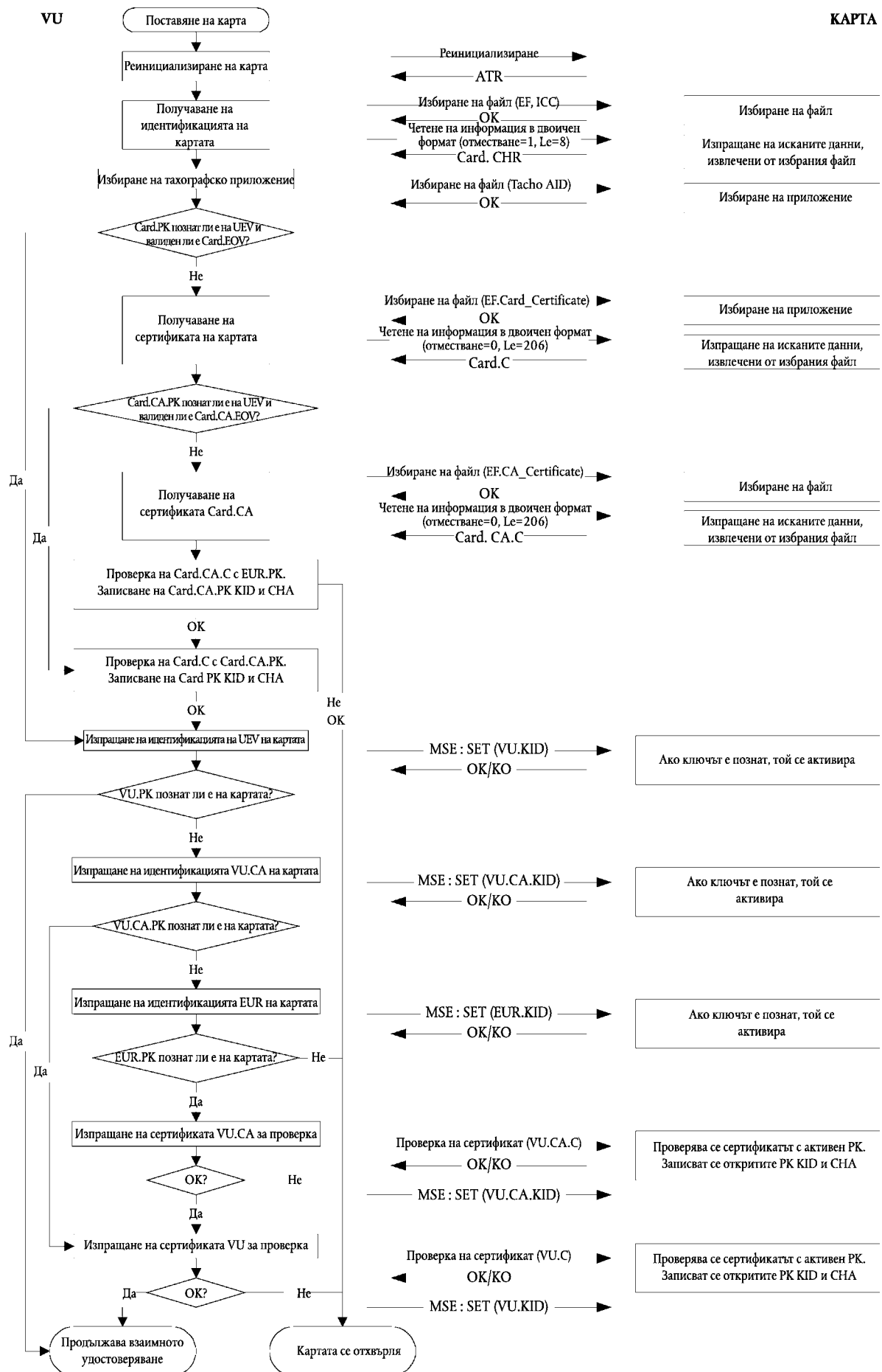
Взаимното удостоверяване между картите и UEV се основава на следния принцип:

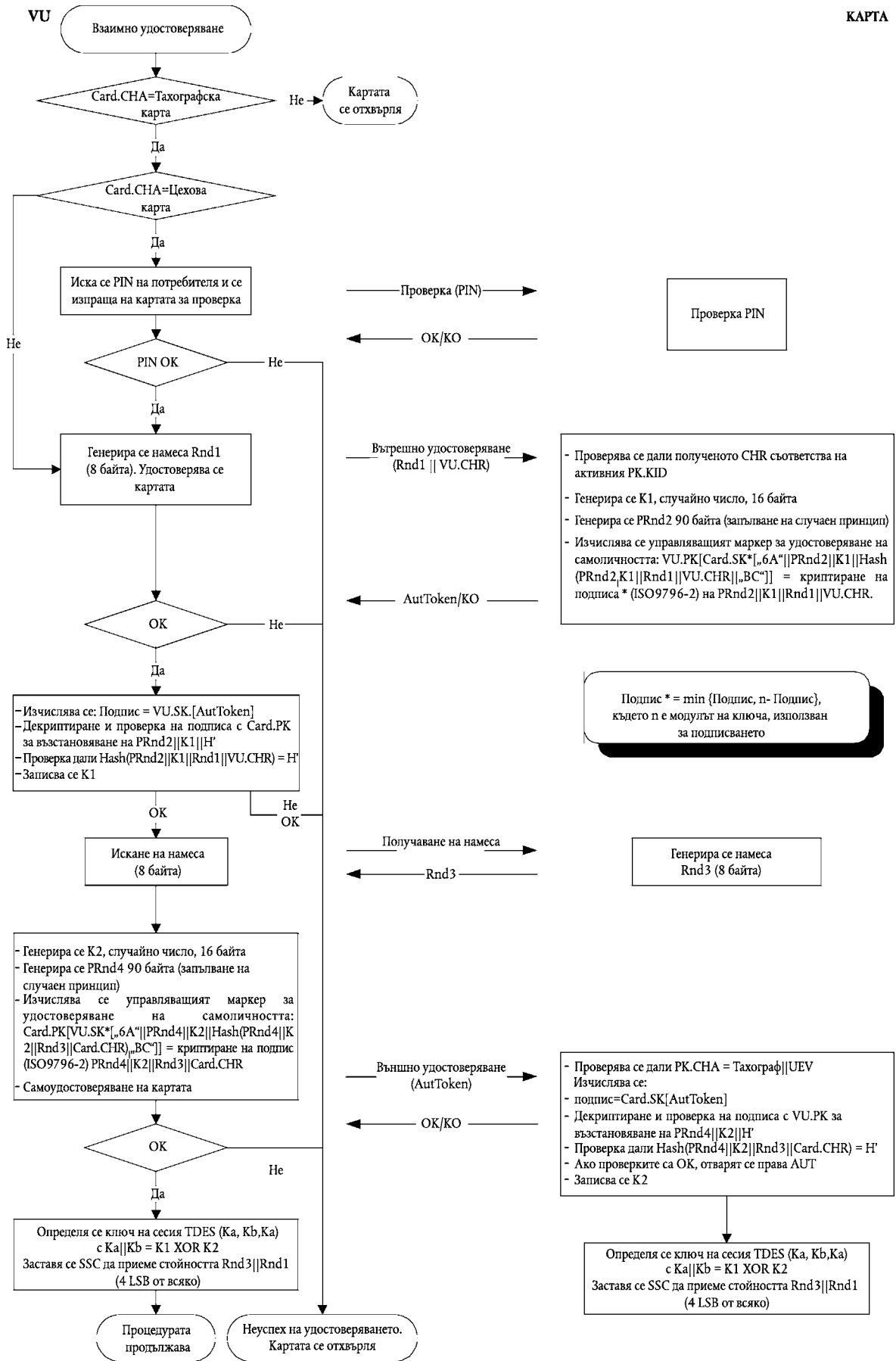
Всяка от страните трябва да докаже на другата, че притежава двойка валидни ключове, като публичният ключ, който е позволил тяхното сертифициране от компетентния национален сертифициращ орган, на свой ред е сертифициран от европейския сертификационен орган.

Това доказване се състои в подписване с частния ключ на случайно число, изпратено от ответната страна, която трябва да възстанови по време на проверката на този подпис изпратеното преди това случайно число.

Съответният блок, монтиран на превозното средство, стартира механизма на удостоверяване след поставянето на картата. Процедурата започва с размяна на сертификатите и разкриването на съдържанието на публичните ключове; тя завършва с определянето на ключа на сесията.

CSM_020 Използва се протоколът, даден по-долу [стрелките указват обменените команди и данни (виж Допълнение 2)]:





5. КОНФИДЕНЦИАЛНОСТ, ЦЯЛОСТ И МЕХАНИЗМИ ЗА УДОСТОВЕРЯВАНЕ НА ДАННИТЕ, ПРЕХВЪРЛЕНИ МЕЖДУ БЛОКА, МОНТИРАН НА ПРЕВОЗНОТО СРЕДСТВО, И КАРТИТЕ

5.1. **Защитен от неоторизиран достъп обмен на съобщения**

- CSM_021 Целостта на данните, прехвърлени между UEV и картите, се предпазва от устройство за защитен от неоторизиран достъп обмен на съобщения, в съответствие със стандартите ISO/CEI 7816-4 и ISO/CEI 7816-8.
- CSM_022 Ако се налага защита на данните по време на трансфера им, системата трябва да добави обект за данни от типа на сумата за криптографски контрол към обектите за данни, предадени в командата или отговора. Приемашата страна трябва да извърши проверка на сумата за криптографски контрол.
- CSM_023 Сумата за криптографски контрол на данните, предадени в команда, трябва да включва заглавната част на тази команда, както и всички изпратени обекти за данни ($= > \text{CLA} = '0C'$, и всички обекти за данни трябва да бъдат оградени от тагове, в рамките на които $b1 = 1$).
- CSM_024 Байтовете за състояние/информация, предадени като отговор, трябва да бъдат защитени от сума за криптографски контрол, ако този отговор не съдържа никакво поле за данни.
- CSM_025 Сумите за криптографски контрол трябва да имат дължина от 4 байта.

Така че при използване на защитения от неоторизиран достъп обмен на съобщения, командите и отговорите имат следната структура:

Използваните инструкции DO представляват частичен комплект от DO на защитения от неоторизиран достъп обмен на съобщения, описани в разпоредбите на стандарт ISO/CEI 7816-4:

Tag	Мнемоничен код	Значение
'81'	T_{PV}	Обикновена стойност, не кодирана в BER-TVL (трябва да бъде защитена от CC)
'97'	T_{LE}	Стойност на L_e в незащитена от неоторизиран достъп команда (трябва да бъде защитена от CC)
'99'	T_{SW}	Информация за състоянието (трябва да бъде защитена от CC)
'8E'	T_{CC}	Сума за криптографски контрол
'87'	$T_{PI\ CG}$	Байт, показател на запълването Криптограма (обикновена стойност, не кодирана в BER-TVL)

При наличие на следната двойка отговори на дадена незащитена от неоторизиран достъп команда:

Заглавна част на командата (CH)	Тяло на командата
CLA INS P1 P2	[поле L_c] [поле за данни] [поле L_e]
Четири байта	Байтове L , указващи от V_1 до V_L

Тяло на отговора	Завършваща част на отговора
[поле за данни]	SW1 SW2
Байтове за данни L_r	Два байта

Съответстващата двойка отговори на дадена защитена от неоторизиран достъп команда се представя по следния начин:

Защитена от неоторизиран достъп команда:

Заглавна част на командата (CH)	Тяло на командата										
CLA INS P1 P2	[ново поле L_c]	[ново поле за данни]									[ново поле L_e]
'0C'	Дължина на новото поле за данни	T_{PV}	L_{PV}	PV	T_{LE}	L_{LE}	L_e	T_{CC}	L_{CC}	CC	'00'
'81'		L_c	Поле за данни	'97'	'01'	L_e	'8E'	'04'	CC		

Данни, които трябва да се включат в сумата за криптографски контрол = CH || PB || T_{PV} || L_{PV} || PV || T_{LE} || L_{LE} || L_c || PB

PB = байтове за запълване (80 .. 00) съгласно стандарти ISO-CEI 7816-4 и ISO 9797, метод 2.

PV и LE на инструкциите DO са налични единствено ако незащитената от неоторизиран достъп команда съдържа определен брой съответстващи данни.

Защитен от неоторизиран достъп отговор:

1. Случай, когато полето за данни на отговора не е празно и не изисква никаква защита с цел запазване на конфиденциалността:

Тяло на отговора						Завършваща част на отговора
[ново поле за данни]						Ново SW1 SW2
T _{PV}	L _{PV}	PV	T _{CC}	L _{CC}	CC	
'81'	L _T	Поле за данни	'8E'	'04'	CC	

Данни, които трябва да се включат в сумата за криптографски контрол = T_{PV} || L_{PV} || PV || PB

2. Случай, когато полето за данни на отговора не е празно, но изисква защита, гарантираща неговата конфиденциалност:

Тяло на отговора						Завършваща част на отговора
[ново поле за данни]						Ново SW1 SW2
T _{PI CG}	L _{PI CC}	PI CG	T _{CC}	L _{CC}	CC	
'87'		PI CG	'8E'	'04'	CC	

Данни, които се маршрутизират чрез CG: данни, които не са кодирани в BER-TLV, и байтове за запълване.

Данни, които трябва да се включат в сумата за криптографски контрол = T_{PI CG} || L_{PI CG} || PI CG || PB

3. Случай, когато полето за данни на отговора е празно:

Тяло на отговора						Завършваща част на отговора
[ново поле за данни]						Ново SW1 SW2
T _{SW}	L _{SW}	SW	T _{CC}	L _{CC}	CC	
'99'	'02'	Ново SW1 SW2	'8E'	'04'	CC	

Данни, които трябва да се включат в сумата за криптографски контрол = T_{SW} || L_{SW} || SW || PB

5.2. Обработка на грешките при защитения от неоторизиран достъп обмен на съобщения

CSM_026 Ако тахографската карта разпознава грешка от тип MS по време на интерпретирането на определена команда, байтовете за състояние трябва да бъдат върнати без MS. Съгласно стандарт ISO/CEI 7816-4 се определят следните байтове за състояние за указване проявата на грешки от тип MS:

'66 88' Неуспешна проверка на сумата за криптографски контрол,

'69 87' Липса на предвидените обекти за данни MS,

'69 88' Неправилни обекти за данни MS.

CSM_027 Ако тахографската карта върне байтове за състояние без или с грешни инструкции DO MS, UEV трябва да прекрати текущата сесия.

5.3. Алгоритъм за изчисление на сумите за криптографски контрол

CSM_028 Съставянето на суми за криптографски контрол се извършва с помощта на подробната процедура за контрол на достъпа до носителя на информация (MAC) в съответствие със стандарт ANSI X9.19 за криптиране DES:

- начален етап: контролният блок y_0 е $E(K_a, SSC)$,
- последващ етап: контролните блокове y_1, \dots, y_n се изчисляват с помощта на K_a ,
- финален етап: сумата за криптографски контрол се изчислява въз основа на последния контролен блок y_n , като се процедира по следния начин: $E[K_a, D(K_b, y_n)]$.

където съкращението $E()$ означава криптирането с DES, а съкращението $D()$ — декриптирането с DES.

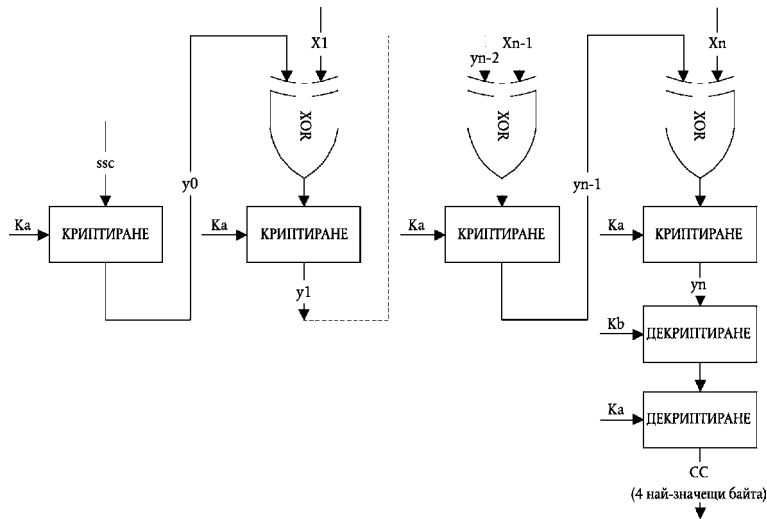
Извършва се трансфер на четирите най-значещи байта на сумата за криптографски контрол.

CSM_029 Броячът на изпратените последователности (SSC) се стартира по време на процедурата по приемане на ключовете:

Начален SSC: Rnd3 (4 най-незначещи байта) || Rnd1 (4 най-незначещи байта).

CSM_030 Броячът на изпратените последователности се увеличава с една единица преди изчисляването на всеки MAC (с други думи, свързаният с първата команда SSC отговаря на началния SSC + 1, докато свързаният с първия отговор SSC отговаря на началния SSC + 2).

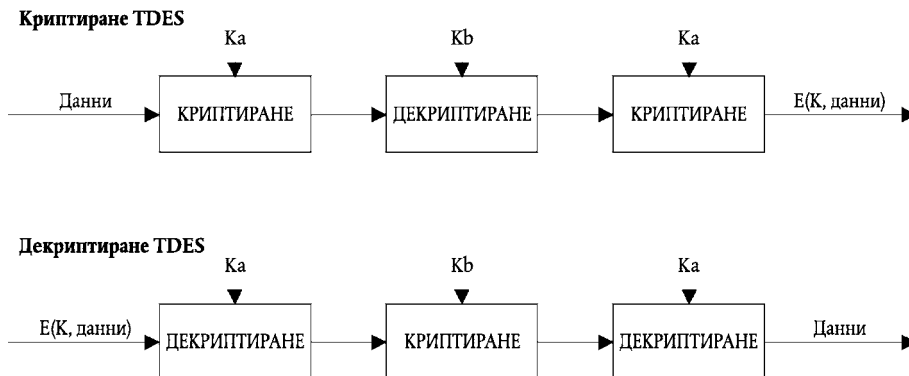
Следващата фигура показва подробно процедурата по изчисляването на MAC:



5.4. Алгоритъм за изчисление на криптограмите, предназначени за инструкциите DO, свързани с конфиденциалността

CSM_031 Тези криптограми се изчисляват с помощта на TDEA в експлоатационен режим TCBC съгласно референтните TDES и TDES-OP и с нулев вектор като блок на начална стойност.

Следващата фигура показва прилагането на ключовете в TDES:



6. МЕХАНИЗМИ ЗА ПОСТАВЯНЕ НА ЦИФРОВ ПОДПИС НА ПРЕХВЪРЛЯНИЯТА НА ДАННИ

CSM_032 Специализирано логическо устройство (IDE) записва във файл с физически данни данните, прехвърлени от определено оборудване (UEV или карта) по време на сесия по трансфер. Този файл трябва да съдържа сертификатите MS₁.C и EQT.C. Той трябва да съдържа и цифровите подписи, свързани с блоковете данни, съгласно указанията, дадени в Допълнение 7 (Протоколи за предаване на данни).

CSM_033 Цифровите подписи на прехвърлените данни трябва да се основават на използването на схема за цифров подпис с допълнение, която позволява при необходимост прехвърлените данни да се четат без никакво декриптиране.

6.1. Генериране на подписи

CSM_034 Генерирането от оборудването на цифровите подписи на данните трябва да съблюдава схемата за цифров подпис с допълнение, определена в референтния документ PKCS1 с функцията за сегментиране SHA-1:

$$\text{Подпис} = \text{EQT.SK}[\text{'00'} \parallel \text{'01'} \parallel \text{PS} \parallel \text{'00'} \parallel \text{DER}[\text{SHA-1}(\text{данниData})]$$

PS Низ от байтове за запълване със стойност 'FF', дължината на който е равна на 128.

DER(SHA-1(M)) съответства на кодирането на идентификатора на алгоритъма на функцията за сегментиране и стойността на сегментиране при стойност ASN.1 от типа DigestInfo (различни правила за кодиране):

'30' || '21' || '30' || '09' || '06' || '05' || '2B' || '0E' || '03' || '02' || '1A' || '05' || '00' || '04' || '14' || стойност на сегментиране.

6.2. Проверка на подписите

CSM_035 Проверката на цифровите подписи на данните, на която се подлагат прехвърлените данни, трябва да съблюдава схемата за цифров подпис с допълнение, определена в референтния документ PKCS1 с функцията за сегментиране SHA-1.

Проверителят трябва да познава (и да одобри) европейския публичен ключ EUR.PK.

Следващата таблица показва протокола, който дадено оборудване IDE, имащо карта за контрол, трябва да може да спазва, за да проверява целостта на данните, които са прехвърлени и записани в ESM (външно запамятащо устройство). Картата за контрол позволява извършването на декриптирането на цифровите подписи. В настоящия случай тази функция не е инсталирана по подразбиране в IDE.

Оборудването, което е взело участие в прехвърлянето и в подписването на данните, които трябва да се анализират, се указва от съкращението EQT.

