

Nařízení komise (ES) č. 1360/2002

ze dne 13. června 2002

kterým se posedmé adaptuje technickému pokroku nařízení Rady (EHS) č. 3821/85
o záznamových zařízeních v silniční dopravě

(Text s významem pro EHP)

Commission Regulation (EC) No. 1360/2002 of 13 June 2002 adapting for the seventh time to
technical progress Council Regulation /EEC) No. 3821/85 on recording equipment in road transport
(text with EEA relevance)

KOMISE EVROPSKÝCH SPOLEČENSTVÍ,

s ohledem na Smlouvu o založení Evropského společenství,

s ohledem na nařízení Rady (EHS) č. 3821/85 ze dne 20. prosince 1985 o
záznamovém zařízení v silniční dopravě¹, naposledy pozměněné nařízením (ES) č.
2135/98², a zejména na článek 17 a 18 tohoto nařízení,

vzhledem k těmto důvodům:

- 1) že technická ustanovení přílohy I(B) nařízení (EHS) č. 3821/85 by se mělo
přizpůsobit technickému pokroku se zvláštní pozorností na všeobecnou
bezpečnost systému a na možnost vzájemné spolupráce mezi záznamovým
zařízením a kartou řidiče;
- 2) že přizpůsobování zařízení také vyžaduje přizpůsobování přílohy II nařízení
(EHS) č. 3821/85, která definuje značení a certifikáty schválení;
- 3) že výbor, ustavený článkem 18 nařízení (EHS) č. 3821/85, nedodal
k opatřením podle návrhu stanovisko a že proto Komise dodala Radě návrh,
který se k těmto opatřením vztahuje;
- 4) že po vypršení období, stanoveném v článku 18 odst. 5 písm. b směrnice
č. 381/85, Rada nejednala a že je proto na Komisi, aby opatření přijala,

PŘIJALA TOTO NAŘÍZENÍ:

¹ Úř. věst. č. L 370, 31. 12. 1985, s. 8.

² Úř. věst. č. L 274, 9. 10. 1998, s. 1.

Článek 1

Příloha nařízení (ES) č. 2135/85 se nahrazuje přílohou tohoto nařízení.

Článek 2

Příloha II nařízení (EHS) č. 3821/85 se mění takto:

1. Kapitola I, bod 1, první pododstavec se mění takto:
 - smluvní označení Řecka 'GR' se nahrazuje označením '23',
 - smluvní označení Irska 'IRL' se nahrazuje označením '24',
 - doplňuje se smluvní označení '12' pro Rakousko,
 - doplňuje se smluvní označení '17' pro Finsko,
 - doplňuje se smluvní označení '5' pro Švédsko.
2. Kapitola I, bod 1, druhý pododstavec se mění takto:
 - za slova 'záznamový list' se vkládají slova 'nebo karty tachografu'.
3. Kapitola I, bod 2 se mění takto:
 - za slova 'záznamovém listu' se vkládají slova 'a na každé kartě tachografu'.
4. V kapitole II se do nadpisu doplňují následující slova 'PRO VÝROBKÝ ODPOVÍDAJÍCÍ PŘÍLOZE I'.
5. Vkládá se následující kapitola III:

'III. CERTIFIKÁT SCHVÁLENÍ VÝROBKŮ, KTERÉ ODPOVÍDAJÍ PŘÍLOZE IB'.

Stát, který udělil schválení, vydá žadateli certifikát schválení, jehož vzor je uveden níže. Při informování ostatních členských států o vydaných schváleních, nebo pokud vznikne takový případ o odejmutí schválení, musí příslušný členský stát užívat kopie tohoto certifikátu.

CERTIFIKÁT SCHVÁLENÍ VÝROBKŮ, ODPOVÍDAJÍCÍCH PŘÍLOZE IB

Název příslušného správního orgánu:

Oznámení, týkající se³:

☐ schválení

³ Zaškrtněte příslušné obdélníky.

- ☐ odejmutí
 - ☐ vzoru záznamového zařízení
 - ☐ součásti záznamového zařízení⁴
 - ☐ karty řidiče
 - ☐ dílenské karty
 - ☐ karty společnosti
 - ☐ karty kontrolora
-

Číslo schválení:

1. Obchodní značka výrobce:
2. Název vzoru:
3. Název výrobce:
4. Adresa výrobce:
5. Ke schválení dodáno dne:
6. Laboratoř (laboratoře):
7. Datum a číslo zkoušky (zkoušek):
8. Datum schválení:
9. Datum odejmutí schválení:
10. Vzor záznamového zařízení, pro jejichž užití je součást (součásti) konstruována:
11. Místo:
12. Datum:
13. Přiložené popisné dokumenty:
14. Poznámky (včetně umístění případných plomb)

.....

(podpis)

Článek 3

Toto nařízení vstupuje v platnost dvacátým dnem po vyhlášení v *Úředním věstníku Evropských společenství*.

⁴ Uved'te součást, o které se v oznámení jedná.

Toto nařízení je závazné ve svém celku a je přímo využitelné ve všech členských státech.

V Bruselu dne 13. června 2002.

Za Komisi
Loyola DE PALACIO
místopředseda

*PŘÍLOHA**PŘÍLOHA IB***POŽADAVKY NA KONSTRUKCI, ZKOUŠENÍ INSTALOVÁNÍ A INSPEKCI****OBSAH**

I.	Definice	9
II.	Obecné vlastnosti a funkce záznamového zařízení	16
1.	Obecné vlastnosti	16
2.	Funkce	16
3.	Provozní režimy	17
4.	Bezpečnost	19
III.	Konstrukční a funkční požadavky na záznamové zařízení	20
1	Vkládání a vyjímání provozní karty	20
2	Měření rychlosti a vzdálenosti	20
2.1	Měření ujeté vzdálenosti	20
2.2	Měření rychlosti	21
3.	Měření času	21
4.	Monitorování činnosti řidiče	22
5.	Monitorování jízdního statutu řízení vozidla	22
6.	Řidičem ručně vkládané údaje	23
6.1	Vložení údaje o místě počátku a/nebo ukončení denní práce	23
6.2	Ruční vkládání údajů o činnostech řidiče	23
6.3	Vkládání údajů o specifických podmínkách	25
7.	Ovládání funkce uzamčení společností	25
8.	Monitorování kontrolních činností	26
9.	Zjišťování událostí a/nebo závad	26
9.1	Vložení neplatné karty	26
9.2	Vložení neodpovídající karty	26
9.3	Překrytí časových údajů	26
9.4	Jízda bez vložení příslušné karty	26
9.5	Vložení karty při jízdě vozidla	27
9.6	Situace, kdy není správně ukončena posledně vložená karta	27
9.7	Situace zjištění překročení povolené rychlosti	27

9.8	Přerušení elektrického napájení	27
9.9	Chybná data o pohybu vozidla	27
9.10	Pokus o porušení bezpečnosti systému	27
9.11	Chybná karta	28
9.12	Chyba záznamového zařízení	28
10.	Vestavěné zkoušky a autotesty	28
11.	Načítání z paměti dat	28
12.	Zaznamenávání a ukládání do paměti dat	29
12.1	Údaje identifikující zařízení	29
12.1.1	Identifikační data celku ve vozidle	29
12.1.2	Identifikační data snímače pohybu	30
12.2	Bezpečnostní prvky	30
12.3	Data související s vložením a vyjmutím karty řidiče	30
12.4	Data o aktivitě řidiče	31
12.5	Místa, kde začíná a/nebo končí doba denní práce	32
12.6	Údaje měřiče ujeté vzdálenosti	32
12.7	Podrobná data o rychlosti	32
12.8	Údaje o událostech	32
12.9	Data o závadách	34
12.10	Kalibrační data	35
12.11	Data o nastavení času	36
12.12	Data o kontrolní činnosti	36
12.13	Data o uzamčení společností	36
12.14	Údaje o stahování dat	37
12.15	Údaje o specifických podmínkách	37
13.	Čtení z karet tachografu	37
14.	Zaznamenávání a uchovávání dat na kartě tachografu	38
15.	Zobrazování	38
15.1	Defaultové zobrazení	39
15.2	Zobrazení výstražných sdělení	40
15.3	Přístupové menu	40
15.4	Ostatní zobrazované informace	40
16.	Tisk	40
17.	Výstražná sdělení	42
18.	Stahování dat do externích médií	42

19.	Výstupní data pro přídavná externí media	43
20.	Kalibrace	43
21.	Seřízení času	44
22.	Funkční charakteristiky	44
23.	Materiály	45
24.	Značení	45
IV.	Konstrukční a funkční požadavky na karty tachografu	46
1.	Visuální údaje	46
2.	Bezpečnostní opatření	50
3.	Standardy	50
4.	Environmentální a elektrické specifikace	51
5.	Ukládání dat	51
5.1	Identifikace karty a bezpečnostní údaje	52
5.1.1	Identifikace použití	52
5.1.2	Identifikace čipu	52
5.1.3	Identifikace čipové karty	52
5.1.4	Bezpečnostní prvky	52
5.2	Karta řidiče	53
5.2.1	Identifikace karty	53
5.2.2	Identifikace držitele karty	53
5.2.3	Informace o řidičském průkazu	53
5.2.4	Údaje o použití vozidel	53
5.2.5	Údaje o řidičových činnostech	54
5.2.6	Místa, kde časy výkonu denní práce začínají a/nebo končí	54
5.2.7	Údaje o událostech	55
5.2.8	Údaje o závadách	56
5.2.9	Údaje o kontrolních činnostech	56
5.2.10	Údaje o použití karty	57
5.3	Dílenská karta	57
5.3.1	Bezpečnostní prvky	57
5.3.2	Identifikace karty	57
5.3.3	Identifikace držitele karty	57
5.3.4	Údaje o použitém vozidle	58
5.3.5	Údaje o řidičových činnostech	58
5.3.6	Začátek a/nebo ukončení doby denní činnosti řidiče	58

5.3.7	Údaje o událostech a závadách	58
5.3.8	Údaje o kontrolních činnostech	58
5.3.9	Údaje o kalibraci a nastavování času	58
5.3.10	Údaje o specifických podmínkách	59
5.4	Kontrolní karta	59
5.4.1	Identifikace karty	59
5.4.2	Identifikace držitele karty	59
5.4.3	Údaje o kontrolních činnostech	60
5.5	Karta společnosti	60
5.5.1	Identifikace karty	60
5.5.2	Identifikace držitele karty	60
5.3.3	Údaje o činnosti společnosti	60
V.	Instalace záznamového zařízení	62
1.	Instalace	62
2.	Instalační plaketa	62
3.	Zapečetění	63
VI.	Kontroly, inspekce a opravy	64
1.	Schvalování oprávněných montérů nebo servisních dílen	64
2.	Kontrola nových nebo opravených zařízení	64
3.	Instalační prohlídky	64
4.	Periodické kontroly	64
5.	Chyby měření	65
6.	Opravy	65
VII	Vydávání karet	66
VIII	Schválení typu záznamového zařízení a karet tachografu	67
1.	Obecná ustanovení	67
2.	Osvědčení o bezpečnosti	67
3.	Osvědčení o funkčnosti	67
4.	Osvědčení interoperability	68
5.	Osvědčení o schválení typu	69
6.	Výjimečný postup: první osvědčení interoperability	69

1. DEFINICE

V této příloze*:

- a) „**aktivací**“ se rozumí:
- fáze, ve které se záznamové zařízení stává plně funkčním a ve které zavádí veškeré funkce, včetně funkcí bezpečnostních;
- aktivace záznamového zařízení vyžaduje užití členské karty a vložení PIN kódu;*
- b) „**prokázáním totožnosti**“ se rozumí:
- funkce, určená ke stanovení a ověření uváděné identity;
- c) „**totožností**“ se rozumí:
- vlastnost, že informace přichází ze strany, jejíž identitu je možno ověřit;
- d) „**vestavěnou zkouškou (BIT – built-in-test)**“ se rozumí:
- zkouška, která proběhne na vyžádání, spouštěná obsluhou nebo externím zařízením;
- e) „**kalendářním dnem**“ se rozumí:
- den v době od 00,00 hod. do 24,00 hod. Veškeré kalendářní dny se vztahují k času UTC (universální koordinovaný čas);
- f) „**kalibrací**“ se rozumí:
- obnovení nebo potvrzení parametrů vozidla, které je třeba podržet v paměti údajů. Parametry vozidla zahrnují identifikaci vozidla (VIN – identifikační číslo vozidla, VRN – registrační číslo vozidla a registrace členského státu) a vlastnosti vozidla (w, k, l, rozměr pneumatik, nastavení omezovače rychlosti (pokud připadá v úvahu), průběžný UTC čas, současný údaj měřiče ujeté vzdálenosti);
- kalibrace záznamového zařízení vyžaduje členskou kartu;*
- g) „**číslem karty**“ se rozumí:
- šestnáctimístné alfanumerické označení, které v členském státu jednoznačně identifikuje kartu tachografu. Číslo karty zahrnuje (popřípadě) pořadový index, index náhrady a index obnovy;

* Pozn. překladatele: dále uvedené definice jsou abecedně řazeny podle definic v angličtině. Proto se jeví řazení v češtině nelogickým.

karta je tedy jednoznačně identifikována kódem vydávajícího členského státu a číslem karty;

h) „**pořadovým indexem karty**“ se rozumí:

čtrnáctimístné alfanumerické označení v čísle karty, které je užito pro rozlišení různých karet vydaných určité společnosti nebo organizaci, které mají právo na vydání více tachografových karet. Společnost nebo organizace je jednoznačně identifikovaná prvními třinácti znaky v čísle karty;

i) „**indexem obnovy karty**“ se rozumí:

šestnáctimístné alfanumerické označení v čísle karty, které je zvyšováno pokaždé, když je karta obnovována;

j) „**indexem náhrady karty**“ se rozumí:

patnáctimístné alfanumerické označení, které je zvyšováno pokaždé, když je karta nahrazována;

k) „**charakteristickým koeficientem vozidla**“ se rozumí:

číselné označení, které udává hodnotu výstupního signálu, vydávaného částí vozidla, která jej propojuje se záznamovým zařízením (výstup převodovky nebo náprava) a který je vyslán, když vozidlo ujede za standardních zkušebních podmínek vzdálenost 1 km (viz kapitolu VI(5)). Charakteristický koeficient se vyjadřuje v počtu impulsů na kilometr ($w = \dots \text{imp/km}$);

l) „**kartou společnosti**“ se rozumí:

karta tachografu, vydaná orgány určitého členského státu vlastníkově nebo držiteli vozidla, která je vložena do záznamového zařízení;

karta společnosti identifikuje společnost a umožňuje zobrazování a výtisk údajů, uložených v záznamovém zařízení, které bylo touto společností zablokováno;

m) „**konstantou záznamového zařízení**“ se rozumí:

číselné označení, udávající hodnotu vstupního signálu, požadovaného pro zobrazení a záznam ujeté vzdálenosti jednoho kilometru tato konstanta se vyjadřuje v počtu impulsů na kilometr ($k = \dots \text{imp/km}$);

n) „**průběžná doba jízdy**“ se vypočítává v záznamovém zařízení jako⁵:

průběžná doba jízdy, která se vypočítává jako běžná součtová doba jízdy určitého řidiče od konce jeho poslední POHOTOVOSTI nebo

⁵ Tento způsob výpočtu průběžné doby jízdy a úhrnné doby přestávek slouží v záznamovém zařízení pro výpočet varování o průběžné době jízdy. To však nenahrazuje zákonnou interpretaci, kterou je třeba uplatnit na tyto doby.

PŘESTÁVKY/ODPOČINKU nebo NEZNÁMÉ⁶ doby 45ti minut nebo doby delší (tato doba může být rozdělena do několika období po 15 minutách, nebo delších).

Příslušné výpočty berou podle potřeby v úvahu minulé aktivity, uložené na kartě řidiče. Pokud řidič nevložil svoji kartu, jsou příslušné výpočty podloženy údaji z paměťových záznamů, které se vztahují k běžné době, kdy nebyla vložena žádná karta a které se vztahují k odpovídajícímu otvoru pro kartu (slot);

- o) „**kontrolní kartou**“ se rozumí:

karta tachografu, vydaná orgány členského státu národní oprávněné kontrolní organizaci;

kontrolní karta identifikuje kontrolní organizaci a případně i kontrolora a umožňuje přístup k datům uloženým v paměti nebo na kartě řidiče pro čtení, tisk a/nebopřevod.

- p) „**celkovou dobou přestávek**“ se rozumí:

celková doba přestávek se z doby jízdy vypočítá z průběžných shromážděných dob DOSTUPNOSTI nebo PŘESTÁVKA/ODPOČINEK nebo NEZNÁMÉ⁵, které jsou dlouhé nebo delší než 45 min (toto období může být rozděleno na několik období dlouhých nebo delších než 15 min.)

Příslušné výpočty berou podle potřeby v úvahu minulé aktivity, uložené na kartě řidiče. Neznámé doby, nebo záporné doby trvání (počátek neznámé doby > konec neznámé doby) vzniklé překrytím mezi dvěma různými záznamovými zařízeními, se při výpočtu neberou v úvahu.

Pokud řidič nevložil svoji kartu, jsou příslušné výpočty podloženy údaji z paměťových záznamů, které se vztahují k běžné době, kdy nebyla vložena žádná karta a které se vztahují k odpovídajícímu otvoru pro kartu (slot);

- q) „**paměťí údajů**“ se rozumí:

zařízení elektronické paměti údajů, které je vestavěné v záznamovém zařízení;

- r) „**digitálním podpisem**“ se rozumí:

údaje, které jsou připojeny nebo kryptograficky transformovány do bloku dat a která příjemci bloku dat umožňují ověření totožnosti a úplnosti bloku dat;

⁶ NEZNÁMÁ doba odpovídá období, kdy není do záznamového zařízení vložena karta řidiče a po které nebyla z řidičovy aktivity vložen manuálně žádný údaj.

s) „**převedením**“ se rozumí:

zkopírování digitálního podpisu a části úplné sady dat, uložených v paměti údajů ve vozidle nebo v paměti karty tachografu;

převedení nemá měnit nebo vymazat jakékoliv uložené údaje;

t) „**kartou řidiče**“ se rozumí:

karta tachografu, vystavená orgány členského státu určitému řidiči;

karta řidiče identifikuje řidiče a umožňuje ukládání údajů o jeho aktivitách;

u) „**efektivním obvodem pneumatik kol**“ se rozumí:

průměrná vzdálenost ujetá každým z kol pohánějícími vozidlo (poháněná kola) v průběhu jedné ukončené otáčky. Tyto vzdálenosti musí být měřeny za normálních zkušebních podmínek (kapitola VI odst. 5) a vyjadřuje se ve tvaru: $l = \dots$ mm. Výrobci vozidla mohou měření těchto vzdáleností nahradit teoretickým výpočtem, který bere v úvahu rozložení hmotností na nápravy pro nenaložené vozidlo v provozním stavu⁷. Postupy pro tyto teoretické výpočty budou schváleny příslušným správním orgánem členského státu.

v) „**událostí**“ se rozumí:

mimořádná činnost detekovaná registračním zařízením, která může pocházet z pokusu o podvod;

w) „**závadou**“ se rozumí:

mimořádná činnost detekovaná registračním zařízením, která může pocházet z chybné funkce nebo z poruchy zařízení;

x) „**instalací**“ se rozumí:

montáž záznamového zařízení do vozidla;

y) „**snímačem pohybu**“^{*} se rozumí:

část záznamového zařízení, která zajišťuje signál odpovídající rychlosti vozidla a/nebo ujeté vzdálenosti vozidlem;

⁷ Směrnice 97/27/ES ze dne 22. července 1997, týkající se hmotností a rozměrů některých kategorií motorových vozidel a jejich přípojných vozidel, která mění směrnici 70/156/EHS (Úř. věst. č. L 233, 25. 8. 1997, s. 1.

^{*} Pozn. překl.: v německé verzi se užívá pojem „snímač rychlosti a ujeté dráhy“. V českém překladu zachováváme pojem podle verze anglické.

z) **„neplatnou kartou“** se rozumí:

karta, která je detekována jako závadná, nebo u které chybí úvodní prokázání totožnosti, nebo u které ještě nebylo dosaženo data platnosti, nebo u které již prošlo datum platnosti;

aa) **„mimo oblast působnosti“** se rozumí:

případ, kdy není podle ustanovení nařízení Rady (EHS) č. 3820/85 užívání záznamového zařízení požadováno;

bb) **„překročením rychlosti“** se rozumí:

překročení povolené rychlosti vozidla, které je definováno jako jakékoliv období delší než 60 s, ve kterém rychlost měřená vozidlem překračuje mezní hodnotu nastavení zařízení pro omezení rychlosti, které bylo stanovené směrnicí Rady 92/6/EHS ze dne 10. února 1992 pro montáž a užívání zařízení k omezování rychlosti určitých kategorií motorových vozidel ve Společenství⁸;

cc) **„periodickou kontrolou“** se rozumí:

sada operací ke kontrole, že záznamové zařízení správně pracuje a že jeho seřízení odpovídá parametrům vozidla;

dd) **„tiskárnou“** se rozumí:

součást záznamového zařízení, které zajišťuje vytištění uložených údajů;

ee) **„záznamovým zařízením“** se rozumí:

zařízení určené pro montáž do silničních vozidel pro automatické nebo poloautomatické zobrazení, záznam a ukládání podrobností o pohybu takovýchto vozidel a o určitých pracovních dobách jejich řidičů;

ff) **„obnovením“** se rozumí:

vydání nové karty tachografu v době, když existující karta dosáhla datum ukončení platnosti, nebo pokud je závadná a pokud je karta vrácena vydávající organizaci. Obnovení vždy zahrnuje ujištění, že neexistují dvě současně platné karty;

gg) **„opravením“** se rozumí:

oprava snímače pohybu nebo celku vozidla, která vyžaduje jeho odpojení od napájení nebo odpojení od jiných součástí záznamového zařízení nebo jeho otevření;

⁸ Úř. věst. č. L 57, 2. č. 1992, s. 27.

hh) **„náhradou“** se rozumí:

vydání karty tachografu jako náhrady za existující kartu, která byla prohlášena za ztracenou, zcizenou nebo poškozenou a která nebyla vrácena vydávající organizaci. Náhrada vždy zahrnuje riziko, že mohou existovat dvě současně platné karty;

ii) **„certifikací bezpečnosti“** se rozumí:

postup, kterým osvědčuje ITSC⁹ certifikační orgán, že zkoumané záznamové zařízení (nebo jeho součást) nebo karta tachografu plní bezpečnostní požadavky, stanovené v dodatku 10 Druhových bezpečnostních cílů;

jj) **„autotestem“** se rozumí:

zkouška, která pro detekci závad probíhá v záznamovém zařízení cyklicky a automaticky;

kk) **„kartou tachografu“** se rozumí:

programovatelná karta, určená k užití se záznamovým zařízením. Karta tachografu umožňuje v záznamovém zařízení identifikaci totožnosti (nebo skupiny totožností) držitele karty a umožňuje převod údajů a jejich ukládání. Karta tachografu může být následujícího typu:

- karta řidiče,
- kontrolní karta,
- dílenská karta,
- karta společnosti;

ll) **„schvalováním typu“** se rozumí:

postup, kterým členský stát osvědčuje, že zkoumané záznamové zařízení (nebo jeho součást) nebo karta tachografu plní požadavky tohoto nařízení;

mm) **„rozměrem pneumatiky“** se rozumí:

stanovení rozměrů pneumatik (vnějších hnacích kol) podle směrnice 92/23/EHS ze dne 31. března 1992¹⁰;

nn) **„identifikací vozidla“** se rozumí:

čísla, která vozidlo identifikují: registrační číslo vozidla (VRN) s údajem registrujícího členského státu a identifikační číslo vozidla (VIN)¹¹;

⁹ Doporučení Rady 95/144/ES ze dne 7. dubna 1995 o kritériích hodnocení obecné bezpečnosti informační technologie (Úř. věst. č. L 93, 26. 4. 1995, s. 27).

¹⁰ Úř. věst. č. L 129, 14. 5. 1992, s. 95.

oo) „**celkem ve vozidle (VU – celek ve vozidle)**“ se rozumí:

záznamové zařízení s výjimkou snímače pohybu a kabelů propojujících snímač pohybu. Celkem ve vozidle může být buď jediný celek nebo několik celků rozmístěných ve vozidle potud, pokud jeho části plní bezpečnostní požadavky tohoto nařízení;

pp) „**týdnem**“ se pro spolehlivost výpočtu v záznamovém zařízení rozumí:

období od 00,00 hodin UTC času v pondělí do 24,00 hodin UTC času v neděli;

qq) „**dílenskou kartou**“ se rozumí:

karta tachografu, vydaná organizací členského státu výrobcí záznamového zařízení, montážnímu podniku, výrobcí vozidla nebo provozovně, schválené členským státem;

dílenská karta identifikuje držitele karty a umožňuje zkoušení, kalibraci a/nebo převádění údajů v záznamovém zařízení.

¹¹ Směrnice 76/114/EHS ze dne 18. prosince 1975 o sbližování právních předpisů členských států týkajících se povinných štítků a nápisů pro motorová vozidla a pro jejich přípojná vozidla a pro jejich umístění a způsob upevnění

II. OBECNÉ VLASTNOSTI A FUNKCE ZÁZNAMOVÉHO ZAŘÍZENÍ

- 000 Jakékoliv vozidlo vybavené záznamovým zařízením, které vyhovuje podmínkám této přílohy, musí mít display rychloměru a měřič ujeté vzdálenosti. Tyto funkce mohou být součástí záznamového zařízení.

1. Obecné vlastnosti

Účelem záznamového zařízení je zaznamenávat, ukládat, zobrazovat, tisknout a být zdrojem údajů týkajících se činností řidiče.

- 001 Záznamové zařízení zahrnuje kabely, snímač pohybu a celek ve vozidle.

- 002 Celek ve vozidle zahrnuje řídicí jednotku, paměťovou jednotku, řídicí hodiny, dvě čtecí zařízení čipových karet (řidiče a druhého řidiče), tiskárnu, display, vizuální výstrahu, kalibrační/stahovací konektor a zařízení pro vkládání uživatelských údajů.

Záznamové zařízení může být propojeno s dalšími zařízeními přídavnými konektory.

- 003 Jakékoliv zapojení nebo propojení záznamového zařízení s jakoukoliv funkcí, zařízením nebo zařízeními, ať již schválenými nebo neschválenými nesmí ovlivňovat nebo být schopno ovlivňovat správný a bezpečný provoz nebo plnění podmínek nařízení.

Uživatelé záznamového zařízení se identifikují v zařízení prostřednictvím karet tachografu.

- 004 Záznamové zařízení zajišťuje selektivní přístupová práva datům a funkcím v závislosti na typu a/nebo identitě uživatele.

Záznamové zařízení zaznamenává a ukládá data do paměti dat a na karty tachografu.

Toto se děje v souladu se směrnicí 95/46/EC ze 24. října 1995 o ochraně osobnosti s ohledem na zpracování osobních a dat a volný pohyb takových dat^{12/}.

2 Funkce

- 005 Záznamové zařízení musí zajistit následující funkce:

- monitorování vkládání a vyjímání karet,
- měření rychlosti a ujeté vzdálenosti,

¹² Úř. věst. č. L 281, 23.11.1995, s. 31.

- měření času,
- monitorování činnosti řidiče,
 - monitorování provozního stavu,
 - údaje vkládané řidičem ručně:
 - vložení místa kde pracovního doba dne začíná a/nebo končí,
- ručně vkládané údaje o činnostech řidiče,
- záznam zvláštních podmínek,
- využívání možnosti uzamčení společnosti,
- monitorování kontrolních činností,
- zjišťování událostí a závad,
- vestavěné zkoušky a autotesty,
- načítání z paměti dat,
- zaznamenávání a ukládání do paměti dat,
- načítání z karet tachografu,
- zaznamenávání a ukládání dat na karty tachografu,
- zobrazování údajů,
- tisk,
- dávání výstrahy,
- stahování dat na externích media,
- výstup dat na přídatná externí zařízení,
- kalibraci,
- nastavení času.

3 Provozní režimy

006 Záznamové zařízení musí být schopno pracovat ve čtyřech režimech:

- provozní režim,
- kontrolní režim,
- kalibrační režim,

- režim společnosti.

007 Záznamové zařízení se přepíná do následujících provozních režimů podle platné karty tachografu vložené do čtecích zařízení:

Provozní režim		Otvor pro vložení karty řidiče				
		Bez karty	Karta řidiče	Kontrolní karta	Dílenská karta	Podniková karta
Otvor pro vložení karty druhého řidiče	Bez karty	Provozní	Provozní	Kontrolní	Kalibrační	Podnikový
	Karta řidiče	Provozní	Provozní	Kontrolní	Kalibrační	Podnikový
	Kontrolní karta	Kontrolní	Kontrolní	Kontrolní(*)	Provozní	Provozní
	Dílenská karta	Kalibrační	Kalibrační	Provozní	Kalibrační(*)	Provozní
	Podniková karta	Podnikový	Podnikový	Provozní	Provozní	Podnikový(*)
(*) V těchto situacích používá záznamové zařízení pouze kartu tachografu vloženou do řidičova otvoru pro vkládání karet.						

009 Záznamové zařízení musí ignorovat vložení neplatné karty, kromě zobrazování, tisku a stahování dat uložených na kartách s prošlým datem, které musí být možné.

010 Všechny funkce uvedené v seznamu v II.2 musí být aktivní v provozním režimu s následujícími výjimkami:

- kalibrační funkce je přístupná pouze v kalibračním režimu,
- funkce nastavení času je omezena pouze na případy, kdy záznamové zařízení není v kalibračním režimu,
- funkce ručního vkládání údajů řidičem je přístupná pouze v provozním a kalibračním režimu,
- ovládání možnosti uzamčení společnosti je přístupné pouze v podnikovém režimu;
- monitorování kontrolních činností je funkční pouze v kontrolním režimu;
- funkce stahování dat není přístupná v provozním režimu (s výjimkou specifikovanou v požadavku 150).

011 Záznamové zařízení může předat data na display, do tiskárny nebo na vnější rozhraní s následujícími výjimkami:

- v provozním režimu musí být jakékoliv identifikační údaje (příjmení nebo jméno(a)), které neodpovídají vložené kartě tachografu ignorována a jakékoliv číslo karty, neodpovídající vložené kartě tachografu, bude částečně ignorováno (každý lichý znak – odleva doprava – bude chybět),

- v podnikovém režimu mohou být data, vztahující se k osobě řidiče (požadavky 081, 084 a 087) dány k dispozici pouze v časových obdobích, která nejsou uzamčena jinou společností (jak je označeno prvními 13 místy číselného kódu podnikové karty),
- pokud není v záznamovém zařízení vložena žádná karta, data vztahující se k osobě řidiče jsou k dispozici pouze pro aktuální den a osm předcházejících dní.

4 Bezpečnost

Bezpečnost systému sleduje ochranu paměti záznamového zařízení takovým způsobem, aby se zabránilo neoprávněnému přístupu, manipulaci s daty a odhalení takového pokusu, stejně jako úplnost a autentičnost dat přenášených mezi snímačem pohybu a celkem ve vozidle, úplnost a autentičnost údajů přenášených mezi záznamovým zařízením a kartami tachografu a ověření úplnosti a autentičnosti stahovaných dat.

- 012 Aby se dosáhlo bezpečnosti systému, musí záznamové zařízení splnit bezpečnostní požadavky specifikované v generických bezpečnostních cílech snímače pohybu a celku ve vozidle (Příloha 10).

III. KONSTRUKČNÍ A FUNKČNÍ POŽADAVKY NA ZÁZNAMOVÉ ZAŘÍZENÍ

1 Vkládání a vyjímání provozní karty

- 013 Záznamové zařízení monitoruje identifikaci vkládání a vyjímání karty do čtecího zařízení karet.
- 014 Při vložení karty stanoví záznamové zařízení, zda vložená karta je platná karta tachografu a v takovém případě identifikuje typ karty.
- 015 Záznamové zařízení se navrhuje tak, že karty tachografu jsou zablokovány v pozici po správném vložení do rozhraní.
- 016 K uvolnění karet tachografu může dojít pouze po zastavení vozidla a příslušná data jsou uložena na kartách. Uvolnění karty musí vyžadovat aktivní zásah uživatele.

2 Měření rychlosti a vzdálenosti

- 017 Tato funkce měří nepřetržitě a musí být schopna dodávat údaje rychloměru odpovídající celkové vzdálenosti ujeté vozidlem.
- 018 Tato funkce nepřetržitě měří a je schopna udávat rychlost vozidla.
- 019 Funkce měření rychlosti musí být schopna dodávat informaci, zda je vozidlo v pohybu nebo zastavilo. Vozidlo se považuje za pohybující se, jakmile funkce registruje od snímače pohybu po dobu nejméně pěti vteřin více, nežli 1 impuls/sec. Jinak se vozidlo považuje za stojící.

Zařízení zobrazující rychlost (rychloměr) a měřidlo ujeté vzdálenosti (tachometr), instalovaná v jakémkoliv vozidle, které je vybaveno záznamovým zařízením, vyhovujícím ustanovením tohoto nařízení Komise, musí vyhovovat požadavkům týkajícím se maximálních tolerancí, které jsou uvedeny v této příloze (kapitola III(2)(1) a III(2)(2)).

2.1 Měření ujeté vzdálenosti

- 020 Ujetá vzdálenost může být měřena buď:
- tak, že se načítá dopředný i zpětný pohyb, nebo
 - že je brán v úvahu pouze dopředný pohyb.
- 021 Záznamové zařízení měří vzdálenost od 0 do 9 999 999,9 km.
- 022 Měření vzdálenosti se pohybuje v následujících tolerancích (vzdálenosti nejméně 1000 m):
- 1 % před instalací,

- 2 % při instalaci a periodické kontrole,
- 4 % v provozu.

023 Vzdálenost se měří s přesností lepší nebo rovnou 0.1 km.

2.2 Měření rychlosti

024 Záznamové zařízení musí měřit v rozsahu 0 až 220 km/hod.

025 Aby byla zajištěna maximální tolerance zobrazované rychlosti ± 6 km/hod a byly vzaty v úvahu:

- tolerance ± 2 km/hod u vstupních změn (proměnlivost pneumatik,...),
- tolerance ± 1 km/hod při měřeních provedených v průběhu instalace a periodických kontrolách,
- záznamové zařízení musí pro rychlosti ležící v rozmezí 20 až 180 km/hod a pro charakteristické koeficienty vozidla mezi 4000 až 25000 imp/hod, měřit rychlost s tolerancí ± 1 km/hod (při konstantní rychlosti).

Poznámka: Rozlišovací schopnost ukládání dat s sebou nese další toleranci $\pm 0,5$ km/hod u rychlosti vozidla ukládané záznamovým zařízením.

025a Rychlost se měří přesně s normální tolerancí během 2 vteřin po ukončení změny, jestliže změna proběhla při hodnotě akcelerace 2 m/s^2 .

026 Měření rychlosti se provádí s rozlišovací schopností lepší a nebo rovnou 1 km/hod.

3. Měření času

027 Funkce měření času musí měřit průběžně a udávat v digitální podobě údaje o referenčním čase UTC a čas.

028 UTC data a čas se musí použít pro průběžné datování záznamového zařízení.

029 Aby bylo možno zobrazit místní čas, musí se dát měnit posun zobrazovaného času s půlhodinovým krokem.

030 Zpoždování nebo zrychlování hodin nesmí překročit ± 2 vteřiny za den v podmínkách schvalování typu.

031 Měření času musí mít rozlišovací schopnost lepší nebo rovnou 1 vteřině.

032 Měření času nesmí být ovlivněno vypnutím externího elektrického napájení na dobu kratší nežli 12 měsíců v podmínkách schvalování typu.

4 Monitorování činnosti řidiče

- 033 Tato funkce musí nepřetržitě a nezávisle monitorovat činnost jednoho řidiče a jednoho druhého řidiče.
- 034 Řidičovy činnosti jsou JÍZDA, PRÁCE, POHOTOVOST a PŘESTÁVKA/ODPOČINEK.
- 035 Mělo by být umožněno řidiči a/nebo druhému řidiči ručně navolit režimy PRÁCE, POHOTOVOST a PŘESTÁVKA/ODPOČINEK.
- 036 Jestliže se vozidlo pohybuje, musí se JÍZDA nastavit automaticky pro řidiče a POHOTOVOST se musí automaticky nastavit u druhého řidiče.
- 037 Jestliže se vozidlo zastaví, musí se u řidiče automaticky nastavit režim PRÁCE.
- 038 První změna činnosti řidiče, která nastane v průběhu 120 vteřin po automatickém nastavení režimu PRÁCE v důsledku zastavení vozidla, musí být považována za příhodivší se v průběhu zastávky vozidla (proto je možné zrušení změny na režim PRÁCE).
- 039 Tato funkce předává informaci o změně činnosti s rozlišením 1 minutY.
- 040 Pokud se v dané kalendářní minutě objeví jakákoliv činnost v režimu JÍZDA, pak bude celá minuta považována za JÍZDU.
- 041 Pokud se v dané kalendářní minutě objeví jakákoliv činnost v režimu JÍZDA, jak v přímo předcházející a tak přímo následující minutě, pak musí být celá minuta považována za režim JÍZDA.
- 042 Pokud jde o danou kalendářní minutu, která není podle předcházejících kritérií považována za režim JÍZDA, pak musí být celá minuta považována za jeden stejný typ činnosti, jako nejdéle nepřetržitě trvající činnost v této minutě (nebo poslední ze stejně dlouho trvajících činností).
- 043 Tato funkce musí průběžně monitorovat nepřetržitý čas jízdy a načítaný čas doby přestávek řidiče.

5 Monitorování jízdního statutu řízení vozidla

- 044 Tato funkce musí průběžně a automaticky monitorovat jízdní statut řízení vozidla.
- 045 Statut řízení vozidla POSÁDKA se musí navolit, jestliže jsou v záznamovém zařízení vloženy dvě platné karty řidiče. V každém jiném případě se navolí statut řízení vozidla SAMOTNÝ ŘIDIČ.

6 Řidičem ručně vkládané údaje**6.1 Vložení údaje o místě počátku a/nebo ukončení denní práce**

- 046 Tato funkce musí umožnit vložení údaje o počátku a/nebo ukončení denní práce řidiče a/nebo druhého řidiče.
- 047 Místa jsou definována jako stát a, pokud je možné oblast.
- 048 V době vyjmutí řidičovy (nebo dílenské) karty vyzve záznamové zařízení (druhého) řidiče, aby vložil údaj o místě ukončení doby denní práce.
- 049 Záznamové zařízení musí umožnit, aby tento požadavek byl ignorován.
- 050 Musí být možné vložit místo začátku a/nebo ukončení doby denní práce bez karty a nebo v jiné době, nežli při vlastním vkládání a nebo vyjímání karty.

6.2 Ruční vkládání údajů o činnostech řidiče

- 050a V době vložení řidičovy (nebo dílenské) karty a pouze v této době záznamové zařízení musí:

- připomenout držiteli karty datum a čas posledního vyjmutí karty a
- požádat držitele karty, aby identifikoval, zda aktuální vložení karty představuje pokračování denní práce v aktuálním dni.

Záznamové zařízení musí umožnit držiteli karty tuto otázku ignorovat a neodpovědět, odpovědět pozitivně a nebo odpovědět i negativně.

- v případě, kdy držitel karty ignoroval otázku a neodpověděl, připomene záznamové zařízení držiteli karty „místo počátku doby denní práce“. Záznamové zařízení umožní ignorování tohoto požadavku. Pokud je místo vloženo, bude zaznamenáno do paměti dat, do karty tachografu a vztaheno k době vložení karty.
- v případě negativní a nebo pozitivní odpovědi záznamové zařízení vyzve držitele karty, aby vložil ručně typ činnosti zvolený pouze mezi PRÁCE, POHOTOVOST nebo PŘESTÁVKA/ODPOČINEK včetně času začátku a ukončení. Tyto údaje musí striktně odpovídat době mezi posledním vyjmutím karty a opětovným vložním, aniž by se činnosti překrývaly. Toto musí být provedeno v souladu s následujícím postupem:
- v případě pozitivní odpovědi držitele karty na otázku záznamové zařízení vyzve držitele karty k ručnímu vložení činností v chronologickém pořádku pro dobu mezi posledním vyjmutím a současným vložním karty. Postup je ukončen v okamžiku, kdy se ručně vložný čas ukončení shoduje s časem vložení karty.
- v případě negativní odpovědi držitele karty, musí záznamové zařízení:

- vyzvat držitele karty k ručnímu vložení činností v chronologickém pořádku pro dobu od vyjmutí karty do ukončení příslušné doby denní práce (nebo činností vztažených k vozidlu v případě, že doba denní práce pokračuje na záznamovém archu). Záznamové zařízení musí tedy dříve, nežli umožní držiteli karty ručně vložit každou činnost, vyzvat držitele karty k identifikaci, zda doba ukončení poslední zaznamenané činnosti představuje ukončení předcházející doby práce (viz poznámka níže).

Poznámky: v případě, že držitel vozidla nedeklaruje, kdy byla ukončena doba předcházející práce a ručně vloží činnost, jejíž doba ukončení se rovná času vložení karty, záznamové zařízení musí:

- předpokládá, že doba denní práce skončila v době začátku prvního ODPOČINKU (nebo zbývajícího času NEZNÁMÝ) po vyjmutí karty a nebo době vyjmutí karty jestliže žádná doba odpočinku nebyla vyznačena (a jestliže nezbývá žádná doba NEZNÁMÝ),
- předpokládá, že počáteční čas (viz níže) se rovná době vložení karty,
- postupuje podle níže uvedených kroků:
 - potom, jestliže doba ukončení času práce se liší od času vyjmutí karty, nebo jestliže nebylo vloženo místo ukončení doby denní práce v tomto čase, vybídne držitele karty, aby „potvrdil nebo vložil místo, kde byla denní práce ukončena“ (záznamové zařízení umožní ignorování této žádosti). Pokud je místo vloženo, bude zaznamenáno pouze do karty tachografu a pouze je-li odlišné od údaje vloženého v době vyjmutí karty (jestliže byl jeden údaj vložen) a byl vztažen k době ukončení doby denní práce,
 - potom vyzve držitele karty k „vyznačení počátku“ současné doby denní práce (nebo činností týkajících se příslušného vozidla v případě, že držitel karty předtím použil záznamový arch v průběhu této doby) a vyzve držitele karty ke vložení „místa, kde denní práce začíná“ (záznamové zařízení umožní ignorování tohoto požadavku). Pokud je tento údaj vložen, bude zaznamenán na kartu tachografu a vztažen k časovému údaji začátku. Pokud je tento počáteční časový údaj shodný s časem vložení karty, bude údaj o místě zaznamenán také do paměti dat,
 - potom, jestliže počáteční časový údaj se liší od doby vložení karty, vyzve držitele karty k ručnímu vložení činností v chronologické pořadí od tohoto počátečního stavu až do doby vložení karty,
 - záznamové zařízení potom umožní držiteli karty pozměňovat údaj jakékoliv činnosti ručně vložené až do ověření údaje volbou zvláštního příkazu a potom již nedovolí žádné podobné úpravy,
 - takové odpovědi na počáteční otázku, po které nenásleduje žádné vložení činnosti bude interpretováno záznamovým zařízením za ignorování otázky držitelem karty.

V průběhu celého postupu bude záznamové zařízení čekat na vložení údajů po dobu nepřesahující následující časové prodlevy:

- jestliže nedojde ke kontaktu s rozhraním záznamového zařízení pro vkládání údajů osobami v průběhu jedné minuty (s vizuálním i možným zvukovým výstražným signálem po 30 vteřinách nebo;
- jestliže je karta vyjmuta a nebo je vložena karta jiného řidiče (nebo dílenská karta) nebo,
- jestliže se vozidlo dá do pohybu,

v tomto případě záznamové zařízení potvrdí jakékoliv již vložené údaje.

6.3 Vkládání údajů o specifických podmínkách

050b Záznamové zařízení umožní řidiči vkládat v reálném čase dva údaje o specifických podmínkách:

- „MIMO ROZSAH PLATNOSTI“ (začátek, konec);
- „PŘEVOZ LODÍ / PŘEVOZ VLAKEM“

Záznam „PŘEVOZ LODÍ / PŘEVOZ VLAKEM“ se nesmí objevit, pokud je aktivovaný údaj „MIMO OBOR PLATNOSTI“.

7 Ovládání funkce uzamčení společností

051 Tato funkce umožňuje uzamčení společností a tím zablokování přístupu společností a vyhrazení možnosti vkládání údajů v podnikovém režimu pouze pro tuto společnost.

052 Uzamčení společností spočívá ve vložení data/času (uzamčení společností) a data/času (odemknutí společností) spojeného s identifikací společnosti, která je vyznačena číslem podnikové karty (při uzamčení společností).

053 Uzamčení aodemknutí společností může být provedeno pouze v reálném čase.

054 Uzamčení společností může být odemknuto pouze společností, kterou byl zámek uzamčen (identifikováno prvními 13 znaky v čísle podnikové karty) nebo,

055 odemknutí podnikového zámku se provede automaticky při uzamčení jinou společností.

055a V případě, že společnost provede uzamčení a předcházející uzamčení společností bylo provedeno toutéž společností, pak se předpokládá, že předcházející uzamčení společností nebylo ukončeno a stále pokračuje.

8 Monitorování kontrolních činností

- 056 Tato funkce musí monitorovat činnosti ZOBRAZOVÁNÍ, TISK a STAHOVÁNÍ DAT z celku ve vozidle nebo karty, které jsou prováděny v kontrolním režimu.
- 057 Tato funkce také monitoruje KONTROLU PŘEKROČENÍ POVOLENÉ RYCHLOSTI v kontrolním režimu. Činnost je považována za kontrolu překročení povolené rychlosti v případě, že v kontrolním režimu dojde k odeslání povelu k vytištění „překročení povolené rychlosti“ do tiskárny nebo zobrazovací jednotky a nebo data „události a závady“ jsou stahována z paměti celku ve vozidle.

9 Zjišťování událostí a/nebo závad

- 058 Tato funkce identifikuje následující události a/nebo závady:

9.1 Vložení neplatné karty

- 059 Tato událost se vyvolá vložení neplatné karty a/nebo karty s prošlým datem.

9.2 Vložení neodpovídající karty

- 060 Tato závada nastane, jestliže se vložení platné karty dosáhne kombinace označená v tabulce X:

Vložení neodpovídající karty		Otvor pro vložení karty řidiče				
		Bez karty	Karta řidiče	Kontrolní karta	Dílenská karta	Podniková karta
Otvor pro vložení karty druhého řidiče	Bez karty					
	Karta řidiče				X	
	Kontrolní karta			X	X	X
	Dílenská karta		X	X	X	X
	Podniková karta			X	X	

9.3 Překrytí časových údajů

- 061 Toto hlášení nastane, jestliže datum/čas posledního vyjmutí karty řidiče, které je přečteno na kartě je pozdější, nežli aktuální datum/čas záznamového zařízení, do kterého je karta vložena.

9.4 Jízda bez vložení příslušné karty

- 062 Toto hlášení nastane při jakékoliv z kombinací údajů karet tachografu označené v následující tabulce X, když se řidičova činnost mění na režim JÍZDA a nebo nastane změna režimu provozu v době nastaveného režimu řidičovy činnosti JÍZDA:

Jízda bez příslušné karty		Otvor pro vložení karty řidiče				
		Žádná nebo neplatná karta	Karta řidiče	Kontrolní karta	Dílenská karta	Podniková karta
Otvor pro vložení karty druhého řidiče	Žádná nebo neplatná karta	X		X		X
	Karta řidiče	X		X	X	X
	Kontrolní karta	X	X	X	X	X
	Dílenská karta	X	X	X		X
	Podniková karta	X	X	X	X	X

9.5 Vložení karty při jízdě vozidla

063 Toto hlášení nastane, jestliže je vložena karta tachografu do otvoru pro vkládání karet v době řidičovy činnosti JÍZDA.

9.6 Situace, kdy není správně ukončena poslední vložená karta

064 Toto hlášení nastane, jestliže při vložení karty záznamové zařízení zjistí, že přes opatření popsaná dále v odstavci III(1), předcházející doba vložení karty nebyla správným způsobem ukončena (karta byla vyjmuta dříve, nežli na ní byla uložena příslušná data). Tato situace musí být zjištěna pouze při vložení řidičovy a nebo dílenské karty.

9.7 Situace zjištění překročení povolené rychlosti

065 Toto hlášení nastane při každém překročení povolené rychlosti.

9.8 Přerušování elektrického napájení

066 Toto hlášení nastane při každém přerušování elektrického napájení snímače pohybu a celku ve vozidle delším nežli 200 milisekund, pokud zařízení není v kalibračním režimu. Prahová charakteristika hranice přerušování bude definována výrobcem. Pokles elektrického napájení v důsledku startování motoru vozidla nesmí být označeno za tuto událost.

9.9 Chybná data o pohybu vozidla

067 Toto hlášení nastane v případě přerušování normálního toku dat mezi snímačem pohybu a celkem ve vozidle a/nebo v případě chyby v úplnosti nebo totožnosti dat přenášovaných mezi snímačem pohybu a celkem ve vozidle.

9.10 Pokus o porušení bezpečnosti systému

068 Toto hlášení nastane v jakémkoliv jiném případě, který ohrožuje bezpečnost systému snímače pohybu a/nebo celku ve vozidle v oblasti generických bezpečnostních cílů těchto komponentů, pokud není zařízení v kalibračním režimu.

9.11 Chybná karta

- 069 Toto hlášení nastane kdykoliv bude v průběhu provozu zjištěna chyba karty tachografu.

9.12 Chyba záznamového zařízení

- 070 Toto hlášení nastane v případě jakékoliv následující závady, pokud zařízení není v kalibračním režimu:

- vnitřní chyba celku ve vozidle,
- chyba tiskárny,
- chyba zobrazovací jednotky,
- chyba snímače.

10 Vestavěné zkoušky a autotesty

- 071 Záznamové zařízení musí samo zjistit vlastní závady v průběhu vestavěných zkoušek a autotestů v souladu s následující tabulkou:

Zkouška subsystému	Autotest	Vestavěná zkouška
Software		Úplnost
Paměť dat	Přístup	Přístup, úplnost údajů
Čtení karet	Přístup	Přístup
Klávesnice		Ruční kontrola
Tiskárna	(u výrobce)	Vytisknout
Zobrazovací jednotka		Visuální kontrola
Stahování údajů (prováděné pouze v průběhu stahování)	Správná funkce	Správná funkce
Snímač	Správná funkce	

11 Načítání z paměti dat

- 072 Záznamové zařízení musí být schopno načíst jakékoliv údaje uložené v paměti dat.

12 Zaznamenávání a ukládání do paměti dat

Pro účely tohoto odstavce,

- „365 dní“ se definuje jako 365 kalendářních dnů průměrné činnosti řidiče ve vozidle. Průměrná činnost v průběhu dne ve vozidle se definuje jako nejméně 6 řidičů nebo druhých řidičů, šest cyklů vložení a vyjmutí karty a 256 změn činnosti. 365 dní tedy obsahuje minimálně 2190 (druhých) řidičů, 2190 cyklů vložení a vyjmutí karty a 93440 změn činnosti,
- časové údaje jsou zaznamenávány s rozlišovací schopností 1 minuty, pokud není stanoveno jinak,
- údaje měřiče ujeté vzdálenosti jsou zaznamenávány s rozlišovací schopností jednoho kilometru,
- údaje rychlosti jsou zaznamenávány s rozlišovací schopností 1 km/hod.

073 Údaje uložené do paměti údajů nesmí být ovlivněny přerušením elektrického napájení z vnějšího zdroje v rozsahu kratším nežli 12 měsíců v podmínkách schvalování typu.

074 Záznamové zařízení musí být schopno zaznamenávat a implicitně nebo explicitně ukládat do své paměti údajů následující data:

12.1 Údaje identifikující zařízení

12.1.1 Identifikační data celku ve vozidle

075 Záznamové zařízení musí být schopno ukládat do své paměti dat následující identifikační údaje o celku ve vozidle:

- jméno výrobce,
- adresa výrobce,
- číslo komponentu,
- výrobní číslo,
- číslo verze software,
- datum instalace aktuální verze software,
- rok výroby zařízení,
- číslo schválení typu.

076 Identifikační údaje o celku ve vozidle jsou zaznamenána a uložena jednou provždy výrobcem celku ve vozidle, s výjimkou dat vztahujících se k software a číslo schválení typu, které se může měnit v případě upgrade softwaru.

12.1.2 Identifikační data snímače pohybu

077 Snímač pohybu musí být schopen uložit do své paměti následující identifikační data:

- jméno výrobce,
- číslo součásti,
- výrobní číslo,
- číslo schválení typu,
- identifikátor vloženého bezpečnostního komponentu (např. číslo součásti vnitřního čipu/číslo procesoru),
- identifikátor operačního systému (např. číslo verze software).

078 Identifikační data snímače pohybu jsou zaznamenána a uložena výrobcem tohoto snímače jednou provždy do snímače.

079 Celek ve vozidle musí být schopen zaznamenat a uložit do své paměti dat následující párovací identifikační data snímače pohybu:

- výrobní číslo,
- číslo schválení typu,
- datum prvního párování.

12.2 Bezpečnostní prvky

080 Záznamové zařízení musí být schopno uložit následující bezpečnostní prvky:

- evropský veřejný klíč,
- certifikát členského státu,
- certifikát zařízení,
- soukromý klíč zařízení.

12.3 Data související s vložením a vyjmutím karty řidiče

081 Při každém cyklu vložení a vyjmutí karty řidiče a nebo dílenské karty musí záznamové zařízení zaznamenat a uložit do své paměti dat následující informace:

- jméno(a) a příjmení držitele karty ve formě uložení těchto informací na kartě,
- číslo karty, členský stát vydávající kartu a datum platnosti ve formě uložení těchto informací na kartě,

- datum a čas vložení karty,
 - hodnotu údaje na měřiči ujeté vzdálenosti v době vložení karty,
 - otvor pro vkládání karet, do kterého byla tato karta vložena,
- datum a čas vyjmutí karty,
- hodnotu údaje na měřiči ujeté vzdálenosti v době vyjmutí karty,
 - následující informace o posledním řidičem použitém vozidle ve formě uložení těchto informací na kartě:
 - registrační číslo vozidla a členský stát, kde bylo vozidlo registrováno,
 - datum a čas vyjmutí karty,
 - značku informující, zda při vložení karty vložil držitel karty ručně údaje o činnosti a nebo ne.

082 Paměť údajů musí být schopna podržet tyto informace nejméně po dobu 365 dní.

083 Jestliže je kapacita paměti vyčerpána, musí nová data nahradit nejstarší údaje.

12.4 Data o aktivitě řidiče

084 Záznamové zařízení musí zaznamenávat a ukládat do své paměti dat kdykoliv dojde ke změně činnosti u řidiče a/nebo druhého řidiče a/nebo dojde ke změně statutu řízení vozidla a/nebo je-li vsunuta nebo vyjmuta karta řidiče nebo dílenská karta:

- jízdní statut řízení vozidla (POSÁDKA, SAMOTNÝ ŘIDIČ),
- otvor pro vkládání karty (ŘIDIČ, DRUHÝ ŘIDIČ),
- statut karty v příslušném otvoru pro vkládání karet (VLOŽENA, NEVLOŽENA) (viz Poznámka),
- činnost (JÍZDA, POHOTOVOST, PRÁCE, PŘESTÁVKA/ ODPOČINEK),
- datum a čas změny.

Poznámka: VLOŽENA znamená, že platná karta řidiče nebo dílenská karta je vložena v otvoru pro vkládání karet. NEVLOŽENA znamená opak, tzn. žádná platná karta řidiče nebo dílenská karta není vložena v otvoru pro vkládání karet (např. podniková karta je vložena, nebo není vložena žádná karta).

Poznámka: Údaje o činnosti vložené ručně řidičem nejsou zaznamenávány do paměti údajů.

085 Paměť údajů musí být schopna uchovat data o činnostech nejméně po dobu 365 dní.

086 Jestliže je kapacita paměti vyčerpána, musí nová data nahradit nejstarší data.

12.5 Místa, kde začíná a/nebo končí doba denní práce

087 Záznamové zařízení musí zaznamenat a uložit do své paměti dat kdykoliv (druhý)řidič vloží místo začátku a/nebo ukončení denní práce:

- pokud přichází v úvahu, číslo karty (druhého)řidiče a členský stát, který vydal kartu,
- datum a čas vložení údajů (nebo datum/čas vztahující se ke vložení údajů, pokud byly vloženy ručně),
- typ vložených údajů (začátek a konec, podmínky vložení údajů),
- vložený údaj o zemi a oblast,
- hodnotu na měřiči ujeté vzdálenosti.

088 Paměť dat musí být schopna uchovat data o začátku a ukončení denní práce nejméně po dobu 365 dnů (za předpokladu, že jeden řidič vkládá data dvakrát za den).

089 Jestliže je kapacita paměti vyčerpána, musí nová data nahradit nejstarší data.

12.6 Údaje měřiče ujeté vzdálenosti

090 Záznamové zařízení musí zaznamenávat do své paměti dat hodnoty údajů měřiče ujeté vzdálenosti a odpovídající datum o půlnoci každého kalendářního dne.

091 Paměť dat musí být schopna ukládat hodnoty měřiče ujeté vzdálenosti o každé půlnoci nejméně po dobu 365 kalendářních dnů.

092 Jestliže je kapacita paměti vyčerpána, musí nová data nahradit nejstarší data.

12.7 Podrobná data o rychlosti

093 Záznamové zařízení musí zaznamenávat a uchovávat ve své paměti dat okamžitou rychlost vozidla a odpovídající datum a čas v každé vteřině po dobu nejméně 24 hodin, jestliže se vozidlo pohybuje.

12.8 Údaje o událostech

Pro účely tohoto pododstavce bude čas zaznamenáván s rozlišovací schopností 1 vteřiny.

094 Záznamové zřízení musí zaznamenávat a uchovávat ve své paměti dat následující údaje o každé zjištěné události podle následujících pravidel ukládání:

Událost	Pravidla ukládání dat	Data, která se ukládají při události
Nesoulad údajů karty	- 10 posledních událostí	- datum a čas zahájení události, - datum a čas ukončení události, - typ karty, číslo a vydávající členský stát každé karty vyvolávající nesoulad údajů.
Jízda bez náležité karty	- nejdelší událost pro každý z posledních 10 dnů, kdy došlo k nesouladu údajů, - pět nejdelších událostí v posledních 365 dnech.	- datum a čas zahájení události, - datum a čas ukončení události, - typ karty, číslo a vydávající členský stát každé karty vložené na začátku a/nebo na konci události, - počet podobných událostí v tomto dni.
Vložení karty v průběhu jízdy	- poslední událost pro každý z posledních 10 dnů, kdy došlo k nesouladu údajů.	- datum a čas události, - typ karty, číslo a vydávající členský stát, - počet podobných událostí v tomto dni.
Poslední použití karty, kdy nebyl režim korektně ukončen	- 10 posledních událostí	- datum a čas vložení karty, - typ karty, číslo a vydávající členský stát, - poslední použití karty přečtené z karty: - datum a čas vložení karty, - registrační číslo vozidla a členský stát registrace vozidla.
Překročení povolené rychlosti ⁽¹⁾	- nejzávažnější událost pro každý z posledních 10 dní (tj. jeden s nejvyšší průměrnou rychlostí), - pět nejzávažnějších událostí v posledních 365 dnech, - první událost, která nastala první po poslední kalibraci.	- datum a čas počátku události, - datum a čas ukončení události, maximální rychlost naměřená v průběhu události, - aritmetická průměrná rychlost změřená v průběhu události, - typ karty, číslo a členský stát vydávající kartu řidiče (pokud se dá použít), - počet podobných událostí v tomto dni.
Přerušování elektrického napájení ⁽²⁾	- nejdelší událost pro každý z posledních 10 dnů zaregistrování události, - pět nejdelších událostí v posledních 365 dnech.	- datum a čas počátku události, - datum a čas ukončení události, - typ karty, číslo a vydávající členský stát pro jakoukoliv kartu vloženou na začátku a/nebo na konci události, - počet podobných událostí v tomto dni.
Chybné údaje o pohybu vozidla	- nejdelší událost pro každý z posledních 10 dnů zaregistrování události,	- datum a čas počátku události, - datum a čas ukončení události, - typ karty, číslo a vydávající

	- pět nejdelších událostí v posledních 365 dnů.	členský stát pro jakoukoliv kartu vloženou na začátku a/nebo na konci události, - počet podobných událostí v tomto dni.
Pokus o porušení bezpečnostních opatření	- 10 posledních událostí pro každý typ události.	- datum a čas počátku události, - datum a čas ukončení události, - typ karty, číslo a vydávající členský stát pro jakoukoliv kartu vloženou na začátku a/nebo při ukončení události, - typ události.
<p>095 ⁽¹⁾Záznamové zařízení musí také zaznamenat a uchovat ve své paměti dat:</p> <ul style="list-style-type: none"> - datum a čas poslední KONTROLY PŘEKROČENÍ POVOLENÉ RYCHLOSTI, - datum a čas prvního překročení povolené rychlosti následující po KONTROLE PŘEKROČENÍ POVOLENÉ RYCHLOSTI, - počet událostí, při kterých došlo k překročení povolené rychlosti od poslední KONTROLY PŘEKROČENÍ POVOLENÉ RYCHLOSTI. <p>⁽²⁾ Tato data mohou být zaznamenávána pouze při opětném připojení elektrického napájení, časové údaje mohou být udávány s přesností jedné minuty.</p>		

12.9 Data o závadách

Pro účely tohoto pododstavce musí být čas zaznamenáván s přesností jedné vteřiny.

- 096 Záznamové zařízení se musí pokusit zaznamenat a uložit následující data pro každou zjištěnou závadu do své paměti podle následujících pravidel o ukládání dat:

Závada	Pravidla ukládání dat	Data, která se ukládají o závadě
Závada karty	- 10 posledních závad karty řidiče	- datum a čas počátku závady, - datum a čas konce závady, - číslo typu karty a vydávající členský stát.
Závada záznamového zařízení	- posledních závad karty řidiče pro každý typ závady, - první závady po poslední kalibraci.	- datum a čas počátku závady, - datum a čas konce závady, - typ závady, - číslo typu karty a vydávající členský stát jakékoliv karty vložené do záznamového zařízení na začátku a/nebo na konci závady.

12.10 Kalibrační data

097 Záznamové zařízení musí zaznamenávat a ukládat do své paměti dat data týkající se:

- známých kalibračních parametrů v okamžiku aktivace,
- jeho první kalibrace po aktivaci,
- první kalibraci v současném vozidle (identifikovaného vlastním VIN),
- pět posledních kalibrací (Jestliže se odehraje několik kalibrací v průběhu jednoho kalendářního dne, pak pouze poslední kalibrace bude zaznamenána).

098 Následující data budou zaznamenána pro každou z těchto kalibrací:

- důvod kalibrace (aktivace, první instalace, instalace, periodická prohlídka),
- název a adresa dílny,
- číslo dílenské karty, členský stát vydávající kartu a doba platnosti karty,
- identifikace vozidla,

aktualizované nebo potvrzené parametry: w, k, l, rozměr pneumatik, nastavení zařízení omezující rychlost vozidla, měřič ujeté vzdálenosti (stará a nová hodnota), datum a čas (stará a nová hodnota).

099 Snímač pohybu musí zaznamenávat a uchovávat ve své paměti dat následující instalační data snímače pohybu:

- první párování s celkem ve vozidle (datum, čas, číslo schválení typu celku ve vozidle, výrobní číslo celku ve vozidle),

- poslední párování s celkem ve vozidle (datum, čas, číslo schválení typu celku ve vozidle, výrobní číslo celku ve vozidle).

12.11 Data o nastavení času

100 Záznamové zařízení musí zaznamenávat a uchovávat ve své paměti dat údaje vztahující se k:

- času posledního nastavení času,
- pěti největším nastavením času od poslední kalibrace, provedené v kalibračním režimu mimo časový rámec pravidelných kalibrací (definice (f)).

101 Následující data musí být zaznamenávána pro každé z těchto nastavení času:

- datum a čas, stará hodnota,
- datum a čas, nová hodnota,
- název a adresa dílny,
- číslo členské karty, členský stát vydávající kartu a datum platnosti karty.

12.12 Data o kontrolní činnosti

102 Záznamové zařízení musí zaznamenávat a uchovávat ve své paměti dat následující data, která se vztahují k posledním 20 případům kontrolní činnosti:

- datum a čas kontroly,
- číslo kontrolní karty a členský stát vydávající kartu,
- typ kontroly (zobrazování a/nebo tisk a/nebo stahování dat z celku ve vozidle a/nebo stahování dat z karty).

103 V případě stahování dat budou zaznamenávána data o nejstarším a posledním stahování dat.

12.13 Data o uzamčení společností

104 Záznamové zařízení musí zaznamenávat a uchovávat ve své paměti dat následující údaje, týkající se 20 posledních případů použití uzamčení společností:

- datum a čas uzamčení společností,
- datum a čas odemknutí společností,
- číslo podnikové karty a členský stát vydávající kartu,

- název a adresa společnosti.

12.14 Údaje o stahování dat

105 Záznamové zařízení musí zaznamenávat a uchovávat ve své paměti data týkající se posledního stahování dat z paměti do externího media ve společnosti nebo v kalibračním režimu:

- datum a čas stahování dat,
- číslo podnikové nebo dílenské karty a členský stát vydávající kartu,
- název společnosti nebo dílny.

12.15 Údaje o specifických podmínkách

105a Záznamové zařízení musí zaznamenávat ve své paměti dat následující údaje týkající se specifických podmínek:

- datum a čas vkládání dat,
- druh specifických podmínek.

105b Paměť údajů musí být schopna uchovat specifické podmínky po dobu nejméně 365 dnů (za předpokladu, že průměrně jedny podmínky jsou otevřeny a uzavřeny během jednoho dne). Jestliže je kapacita paměti vyčerpána, nová data musí nahrazovat postupně nejstarší údaje.

13 Čtení z karet tachografu

106 Záznamové zařízení musí být schopno, pokud je třeba, přečíst z karet tachografu příslušné údaje, aby:

- identifikovalo typ karty, držitele karty, předcházející použité vozidlo, datum a čas posledního vyjmutí karty a v té době navolené činnosti,
- zkontrolovalo, že poslední použití karty bylo korektně ukončeno,
- spočítalo dobu řidičovy nepřetržité jízdy, kumulativní dobu přestávek a kumulativní dobu jízdy v předcházejícím a aktuálním týdnu,
- vytisklo požadovaná data zaznamenaná na kartě řidiče,
- stáhlo data z karty řidiče na externí media.

107 V případě chyby načítání dat, se musí záznamové zařízení maximálně třikrát pokusit o vyplnění stejného příkazu k přečtení dat a pak v případě neúspěchu vyznačí chybu karty a nebo její neplatnost.

14 Zaznamenávání a uchovávání dat na kartě tachografu

- 108 Záznamové zařízení musí v kartě řidiče nebo dílenské kartě nastavit režim „data o použití karty“ okamžitě po vložení karty.
- 109 Záznamové zařízení musí aktualizovat data uložená na platných kartách řidiče a/nebo dílenských a kontrolních kartách o všechna data vztahující se k době, kdy byla karta vložena a k osobě držitele karty. Údaje uložené na kartách jsou specifikované v kapitole IV.
- 109a Záznamové zařízení musí aktualizovat údaje o činnostech řidiče a místě (jak je specifikováno v kapitole IV, odstavec 5.2.5 a 5.2.6), které jsou uloženy na platných kartách řidiče a/nebo na dílenských kartách, o data týkající se činností řidiče a míst, která byla ručně vložena držitelem karty.
- 110 Data uložená na kartách musí být aktualizována takovým způsobem a v takovou dobu, kdy to bude třeba s ohledem na kapacitu paměti dat a nahrazení nejdříve uložených dat posledními údaji.
- 111 V případě chybného zápisu se záznamové zařízení maximálně třikrát pokusí vyplnit tento příkaz k zápisu a pokud zůstanou pokusy neúspěšné, vyznačí chybu karty a nebo její neplatnost.
- 112 Před uvolněním karty řidiče a po uložení všech příslušných dat, která se měla na kartu uložit, záznamové zařízení znovu nastaví údaje o použití karty.

15 Zobrazování

- 113 Display musí mít minimálně 20 znaků.
- 114 Minimální výška znaku musí být 5 mm a šířka 3.5 mm.
- 114a Zobrazovací jednotka musí podporovat fonty znaků Latin 1 a řecká písmena definovaná normou ISO 8859 část 1 a 7, jak je uvedeno v dodatku 1, kapitole 4 „Sady znaků“. Zobrazovací jednotka může používat zjednodušené znaky (např. znaky s diakritikou mohou být zobrazeny bez diakritiky a nebo malá písmena mohou být zobrazena jako velká).
- 115 Zobrazovací jednotka musí vydávat přiměřené, neoslňující světlo.
- 116 Údaje záznamového zařízení musí být dobře viditelné.
- 117 Záznamové zařízení musí být schopno zobrazit:
- defaultové údaje,
 - údaje vztahující se k výstražným sdělením,
 - data vztahující se k přístupovému menu,
- ostatní údaje požadované uživatelem.

Dodatečné informace mohou být zobrazeny záznamovým zařízením za předpokladu, že je jasně odlišitelné od výše uvedených informací.

- 118 Display záznamového zařízení musí používat piktogramy nebo kombinace piktogramů uvedených v dodatku 3. Dodatečné piktogramy nebo kombinace piktogramů mohou být zobrazeny displayem za předpokladu, že jsou jasně odlišitelné od dříve uvedených piktogramů nebo kombinací piktogramů.
- 119 Display musí být vždy zapnut, pokud je vozidlo v pohybu.
- 120 Záznamové zařízení může obsahovat ruční nebo automatickou možnost vypnutí displaye, pokud se vozidlo nepohybuje.

Formát zobrazení je specifikován v dodatku 5.

15.1 Defaultové zobrazení

- 121 Pokud není třeba zobrazit žádnou jinou informaci, musí záznamové zařízení zobrazit defaultově následující:

- místní čas (jako výsledek referenčního času UTC + posunutí času nastavené řidičem),
- provozní režim,
- aktuální činnost řidiče a aktuální činnost druhého řidiče,
- informace vztahující se k řidiči:
 - pokud je jeho současná činnost JÍZDA, jeho současný čas nepřetržité jízdy a jeho současný kumulativní čas přestávek,
 - pokud jeho současnou činností není JÍZDA, aktuální trvání současné činnosti (od doby, kdy byla navolena) a jeho současný kumulativní čas přestávek,
- informace vztahující se k druhému řidiči:
 - současné trvání jeho činnosti (od doby, kdy byla navolena).

- 122 Zobrazení dat vztahujících se ke každému řidiči musí být jasné, prosté a jednoznačné. V případě, že informace o řidiči i druhém řidiči nemohou být zobrazeny současně, musí záznamové zařízení defaultově ukazovat informaci týkající se řidiče a musí umožnit uživateli zobrazit informaci týkající se druhého řidiče.

- 123 V případě, že šířka zobrazovací jednotky nedovoluje zobrazit defaultově provozní režim, pak záznamové zařízení musí krátce zobrazit nový provozní režim v okamžiku, kdy se mění.

- 124 Záznamové zařízení musí při vložení karty krátce zobrazit jméno držitele karty.

- 124a Jestliže jsou otevřené podmínky „MIMO ROZSAH PLATNOSTI“, potom musí display ukázat odpovídající piktogram, že podmínky jsou otevřené (Je povoleno, aby současně nebyla zobrazena současná informace o činnosti řidiče).

15.2 Zobrazení výstražných sdělení

- 125 Záznamové zařízení musí zobrazit výstražné sdělení primárně použitím piktogramů podle dodatku 3, doplněné v případě potřeby dodatečnými numericky kódovanými informacemi. Přesné popisy výstražných sdělení mohou být také zobrazeny v řidičem preferované řeči.

15.3 Přístupové menu

- 126 Záznamové zařízení musí nabídnout nezbytné příkazy prostřednictvím příslušné struktury menu.

15.4 Ostatní zobrazované informace

- 127 Mělo by být možné zobrazit selektivně podle žádosti:
- referenční datum UTC a čas,
 - provozní režim (pokud není nabízen defaultově),
 - kontinuální čas jízdy a kumulativní čas přestávek řidiče,
 - kontinuální čas jízdy a kumulativní čas přestávek druhého řidiče,
 - kumulativní čas jízdy řidiče v předcházející a současném týdnu,
 - kumulativní čas jízdy druhého řidiče v předcházející a současném týdnu,
 - obsah kteréhokoliv ze šesti výtisků v témže formátu, jaký má poslední výtisk záznamů.
- 128 Zobrazování výtisku informací musí probíhat sekvenčně, řádka po řádce. Jestliže je šířka displaye menší nežli 24 znaků uživateli musí být nabídnuta úplná informace vhodným způsobem (několik řádek, rolování, ...). Linky výtisku věnované ručně psaným informacím mohou být vypuštěny ze zobrazení.
- ## **16. Tisk**
- 129 Záznamové zařízení musí být schopno vytisknout údaje z vlastní paměti dat a/nebo karet tachografu v souladu se šesti následujícími záznamy:
- činnosti řidiče podle denního výtisku karty,
 - činnosti řidiče podle denního výtisku celku ve vozidle,
 - události a závady ve výtisku karty,

- události a závady ve výtisku z celku ve vozidle,
- technické údaje,
- překročení povolené rychlosti.

Detailní popis formátu a obsahu těchto výtisků je specifikován v dodatku 4.

Dodatečné datové údaje mohou být přidány na konci výtisků.

Ze záznamového zařízení mohou být pořízeny i dodatečné výtisky, pokud jsou jasně odlišitelné od dříve popsaných šesti výtisků.

- 130 Záznam „činností řidiče z denního výtisku karty“ a „události a závady z výtisku karty“ musí být k dispozici pouze, pokud je v záznamovém zařízení vložena karta řidiče a nebo dílenská karta. Záznamové zařízení musí aktualizovat uložená data na příslušné kartě před započítáním tisku.
- 131 Aby zpřístupnilo záznam „činností řidiče z denního výtisku karty“ a „událostí a závad z výtisku karty“ musí záznamové zařízení:
- buď automaticky rozlišit, zda je vložena pouze jedna z karet řidiče a dílenské karty,
 - nebo nabídnout příkaz k volbě zdrojové karty a nebo zvolit kartu vloženou v otvoru pro vložení karty řidiče, pokud jsou dvě karty vloženy v záznamovém zařízení.
- 132 Tiskárna musí být schopna vytisknout 24 znaků na řádku.
- 133 Minimální velikost znaků musí být 2,1 mm vysoká a 1,5 mm široká.
- 133a Tiskárna musí podporovat fonty znaků Latin 1 a Greek, definované v normě ISO 8859, část 1 a 7, jak je popsáno v dodatku 1, kapitola 4 „Fonty znaků“.
- 134 Tiskárny musí být navrženy tak, aby se při tisku výtisků s dostatečnou pravděpodobností vyhnuly jakékoliv nejednoznačnosti při čtení.
- 135 Výtisky si musí podržet své rozměry a záznamy za normálních podmínek vlhkosti (10 až 90 %) a teploty.
- 136 Papír používaný v záznamové zařízení musí nést příslušnou značku schválení typu a označení typu(ů) záznamových zařízení, ve kterém se používá.
- 137 Na tyto dokumenty by mělo být možné udělat ručně psané poznámky, jako řidičův podpis.
- 138 Záznamové zařízení by mělo být v průběhu tisku schopno oznámit „došel papír“, pokud byl stejný papír opětovně vložen do záznamového zařízení, tisk bude restartován od úplného počátku výtisku a nebo bude tisk pokračovat s jednoznačným odkazem na dříve vytištěnou část.

17 Výstražná sdělení

- 139 Záznamové zařízení musí dát výstražné znamení řidiči při zjištění jakékoliv události a/nebo závady.
- 140 Výstražné sdělení při přerušení elektrického napájení mohou být odloženo až do opětovného připojení elektrického napájení.
- 141 Záznamové zařízení musí dát řidiči výstražné sdělení 15 minut před a při překročení 4 hod. a 30 min. nepřetržité jízdy.
- 142 Výstražné sdělení musí být vizuální. Zvuková výstraha může být také použita jako doplněk vizuální výstrahy.
- 143 Vizuální výstraha musí být jasně rozeznatelná uživatelem, musí být umístěna v zorném poli řidiče a musí být jasně čitelná ve dne i v noci.
- 144 Vizuální výstražné sdělení může být zabudováno v záznamovém zařízení a/nebo umístěno mimo záznamové zařízení.
- 145 Ve druhém případě musí nést symbol „T“ a mít žlutou nebo oranžovou barvu.
- 146 Výstražné sdělení musí trvat nejméně 30 vteřin, pokud není uživatelem potvrzeno vzetí na vědomí stiskem jakéhokoliv ovládacího prvku záznamového zařízení. První potvrzení zaregistrování nesmí zrušit výstražné sdělení v souladu s následujícím odstavcem.
- 147 Výstražné sdělení musí být zobrazeno na záznamovém zařízení a zůstat viditelné pokud nebude potvrzeno vzetí na vědomí použitím specifického ovladače a nebo vložení příkazu do záznamového zařízení.
- 148 Dodatečné výstražné sdělení může být také použito pokud nezmáte řidiče ve vztahu ke sdělení výše popsanému.

18. Stahování dat do externích médií

- 149 Záznamové zřízení musí být schopno v případě potřeby stáhnout údaje z paměti dat nebo z karty řidiče na externí medium, pro uložení dat prostřednictvím kalibračního/stahovacího konektoru. Záznamové zařízení před počátkem stahování dat aktualizuje údaje uložené na příslušné kartě.
- 150 Kromě toho jako přídatná funkce mohou být data stahována v jakémkoliv provozním režimu jiným konektorem pro společnost, která tímto kanálem prokáže svoji totožnost. V tomto případě se při stahování využijí přístupová práva společnosti pro stahování dat.
- 151 Stahování dat nesmí změnit nebo odstranit žádné uložené údaje.

Spojovací konektor pro kalibraci/stahování dat je popsán v dodatku 6.

Protokol o stahování dat je popsán v dodatku 7.

19. Výstupní data pro přídavná externí media

- 152 Jestliže záznamové zařízení neobsahuje display rychlosti a/nebo ujeté vzdálenosti, musí záznamové zařízení být zdrojem výstupního signálu(ů), které umožní zobrazení rychlosti (rychloměr) a/nebo vozidlem celkem ujeté vzdálenosti (měřič ujeté vzdálenosti).
- 153 Celek ve vozidle musí být také schopen dodat, prostřednictvím příslušné sériové linky nezávislé na přídavném CAN bus připojení (ISO 11898 Silniční vozidla – Výměna digitálních informací – Oblast sítě řídicích obvodů pro rychlou komunikaci), výstupní signál odpovídající následujícím údajům, což umožní jejich elektronické zpracování dalšími elektronickými jednotkami instalovanými ve vozidle:
- aktuální UTC datum a čas,
 - rychlost vozidla,
 - celková vozidlem ujetá vzdálenost (měřič ujeté vzdálenosti),
 - současně navolená činnost řidiče a druhého řidiče,
 - informace o jakékoliv kartě současně vložené do řidičova otvoru pro vkládání karty a otvoru druhého řidiče a (pokud přichází v úvahu) identifikační data karty (číslo karty a členský stát, který kartu vydal).

Další data mohou být k dispozici jako doplněk tohoto minimálního výčtu.

Jestliže je zapnuto „zapalování“ vozidla, uvedená data musí být neustále k dispozici na výstupní lince. Jestliže je „zapalování“ vypnuto musí být minimálně indikovány jakékoliv změny činnosti řidiče nebo druhého řidiče a/nebo jakékoliv vyjmutí nebo vložení karty tachografu musí vyvolat odpovídající výstupní datový signál. V případě, že výstupní datový signál není k dispozici při vypnutém „zapalování“ vozidla, musí se tyto údaje zpřístupnit okamžitě po zapnutí „zapalování“ vozidla.

20. Kalibrace

- 154 Kalibrační funkce musí umožnit:
- automatické párování snímače pohybu a celku ve vozidle,
 - digitálně přizpůsobí konstantu záznamového zařízení (k) charakteristickému součiniteli vozidla (w) (vozidla vybavená dvěma a více převodovými poměry koncového převodu musí být vybavena spínacím zařízením, kterým se automaticky příslušné převodové poměry uvedou do souladu s převodovým poměrem, se kterým bylo záznamové zařízení párováno).

- seřízení aktuálního času (bez omezení),
- nastavit současnou hodnotu měřiče ujeté vzdálenosti,
- aktualizovat identifikační data snímače pohybu uložené v paměti údajů,
- aktualizovat nebo potvrdit další parametry známé záznamovému zařízení: identifikace vozidla, w, l, rozměr pneumatik a nastavení omezovače rychlosti, pokud přichází v úvahu.

155 Párování snímače pohybu s celkem ve vozidle spočívá minimálně v:

- aktualizace instalačních dat snímače pohybu, ukládané do snímače pohybu (pokud je to možné),
- kopírování identifikačních dat snímače pohybu ze snímače do celku ve vozidle.

156 Kalibrační funkce musí být schopna vložit nezbytná data prostřednictvím kalibračního/stahovacího konektoru v souladu s kalibračním protokolem definovaným v dodatku 8. Kalibrační funkce musí být schopna vložit nezbytné údaje i prostřednictvím jiných konektorů.

21. Seřízení času

157 Funkce seřízení času musí umožnit nastavení aktuálního času maximálně o jednu minutu v intervalech nejméně sedmi dní.

158 Funkce seřízení času musí umožnit nastavení aktuálního času bez omezení v kalibračním režimu.

22. Funkční charakteristiky

159 Celek ve vozidle musí být plně funkční v rozsahu teplot od -20°C do 70°C a snímač pohybu v rozmezí od -40°C do 135°C. Paměť dat musí být chráněna při teplotách pod -40°C.

160 Záznamové zařízení musí být plně funkční v rozsahu vlhkosti 10% až 90%.

161 Záznamové zařízení musí být chráněno proti přepětí, přepólování elektrického napájení a zkratu.

162 Záznamové zařízení musí vyhovovat směrnici 95/54/EC z 31. října 1995¹³/přizpůsobující technickému pokroku směrnici Rady 72/245/EC¹⁴/ z hlediska elektromagnetické kompatibility a mělo by být chráněno proti výbojům a kolísání napájení.

¹³ Úř. věst. č. L 266, 8.11.1995, s. 1.

¹⁴ Úř. věst. č. L 152, 6.7.1972, s. 15.

23. Materiály

- 163 Všechny komponenty, ze kterých se záznamové zařízení skládá musí být vyrobeny z materiálů s dostatečnou stabilitou, mechanickou odolností a stabilními elektrickými i magnetickými charakteristikami.
- 164 Při normálním použití musí být všechny vnitřní části zařízení chráněny proti vlhkosti a prachu.
- 165 Celek ve vozidle musí vyhovovat stupni ochrany IP 40 a snímač pohybu stupeň ochrany IP 64 podle normy IEC 529.
- 166 Zařízení musí vyhovovat příslušným technickým specifikacím vztahujícím se k ergonomii konstrukce.
- 167 Zařízení musí být chráněno proti náhodnému poškození.

24. Značení

- 168 Pokud záznamové zařízení zobrazuje údaje měřiče vzdálenosti a rychloměru, musí se na zobrazovací jednotce objevit i následující podrobnosti:
- v blízkosti údaje ujeté vzdálenosti budou uvedeny jednotky vzdálenosti vyznačené zkratkou „km“,
 - v blízkosti údaje zobrazujícího rychlost bude značka „km/hod“.
- Záznamové zařízení může být také přepnuto, aby zobrazovalo rychlost v mílech za hodinu a v tomto případě bude jednotka měřené rychlosti vyznačena zkratkou „mph“.
- 169 Popisná plaketa bude připevněna na každý samostatný komponent záznamového zařízení a musí nést následující údaje:
- jméno a adresa výrobce zařízení,
 - katalogové číslo součásti podle výrobce a rok výroby zařízení,
 - výrobní číslo,
 - značka schválení typu záznamového zařízení.
- 170 Pokud není k dispozici dostatečný prostor pro zobrazení všech výše uvedených podrobností, popisná plakety musí obsahovat minimálně: jméno nebo logo výrobce a katalogové číslo komponentu.

IV. KONSTRUKČNÍ A FUNKČNÍ POŽADAVKY NA KARTY TACHOGRAFU

1. Visuální údaje

Přední strana bude obsahovat:

- 171 slova „Karta řidiče“ nebo „Kontrolní karta“ nebo „Dílenská karta“ nebo „Karta společnosti“ vytištěná velkými písmeny v oficiálním jazyce nebo jazyce členského státu vydávajícího kartu, podle typu karty:
- 172 stejná slova v jiném oficiálním jazyce Evropské Unie vytištěná na zadní straně:

ES	TARJETA DEL CONDUCTOR	TARJETA DEL CONTROL	TARJETA DEL CENTRO ENSAYO	TARJETA DE LA EMPRESA
DK	FORERKORT	KONTROLKORT	VAERKSTEDKOR T	VIRKSOMHEDSK ORT
DE	FAHRERKARTE	KONTROLLKART E	WERKSTATTKAR TE	UNTERNEHMENS KARTE
EL				
EN	DRIVER CARD	CONTROL CARD	WORKSHOP CARD	COMPANY CARD
FR	CARTE DE CONDUCTEUR	CARTE DE CONTROLEUR		
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	CONTROLEKAAR T	WERKPLAATSKA ART	BEDRIJFSKAART
PT	CARTAO DE CONDUTOR	CARTAO DE CONTROLO	CARTAO DO CENTRO DE ENSAIO	CARTAO DE EMPRESA
FI	KULJETTAJA KORTTILLA	VALVONTA KORTTILLA	TESTAUSASEMA KORTTILLA	YRITYSKORTTIL LA
SV	FÖRARKORT	KONTROLLKORT	VERKSTADSKOR T	FÖRETAGSKORT

- 173 jméno členského státu vydávajícího kartu (volitelné)

174 rozlišovací značky členských států vydávajících kartu, v negativním provedení oklopeném 12 žlutými hvězdami na modrém obdélníkovém podkladu. Rozlišovací značky mají následující význam:

B Belgie

DK Dánsko

D Německo

GR Řecko

E Španělsko

F Francie

IRL Irsko

I Itálie

L Lucembursko

NL Nizozemí

A Rakousko

P Portugalsko

FIN Finsko

S Švédsko

UK Spojené království

175 specifická data k vydaným kartám, číslovaná podle následujícího schématu:

	Karta řidiče	Kontrolní karta	Karta společnosti nebo dílenská karta
1.	Příjmení řidiče	Jméno Kontrolního orgánu	Karta společnosti nebo dílenská karta
2.	Křestní jméno řidiče	Příjmení kontrolora (pokud přichází v úvahu)	Příjmení držitele karty (pokud přichází v úvahu)
3.	Narození řidiče	Křestní jméno kontrolora (pokud přichází v úvahu)	Křestní jméno držitele karty (pokud přichází v úvahu)
4.(a)	Datum začátku platnosti karty		
(b)	Datum vypršení platnosti karty (pokud přichází v úvahu)		
(c)	Jméno kartu vydávajícího úřadu (může být vytištěno na druhé straně)		
(d)	Číslo odlišné od čísla uvedeného v řádku 5, pro administrativní účely (volitelné)		
5.(a)	Číslo řidičského průkazu (k datu vydání karty řidiče)		
5.(b)	Číslo karty		
6.	Fotografie řidiče	Fotografie kontrolora (možno uvést)	—
7.	Podpis řidiče	Podpis držitele (možno uvést)	
8.	Obvyklé místo pobytu nebo adresa držitele (volitelné)	Poštovní adresa kontrolního orgánu	Poštovní adresa společnosti nebo dílny













176 data musí být uváděna ve formátu „dd/mm/yyyy“ (den, měsíc, rok);

rubová strana bude obsahovat:

177 vysvětlení očíslovaných položek, které se objevily na přední straně karty;

178 na základě zvláštní psané dohody s držitelem mohou být uvedeny informace, které se nevztahují k registraci karty, ale tato změna nemění způsob použití daného modelu karty tachografu.

COMMUNITY MODEL TACHOGRAPH CARDS

FRONT		REVERSE	
 DRIVER CARD 1. 2. 3. 4a. 4c. 5a. 5b. 6. 7. (8.)	MEMBER STATE TARJETA DEL CONDUCTOR FÖRARKORT FAHRERKARTE KAPTA O - 3HT'OF 4b. DRIVER CARD CARTE DE CONDUCTEUR CARTA TROMANA CARTA DEL CONDUCENTE BESTUURDESKAART CARTÃO DE CONDUTOR KULJETTAJAKORTILLA FÖRARKORT	 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 Please return to: NAME OF AUTHORITY AND ADDRESS	
 CONTROL CARD 1. (2.) (3.) 4a. 4c. (4d.) 5b. (6.) 7. 8.	MEMBER STATE TARJETA DE CONTROL KONTROLKORT KONTROLLKARTE KAPTA EMEYOT (4b.) CONTROL CARD CARTE DE CONTROLEUR CARTA STIURTHA CARTA DI CONTROLLO CONTOLEKAART CARTÃO DE CONTROLO VALVONTAKORTILLA KONTROLLKORT	 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 Please return to: NAME OF AUTHORITY AND ADDRESS	
 WORKSHOP CARD 1. (2.) (3.) 4a. 4c. (4d.) 5b. (7.) 8.	MEMBER STATE TARJETA DEL CENTRO DE ENSAYO VÆRKSTEDSKORT WERKSTATTKARTE KAPTA EINTROY AOKIMIN 4b. WORKSHOP CARD CARTE D'ATELIER CARTA CEARDLAINNE CARTA DELL'OFFICINA WERKPLAATSKAART CARTÃO DO CENTRO DE ENSAIO TESTAUSASEMAKORTILLA VERKSTADSKORT	 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 Please return to: NAME OF AUTHORITY AND ADDRESS	
 COMPANY CARD 1. (2.) (3.) 4a. 4c. (4d.) 5b. (7.) 8.	MEMBER STATE TARJETA DE LA EMPRESA VIRKSOMHEDSKORT UNTERNEHMENSKARTE KAPTA EIDNEPES 4b. COMPANY CARD CARTE D'ENTREPRISE CARTA COMHACHTA CARTA DELL'AZIENDA BEDRIJFSKAART CARTÃO DE EMPRESA YRITYSKORTILLA FÖRETAGSKORT	 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 Please return to: NAME OF AUTHORITY AND ADDRESS	

MODELÝ KARET TACHOGRAFU VE SPOLEČENSTVÍ

(překlad textů na vzorech karet)

Driver Card	Karta řidiče
Member State	Členský stát
Surname / First name / Birth date	Příjmení / jméno / datum narození
Date of start of validity of card	Počáteční datum platnosti karty
Administrative expiry date of card	Administrativní doba vypršení platnosti karty
Issuing authority	Vydávající orgán
No. for national administrative purposes	Číslo pro národní registrační účely
Driving licence number	Číslo řidičského průkazu
Card number	Číslo karty
Photograph/Signature/Address	Fotografie/Podpis/Adresa
Please return to:	Prosím vrátit na adresu:
Name of Authority and Address	Jméno orgánu a adresa
Control Card	Kontrolní karta
Control Body	Kontrolní orgán

Workshop Card	Dílenská karta
Workshop Name	Název dílny
Company Card	Karta společnosti

179 Karty tachografu musí být vydávány s pozadím, na kterém převládají následující barvy:

- karta řidiče: bílá barva
- kontrolní karta: modrá barva
- dílenská karta: červená barva
- karta společnosti: žlutá barva.

180 Karty tachografu musí nést minimálně následující ochranné prvky, chránící karty proti padělání a poškozování:

- bezpečnostní provedení pozadí ve formě proplétané textury a duhový tisk,
- v oblasti fotografie, se musí překrývat bezpečnostní provedení pozadí a fotografie,
- nejméně jedna dvoubarevná mikrotisková linka.

181 Po konzultaci se Společenstvím mohou členské státy přidat barvy nebo označení, jako národní symboly a bezpečnostní prvky, aniž by došlo ke znehodnocení opatření tohoto dodatku.

2. Bezpečnostní opatření

Systémová bezpečnost se zaměřuje na ochranu autentičnosti dat přenášených mezi kartou a záznamovým zařízením, ochranu kompletnosti a autenticitu dat stahovaných z karet, umožňuje zapsání jistých dat na kartu pouze záznamovým zařízením a ochránění karty proti poškození resp. zjištění pokusu o podobné jednání.

182 Aby se dosáhlo systémové bezpečnosti musí karty tachografu splňovat bezpečnostní požadavky definované v popisu generických bezpečnostních cílů (Dodatek 10).

183 Karty tachografu musí být čitelné dalšími zařízeními jako osobními počítači.

3. Standardy

184 Karty tachografu musí vyhovovat následujícím standardům:

- ISO/IEC 7810 Identifikační karty – Fyzikální charakteristiky,

- ISO/IEC 7816 Identifikační karty – Integrované okruhy s kontakty:
 - Část 1: Fyzikální charakteristiky,
 - Část 2: Rozměry a umístění kontaktů,
 - Část 3: Elektronické signály a komunikační protokoly,
 - Část 4: Formáty pro výměnu informací mezi průmyslovými odvětvími,
 - Část 8: Bezpečnost komunikace mezi průmyslovými odvětvími,
- ISO/IEC 10373 Identifikační karty – Zkušební postupy.

4. Environmentální a elektrické specifikace

- 185 Karty tachografu musí být schopny správné funkce za všech klimatických podmínek nacházejících se na teritoriu Společenství a nejméně v rozsahu teplot od minus 25 °C do +70 °C s náhodnými špičkami do +85 °C. Náhodnými špičkami se myslí na dobu nepřesahující 4 hodiny v průběhu špičky a ne více nežli 100 x v průběhu životnosti karty.
- 186 Karty tachografu musí být schopny správné funkce při vlhkosti v rozsahu 10 % až 90 %.
- 187 Karty tachografu musí být schopny správné funkce po dobu pěti let, pokud jsou používány ve shodě s předepsaným prostředím a elektrickými specifikacemi.
- 188 V průběhu používání musí karty tachografu vyhovovat požadavkům směrnice Společenství 95/54/EC ze 31. října 1995 ¹⁵/, vztahující se k elektromagnetické slučitelnosti a musí být ochráněny proti elektrostatickým výbojům.

5. Ukládání dat

Pro účely tohoto článku,

- časové údaje jsou zaznamenávány s rozlišovací schopností jedné minuty pokud není stanoveno jinak,
- údaje měřiče ujeté vzdálenosti jsou zaznamenávány s rozlišovací schopností jednoho kilometru,
- rychlost je zaznamenávána s rozlišovací schopností 1 km/hod.

Funkce karty tachografu, pokyny a logická stavba ukládání dat do paměti jsou popsány v dodatku 2.

¹⁵ Úř. věst. č. L 266, 8.11.1995, s. 1

- 189 Tento odstavec stanovuje minimální kapacitu pro ukládání dat v různých aplikačních souborech. Karty tachografu musí být schopny informovat záznamové zařízení o současné kapacitě těchto souborů.

Jakékoliv dodatečné údaje, vztahující se k jiným účelům, eventuálně vygenerovaná kartou, mohou být ukládány na kartu tachografu v souladu se směrnicí 95/46/EC z 24. října 1995 o ochraně jednotlivce s ohledem na zpracování osobních dat a jejich volný pohyb¹⁶.

5.1 Identifikace karty a bezpečnostní údaje

5.1.1 Identifikace použití

- 190 Karty tachografu musí být schopny uchovávat následující identifikační data použití:

- identifikace tachografového použití,
- identifikace typu karet tachografu.

5.1.2 Identifikace čipu

- 191 Karty tachografu musí být schopny ukládat následující identifikační data integrovaného obvodu (IC):

- sériové číslo IC,
- výrobní reference IC.

5.1.3 Identifikace čipové karty

- 192 Karty tachografu musí být schopny uchovat následující identifikační údaje čipové karty:

- sériové číslo karty (včetně výrobních referencí),
- číslo schválení typu karty,
- identifikátor karty tachografu (ID),
- embedder ID,
- IC identifikátor.

5.1.4 Bezpečnostní prvky

- 193 Karty tachografu musí být schopny uchovat údaje o následujících bezpečnostních prvcích:

¹⁶ Úř. věst. č. L 281, 23.11.1995, s. 31

- evropský veřejný klíč,
- certifikát členského státu,
- certifikát karty,
- soukromý klíč karty.

5.2 Karta řidiče

5.2.1 Identifikace karty

194 Karta tachografu musí být schopna uchovat následující identifikační data karty:

- číslo karty,
- kartu vydávající členský stát, vydávající orgán, datum vydání.

5.2.2 Identifikace držitele karty

195 Karta řidiče musí být schopna uchovat následující identifikační data karty řidiče:

- příjmení držitele karty,
- jméno(a) držitele karty,
- datum narození,
- přednostní komunikační jazyk.

5.2.3 Informace o řidičském průkazu

196 Karta řidiče musí být schopna uchovat následující údaje o řidičském průkazu:

- kartu vydávající členský stát, název vydávajícího orgánu,
- číslo řidičského průkazu (u data vydání karty).

5.2.4 Údaje o použití vozidel

197 Karta řidiče musí být schopna uchovat pro každý den, kde byla použita a pro každý časový úsek, kdy byla užitá v daném vozidle (časový úsek obsahuje všechny po sobě jdoucí cykly mezi vložení a vyjmutím karty v tomto vozidle z pohledu této karty) následující údaje:

- datum a čas prvního použití vozidla (tzn. první ložení karty v tomto časovém úseku použití vozidla, nebo 00.00 jestliže použití vozidla pokračuje v této době),
- údaj měřiče ujeté vzdálenosti v této době,

- registrační číslo vozidla a členský stát, ve kterém je vozidlo registrováno.

198 Karta řidiče musí být schopna uchovat nejméně 84 takových záznamů.

5.2.5 Údaje o řidičových činnostech

199 Karta řidiče musí být schopna uchovat pro každý kalendářní den, kde byla karta použita nebo pro každou činnost, kterou řidič vložil ručně, následující údaje:

- datum,
- stav počítadla dní od instalace jednotky do vozidla (vzroste o jednotku každý kalendářní den),
- celkovou vzdálenost ujetá řidičem v průběhu dne,
- statut řidiče v 00.00,
- kdykoliv se změní činnost řidiče a/nebo se změnil jeho statut a/nebo byla vložena nebo vyjmuta jeho karta:
 - statut posádky (POSÁDKA, SAMOTNÝ ŘIDIČ),
 - otvor pro vložení karty (ŘIDIČ, DRUHÝ ŘIDIČ),
 - statut karty (VLOŽENA, VYJMUTA),
 - činnost (JÍZDA, POHOTOVOST, PRÁCE, PŘESTÁVKA/ODPOČINEK),
 - čas změny.

200 Paměť karty řidiče musí být schopna uchovat údaje o činnosti řidiče nejméně po 28 dní (průměrná činnost řidiče je definována jako 93 změn činnosti za den).

201 Údaje uvedené v požadavcích 197 a 199 musí uchovány způsobem umožňujícím vyhledání v chronologickém pořadí, dokonce i v případě překrývajících se údajů.

5.2.6 Místa, kde časy výkonu denní práce začínají a/nebo končí

202 Karta řidiče musí být schopna uchovat následující údaje vložené řidičem a vztahující se k místům, kde úseky denní práce začínají a/nebo končí:

- datum a čas vložení údajů (a/nebo datum/čas vztahující se ke vložení údajů, pokud jsou zadávány řidičem ručně),
- typ vložených údajů (začátek nebo konec, podmínky vložení údajů),
- stát nebo oblast, kde byly údaje vloženy

- hodnota měřiče ujeté vzdálenosti.

203 Paměť karty řidiče musí být schopna uchovat nejméně 42 párů takových údajů.

5.2.7 Údaje o událostech

Pro účely tohoto pododstavce musí být čas ukládán s rozlišovací schopností jedné vteřiny.

204 Karta řidiče musí být schopna uchovat údaje vztahující se k následujícím událostem registrovaným záznamovým zařízením v okamžiku vložení karty:

- časové překrytí (když je karta důvodem této události),
- vložení karty v průběhu jízdy,
- poslední použití karty, které nebylo správně ukončeno (když je karta důvodem této události),
- přerušení elektrického napájení,
- chyba údajů o pohybu vozidla,
- pokus o porušení bezpečnostních opatření.

205 Karta řidiče musí být schopna uchovat následující údaje o těchto událostech:

- kód události,
- datum a čas počátku události (nebo vložení karty, pokud událost v této době pokračuje),
- datum a čas ukončení události (nebo čas vyjmutí karty, pokud událost v této době pokračuje),
- registrační číslo vozidla a členský stát, ve kterém bylo vozidlo registrováno.

Poznámka: V případě časového překrytí událostí:

- datum a čas počátku události by měl odpovídat datu a času vyjmutí karty z předcházejícího vozidla,
- datum a čas ukončení události by měl odpovídat datu a času vložení karty v současně používaném vozidle,
- údaje o vozidle by měly odpovídat současně používanému vozidlu v průběhu události.

Poznámka: V případě „posledního nesprávně ukončeného použití“:

- datum a čas počátku události by měl odpovídat datu a času vložení karty v případě jejího nesprávně ukončeného použití,
- datum a čas události by měl odpovídat datu a času vložení karty v průběhu identifikované události (současné použití karty),
- údaje o vozidlu by měly odpovídat vozidlu, ve kterém nebylo použití karty správně ukončeno.

206 Karta řidiče musí být schopna uchovat data vztahující se k posledním šesti událostem každého typu (tzn. 36 událostí).

5.2.8 Údaje o závadách

Pro účely tohoto pododstavce musí být čas zaznamenáván s rozlišovací schopností jedné vteřiny.

207 Karta řidiče musí být schopna uchovat data vztahující se k následujícím chybám zjištěným záznamovým zařízením při vložení karty:

- chyba karty (v případě, že karty je dotčena událostí),
- chyba záznamového zařízení.

208 Karta řidiče musí být schopna uchovat následující údaje vztahující se k těmto chybám:

- chybný kód,
- datum a čas počátku chyby (nebo vložení karty pokud chyba v té době již pokračuje),
- datum a čas ukončení chyby (nebo vyjmutí karty, jestliže chyb v té době pokračuje),
- registrační číslo vozidla a členský stát registrující vozidlo, ve kterém chyba nastala.

209 Karta řidiče musí být schopna uchovat údaje vztahující se k posledním dvanácti chybám každého typu (tzn. 24 chyb).

5.2.9 Údaje o kontrolních činnostech

210 Karta řidiče musí být schopna uchovat údaje vztahující se ke kontrolním činnostem:

- datum a čas provedení kontroly,
- číslo kontrolní karty a členský stát vydávající kartu,
- typ kontrolní činnosti (zobrazení a/nebo vtištění a/nebo stahování do celku ve vozidle a/nebo stahování dat na kartu (viz poznámka)),

- dobu stahování dat, pokud k němu došlo,
- REGISTRAČNÍ ČÍSLO VOZIDLA a členský stát registrující vozidlo, u kterého kontrolní činnost proběhla.

Poznámka: Bezpečnostní požadavky implicitně předpokládají, že stahování na kartu se zaznamená, jestliže stahování proběhne přes záznamové zařízení.

211 Karta řidiče musí být schopna uchovat jeden takový záznam.

5.2.10 Údaje o použití karty

212 Karta řidiče musí být schopna uchovat údaje vztahující se k vozidlu, které otevřelo současné použití karty:

- datum a čas otevření použití karty (tzn. vložení karty) s rozlišovací schopností jedné vteřiny;
- REGISTRAČNÍ ČÍSLO VOZIDLA a registrující členský stát.

212a Karta řidiče musí být schopna uchovat údaje vztahující se ke zvláštním podmínkám, které jsou vloženy v průběhu doby, kdy je karta vložena (v jakémkoliv otvoru pro vkládání karet):

- datum a čas uložení dat,
- druh zvláštních podmínek.

212b Karta řidiče musí být schopna uchovat 56 takových údajů.

5.3 Dílenská karta

5.3.1 Bezpečnostní prvky

213 Dílenská karta musí být schopna uložit osobní identifikační číslo (PIN kód)-

214 Dílenská karta musí být schopna uložit kryptografické klíče pro párování snímačů pohybu s celky ve vozidle.

5.3.2 Identifikace karty

215 Dílenská karta musí být schopna uložit následující identifikační data karty:

- číslo karty,
- vydávající členský stát, název vydávajícího orgánu, datum vydání,
- datum počátku platnosti karty, datum vypršení platnosti.

5.3.3 Identifikace držitele karty

216 Dílenská karta musí být schopna uložit následující identifikační data držitele karty:

- název dílny,
- adresa dílny,
- příjmení držitele,
- křestní jméno držitele,
- jazyk, kterému držitel dává přednost.

5.3.4 Údaje o použitém vozidle

- 217 Dílenská karta musí být schopna uložit záznamy o použitém vozidle stejným způsobem jako karta řidiče.
- 218 Dílenská karta musí být schopna uložit minimálně 4 takové záznamy.

5.3.5 Údaje o řídicích činnostech

- 219 Dílenská karta musí být schopna uložit údaje o řídicích činnostech stejným způsobem, jako karta řidiče.
- 220 Dílenská karta musí být schopna uchovat data minimálně o jednom průměrném dni řídicích činností.

5.3.6 Začátek a/nebo ukončení doby denní činnosti řidiče

- 221 Dílenská karta musí být schopna uložit záznamy dat o začátcích a ukončeních denní práce stejným způsobem jako karta řidiče.
- 222 Dílenská karta musí být schopna uchovat minimálně tři páry takových záznamů.

5.3.7 Údaje o událostech a závadách

- 223 Dílenská karta musí být schopna uložit údaje o událostech a závadách stejným způsobem jako karta řidiče.
- 224 Dílenská karta musí být schopna uložit údaje o třech posledních událostech takového typu (tzn. 18 událostí) a šest posledních záznamů o závadách takového typu (tzn. 12 závad).

5.3.8 Údaje o kontrolních činnostech

- 225 Dílenská karta musí být schopna uložit údaje o kontrolních činnostech stejným způsobem jako karta řidiče.

5.3.9 Údaje o kalibraci a nastavování času

- 226 Dílenská karta musí být schopna uchovat záznamy o kalibracích a/nebo nastavování času v době, kdy je karta vložena v záznamovém zařízení.
- 227 Každý kalibrační záznam musí být schopen uchovat následující údaje:

- důvod kalibrace (první instalace, instalace, periodická prohlídka),
- identifikace vozidla,
- aktualizovaná nebo potvrzená data (w, k, l, rozměr pneumatik, nastavení zařízení omezujícího rychlost vozidla, údaje měřiče ujeté vzdálenosti (nová a stará hodnota), datum a čas (nový a starý údaj),
- identifikace záznamového zařízení (katalogové číslo celku ve vozidle, výrobní číslo celku ve vozidle, výrobní číslo snímače rychlosti).

228 Dílenská karta musí být schopna uložit minimálně 88 takových záznamů.

229 Dílenská karta musí být schopna uchovat data odpovídající celkovému počtu s kartou provedených kalibrací.

230 Dílenská karta musí být schopna uchovat data o počtu provedených kalibrací od posledního stahování dat.

5.3.10 Údaje o specifických podmínkách

230a Dílenská karta musí být schopna uložit data týkající se specifických podmínek stejným způsobem jako karta řidiče. Dílenská karta musí být schopna uložit dva takové záznamy.

5.4 Kontrolní karta

5.4.1 Identifikace karty

231 Kontrolní karta musí být schopna uložit následující identifikační data:

- číslo karty,
- vydávající členský stát, název vydávajícího orgánu, datum vydání,
- datum počátku platnosti karty, datum vypršení platnosti karty (pokud přichází v úvahu).

5.4.2 Identifikace držitele karty

232 Kontrolní karta musí být schopna uložit následující identifikační data držitele karty:

- název kontrolního orgánu,
- adresa kontrolního orgánu,
- příjmení držitele karty,
- křestní jméno držitele karty,
- jazyk, kterému držitel dává přednost.

5.4.3 Údaje o kontrolních činnostech

233 Kontrolní karta musí být schopna uložit následující data o kontrolní činnosti:

- doba stahování dat (pokud přichází v úvahu),
- REGISTRAČNÍ ČÍSLO VOZIDLA a registrační orgán členského státu, kde bylo vozidlo registrováno,
- číslo karty a členský stát vydávající kontrolovanou karty řidiče.

234 Kontrolní karta musí být schopna uchovat minimálně 230 takových záznamů.

5.5 Karta společnosti

5.5.1 Identifikace karty

235 Karta společnosti musí být schopna uložit následující identifikační data:

- číslo karty,
- vydávající členský stát, název vydávajícího orgánu, datum vydání,
- datum počátku platnosti karty, datum vypršení platnosti (pokud je vyznačeno).

5.5.2 Identifikace držitele karty

236 Karta společnosti musí být schopna uložit následující identifikační data držitele karty:

- název společnosti,
- adresa společnosti.

5.3.3 Údaje o činnosti společnosti

237 Karta společnosti musí být schopna uložit následující údaje o činnostech společnosti:

- datum a čas činnosti,
- typ činnosti (uzamčení celku ve vozidle a/nebo odemknutí, a/nebo stahování dat záznamového zařízení a/nebo stahování dat karty),
- doba stahování dat (pokud proběhlo),
- REGISTRAČNÍ ČÍSLO VOZIDLA a členský stát registračního orgánu vozidla,
- číslo karty a kartu vydávající členský stát (v případě stahování dat karty).

238 Karta společnosti musí být schopna uložit nejméně 230 takových záznamů.

V. INSTALACE ZÁZNAMOVÉHO ZAŘÍZENÍ

1. Instalace

- 239 Nové zařízení musí být dodáno oprávněné servisní dílně nebo výrobcí vozidla neaktivované, se všemi kalibračními parametry, jak je uvedeno v kapitole III(20), a s nastavenými příslušnými platnými defaultovými hodnotami. V případě, že žádná specifická hodnota není považována za „příslušnou“, měla by být vložena následující sekvence znaků “?” a numerické parametry musí být nastaveny na “0”.
- 240 Před aktivací záznamového zařízení, musí zařízení umožnit přístup ke kalibrační funkci dokonce i když není v kalibračním režimu.
- 241 Před jeho aktivací nesmí záznamové zařízení zaznamenávat nebo ukládat údaje vztahující se k bodům III.1.2.3 až III.12.9 a III.12.12 až III.12.14 včetně.
- 242 V průběhu instalace musí výrobce před-nastavit všechny známé parametry.
- 243 Výrobce vozidla nebo oprávněná servisní dílna musí aktivovat instalované záznamové zařízení před tím, než vozidlo opustí prostory, kde instalace probíhá.
- 244 Aktivace záznamového zařízení se musí spustit automaticky prvním vložením dílenské karty do kteréhokoliv rozhraní.
- 245 Specifické úkony párování potřebné mezi snímačem pohybu a celkem ve vozidle, pokud je instalován, musí proběhnout automaticky před a nebo v průběhu aktivace.
- 246 Po aktivaci záznamového zařízení musí být plně aktivní funkce zařízení a přístupová práva.
- 247 Záznamové a ukládací funkce záznamového zařízení musí být po aktivaci plně funkční.
- 248 Po instalaci musí následovat kalibrace. První kalibrace musí zahrnovat vložení registračního čísla vozidla a proběhne v průběhu 2 týdnů od této instalace nebo přidělení registračního čísla vozidla, podle toho co nastane později.
- 248a Záznamové zařízení se musí ve vozidle umístit takovým způsobem, aby umožňovalo řidiči vykonávat všechny funkce z jeho sedadla.

2. Instalační plaketa

- 249 Po provedení prohlídky záznamového zařízení, která následuje po instalaci se umístí na, do a nebo vedle záznamového zařízení instalační plaketa tak, aby

byla dobře viditelná a snadno přístupná. Po každé prohlídce, provedené oprávněným montérem nebo servisní dílnou nebo dílnou musí být původní plaketa nahrazena novou.

Plaketa musí obsahovat minimálně následující údaje:

- jméno, adresu a obchodní název oprávněného montéra nebo servisní dílny,
- charakteristický součinitel vozidla ve formě „ $w = \dots$ impulsů/km“,
- konstantu záznamového zařízení ve formě „ $k = \dots$ impulsů/km“,
- skutečný obvod pneumatiky ve formě „ $l = \dots$ mm“,
- rozměr pneumatiky,
- datum, kdy byl stanoven charakteristický součinitel vozidla a kdy byl měřen skutečný obvod pneumatiky,
- identifikační číslo vozidla.

3 Zapečetění

251 Následující díly musí být zapečetěny:

- jakékoliv spojení, jehož rozpojení by umožnilo provedení neidentifikovatelných změn nebo neidentifikovatelnou ztrátu dat,
- instalační plaketa musí být umístěna tak, aby nemohla být sejmuta bez zničení jejího popisu.

252 Výše uvedené pečete mohou být sejmuty:

- v nouzových situacích,
- při instalaci, seřizování nebo opravě omezovače rychlosti vozidla nebo jiného zařízení přispívajícího k bezpečnosti silničního provozu za předpokladu, že záznamové zařízení bude nadále spolehlivě a správně fungovat a bude opětovně zapečetěno oprávněným montérem nebo servisní dílnou (v souladu s kapitolou VI) okamžitě po zpětném namontování omezovače rychlosti nebo jiného zařízení přispívajícího k bezpečnosti silničního provozu a nebo v průběhu sedmi dnů v ostatních případech.

253 V každém případě, kdy jsou zlomeny tyto pečete musí být vyhotoven písemný zápis se zdůvodněním celé události a musí být dán na vědomí příslušnému orgánu.

VI. KONTROLY, INSPEKCE A OPRAVY

Požadavky týkající se okolností, za kterých mohou být odstraněny pečeteř uváděné v článku 12.5 nařízení (EEC) č. 3821/85 posledně měněného nařízením (EC) č. 2135/98, jsou definované v kapitole V(3) tohoto dodatku.

1. Schvalování oprávněných montérů nebo servisních dílen

Členské státy schvalují, pravidelně kontrolují a certifikují oprávněné montéry nebo servisní dílny k provádění:

- instalací,
- kontrol,
- inspekci,
- oprav.

V rámci článku 12(1) tohoto nařízení se vydávají karty pouze servisům a/nebo dílnám oprávněným k aktivaci a/nebo kalibraci záznamových zařízení v souladu s tímto dodatkem a pokud nejsou úředně:

- oprávněny k použití karty společnosti,
- a jejichž další profesní činnosti nepředstavují potenciální střet zájmů z hlediska celkové bezpečnosti systému definovaného dodatkem 10.

2. Kontrola nových nebo opravených zařízení

254 Každé jednotlivé zařízení, ať již nové nebo opravené, musí být kontrolováno s ohledem na jeho správnou funkci a přesnost odečtů a záznamů, která musí odpovídat limitům stanoveným v kapitole III.2.1 a III.2.2, vybaveno pečetiřmi v souladu s kapitolou V.3 a kalibrováno.

3 Instalační prohlídky

255 Po zamontování záznamového zařízení do vozidla musí celá instalace (včetně záznamového zařízení) vyhovovat opatřením vztahujícím se k přípustným tolerancím uvedeným v kapitole III.2.1 a III.2.2.

4 Periodické kontroly

256 Periodická kontrola zařízení instalovaného do vozidla musí proběhnout po každé opravě záznamového zařízení, po jakékoliv změně charakteristického součinitele vozidla, skutečného obvodu pneumatiky, odchylce referenčního času UTC o více nežli 20 minut, při změně registračního čísla vozidla ale minimálně jednou v průběhu dvou let (24 měsíců) od poslední kontroly.

- 257 Tyto kontroly musí obsahovat následující kontrolní kroky zajišťující, že:
- je zajištěna správná funkce záznamového zařízení včetně ukládání dat v kartě tachografu,
 - je zajištěn soulad s opatřeními kapitol III.2.1 a III.2.2., které se týkají povolených tolerancí při instalaci,
 - záznamové zařízení nese značku schválení typu,
 - existuje instalační plaketa,
 - pečete na záznamovém zařízení a dalších instalovaných částech jsou nedotčené,
 - odpovídají rozměr a obvod pneumatiky.
- 258 Tyto kontroly musí obsahovat kalibraci

5 Chyby měření

- 259 Měření chyb při instalaci a v průběhu provozu musí být provedeno za následujících podmínek, které jsou považovány za nedílnou část zkušebních podmínek:
- nenaložené vozidlo v normálním provozním stavu,
 - tlak v pneumatikách souhlasí s pokyny výrobce,
 - opotřebení pneumatiky je v toleranci povolené národní legislativou,
 - pohyb vozidla:
 - vozidlo se pohybu vlastní silou po přímé a vodorovné trati rychlostí 50 ± 5 km/hod. Měřená vzdálenost je minimálně 1000 m,
 - za předpokladu, že bude zajištěna rovnocenná přesnost, může být pro provedení zkoušky použito alternativních metod, jako je vhodný válcový dynamometr.

6 Opravy

- 260 Dílny musí být schopny stahovat data ze záznamového zařízení, aby údaje mohly být předloženy zpět příslušné dopravní společnosti.
- 261 Oprávnění montéři a servisní dílny musí dopravní společnosti vydat certifikát o nestáhnutelnosti dat, pokud špatná funkce záznamového zařízení brání stažení dříve zaznamenaných dat i v případě, že oprava byla prováděna v téže dílně. Servisy a dílny musí archivovat kopie vydaných certifikátů nejméně po dobu jednoho roku.

VII VYDÁVÁNÍ KARET

Postupy vydávání karet stanovené jednotlivými členskými státy musí vyhovovat následujícím podmínkám:

- 262 Číslo karty při prvním vydání karty tachografu žadateli musí obsahovat pořadový index (pokud je to vhodné), výměnný index a index obnovení, které jsou nastaveny na hodnotu „0“.
- 263 Čísla karet všech karet tachografu vydaných organizací nebo společností („ne-osobní karty“), které se vydávají jednotlivým kontrolním orgánům, jednotlivým dílnám a dopravním společnostem mají shodných prvních 13 číslic, ale mají odlišné pořadové indexy.
- 264 Karta tachografu, která se vydává jako náhrada již existující karty musí mít stejné číslo karty jako nahrazovaný exemplář s výjimkou indexu výměny, který se zvedne o „jednotku“ (v pořadí 0, ..., 9, A, ..., Z).
- Karta tachografu, která se vydává jako náhrada již existující karty musí mít shodné datum vypršení platnosti jako nahrazovaný exemplář.
- Karta tachografu vydávaná při obnovení již existující karty musí mít stejné číslo karty jako obnovovaný exemplář s výjimkou indexu výměny, který bude nastaven na hodnotu „0“ a indexu obnovení, který bude zvýšen o „1“ (v pořadí 0, ..., 9, A, ..., Z).
- 267 Výměna existující karty tachografu při úpravách administrativních údajů, musí proběhnout podle pravidel platných pro obnovu karty, pokud proces probíhá uvnitř stejného členského státu a nebo podle pravidel platných ve státě, který vydal první kartu.
- 268 „Příjmení držitele karty“ u karet vydaných organizací nebo společností (ne-osobní karta) a nebo kontrolních karet bude vyplněno názvem dílny nebo kontrolního orgánu.

VIII SCHVÁLENÍ TYPU ZÁZNAMOVÉHO ZAŘÍZENÍ A KARET TACHOGRAFU

1 Obecná ustanovení

Pro účely této kapitoly výraz „záznamové zařízení“ znamená „záznamové zařízení nebo jeho komponenty“. Schválení typu není vyžadováno pro kabel(y) spojující snímač pohybu s celkem ve vozidle.

269 Záznamové zařízení by mělo být předloženo ke schválení typu úplné se všemi integrovanými přídatnými zařízeními.

270 Schvalovací postup záznamového zařízení a karet tachografu musí obsahovat zkoušky bezpečnostních opatření, funkční zkoušky a zkoušky interoperability. Positivní výsledky těchto zkoušek se potvrdí příslušnými osvědčeními.

271 Schvalovací orgány členských států nevydají osvědčení o schválení typu v souladu s článkem 5 tohoto nařízení, pokud neobdrží:

- osvědčení o bezpečnosti zařízení,
- osvědčení o funkčnosti,
- a osvědčení interoperability.

pro záznamové zařízení nebo kartu, která je předmětem žádosti o schválení typu.

272 Jakákoliv úprava týkající se software nebo hardware zařízení a nebo povahy materiálu použitého pro jeho výrobu, musí být před zavedením notifikována orgánem vydávajícím schválení typu zařízení. Tento orgán potvrdí výrobci rozšíření schválení typu a nebo může požadovat aktualizaci nebo potvrzení funkčních, bezpečnostních a/nebo interoperabilitních osvědčení.

273 Postup pro schválení upgrade instalovaného software musí být schválen orgánem, který vydal schválení typu pro záznamové zařízení.

2 Osvědčení o bezpečnosti

274 Osvědčení o bezpečnosti se provede v souladu s podmínkami dodatku 10 této přílohy.

3 Osvědčení o funkčnosti

275 Každý žadatel o vydání schválení typu dodá schvalovacímu orgánu členského státu všechny materiály a dokumentaci, kterou orgán považuje za nezbytnou.

276 Osvědčení o funkčnosti musí být výrobci vydáno teprve po úspěšném absolvování funkčních zkoušek minimálně v rozsahu specifikovaném v dodatku 9.

277 Schvalovací orgán vydá osvědčení o funkčnosti. Toto osvědčení musí obsahovat, kromě jména příjemce osvědčení a identifikace modelu, podrobný seznam provedených zkoušek a získaných výsledků.

4 Osvědčení interoperability

278 Zkoušky interoperability se provádějí v jediné zkušebně schválené a podléhající Evropské Komisi.

279 Laboratoř zaznamenává požadavky výrobců o zkoušky interoperability v chronologickém pořadí, jak byly doručeny.

280 Požadavky budou oficiálně registrovány pouze tehdy, jestliže zkušebně již byly dodány:

- úplná sada materiálů a dokumentů nezbytných pro takové zkoušky interoperability,
- příslušné osvědčení o bezpečnosti,
- příslušné osvědčení o funkčnosti.

Datum registrace žádosti musí být notifikován výrobcem.

281 Žádné zkoušky interoperability nebude zkušebna provádět u záznamového zařízení nebo karty tachografu, ke kterým nebyla poskytnuta osvědčení o bezpečnosti a funkčnosti.

282 Každý výrobce požadující zkoušky interoperability se zaváže ponechat laboratoři, která je odpovědná za provedení zkoušek, úplnou sadu materiálů a dokumentace, které byly ke zkouškám dodány.

283 Zkoušky interoperability musí být provedeny v souladu s ustanoveními paragrafu 5 dodatku 9 této přílohy, vztahující se na všechny typy záznamových zařízení a karet tachografu:

- jejichž schválení typu je dosud platné nebo
- jejichž schválení typu bylo pozastaveno, ale mají platné osvědčení interoperability.

284 Osvědčení interoperability musí být laboratoři doručeno výrobci teprve tehdy, až budou úspěšně absolvovány všechny požadované zkoušky interoperability.

285 Jestliže zkoušky interoperability nebudou úspěšné s jedním nebo několika záznamovými zařízeními nebo tachografovými kartami, podle požadavku

283, osvědčení interoperability nebude vydáno, pokud výrobce žádající o schválení neprovede nezbytné úpravy a neabsolvuje úspěšně interoperabilitní zkoušky. Zkušebna musí identifikovat důvod problému s pomocí příslušného výrobce a musí se pokusit mu pomoci nalézt technické řešení. V případě, že výrobce již upravil svůj výrobek, je jeho odpovědností zajistit od příslušných orgánů potvrzení platnosti svého osvědčení o bezpečnosti a funkčnosti.

- 286 Osvědčení interoperability je platné šest měsíců a postup bude muset být opakován na konci tohoto období, pokud výrobce neobdržel odpovídající schválení typu. Osvědčení je doručeno výrobcem schvalovacímu orgánu členského státu, který vydal osvědčení o funkčnosti.
- 287 Jakýkoliv prvek, který by mohl způsobit závadu interoperability nesmí být použit pro vytvoření zisku a nesmí vést k získání dominantního postavení.

5 Osvědčení o schválení typu

- 288 Schvalovací orgán členského státu může vydat osvědčení o schválení typu, jakmile obdrží tři požadovaná osvědčení.
- 289 Schvalovací orgán okopíruje osvědčení o schválení typu a zašle kopii pověřené zkušebně v době vydání osvědčení výrobcí.
- 290 Oprávněná zkušebna interoperability musí udržovat internetové stránky, na kterých bude aktualizovaný seznam modelů záznamových zařízení a karet tachografu:
- pro které byla zaregistrována žádost o zkoušky interoperability,
 - které obdržely osvědčení interoperability (i dočasné),
 - které získaly schválení typu.

6 Výjimečný postup: první osvědčení interoperability

- 291 V průběhu čtyř měsíců po certifikaci prvního páru záznamového zařízení a karet tachografu (řidiče, dílenské, kontrolní a společností) z hlediska interoperability, jakýkoliv vydaný interoperabilitní certifikát (včetně úplně prvního), týkající se žádostí registrovaných v tomto období, bude považován za dočasný.
- 292 Jestliže na konci tohoto období budou všechny uvažované výrobky vzájemně interoperabilní, stanou se všechna příslušná osvědčení definitivními.
- 293 Jestliže budou v tomto období zjištěny závady z hlediska interoperability, zkušebna odpovědná za zkoušky interoperability musí identifikovat za pomoci všech zainteresovaných výrobců zdroje problému a vyzve výrobce k provedení nezbytných úprav.

- 294 Jestliže na konci tohoto období budou problémy interoperability přetrvávat, pak odpovědná zkušebna ve spolupráci se zainteresovanými výrobci a schvalovacími orgány, které vydaly odpovídající funkční osvědčení musí zjistit důvody problému a stanovit nezbytné úpravy, které musí být provedeny zainteresovanými výrobci. Hledání technického řešení smí trvat maximálně dva měsíce, po kterých v případě nenalezení odpovídajícího řešení rozhodne Komise, po konzultaci se zkušebnou interoperability, které(á) zařízení obdrží definitivní certifikát interoperability a zdůvodní proč.
- 295 Jakákoliv žádost o zkoušky interoperability, registrovaná mezi koncem čtyřměsíčního období, kdy byly vydány dočasné certifikáty a datem rozhodnutí Komise podle požadavku 294, musí být odložena pokud nebudou počáteční problémy s interoperabilitou vyřešeny.. Tyto žádosti budou potom vyřízeny v chronologickém pořádku podle jejich registrace.
-

*DODATEK I***SLOVNÍK DAT****OBSAH**

1.1.	Podklad pro definice typů dat	76
1.2.	Odkazy	76
2.	DEFINICE TYPU DAT	77
2.1.	ActivityChangeInfo	77
2.2.	Address	79
2.3.	BCDString	79
2.4.	CalibrationPurpose	79
2.5.	CardActivityDailyRecord	80
2.6.	CardActivityLengthRange	80
2.7.	CardApprovalNumber	81
2.8.	CardCertificate	81
2.9.	CardChipIdentification	81
2.10.	CardConsecutiveIndex	81
2.11.	CardControlActivityDataRecord	81
2.12.	CardCurrentUse	82
2.13.	CardDriverActivity	82
2.14.	CardDrivingLicenceInformation	83
2.15.	CardEventData	84
2.16.	CardEventRecord	84
2.17.	CardFaultData	84
2.18.	CardFaultRecord	85
2.19.	CardIccIdentification	85
2.20.	CardIdentification	86
2.21.	CardNumber	86
2.22.	CardPlaceDailyWorkPeriod	87
2.23.	CardPrivateKey	88
2.24.	CardPublicKey	88
2.25.	CardRenewalIndex	88
2.26.	CardReplacementIndex	88

2.27.	CardSlotNumber	88
2.28.	CardSlotsStatus	88
2.29.	CardStructureVersion	89
2.30.	CardVehicleRecord	89
2.31.	CardVehiclesUsed	90
2.32.	Certificate	90
2.33.	CertificateContent	90
2.34.	CertificateHolderAuthorisation	91
2.35.	CertificateRequestID	92
2.36.	CertificationAuthorityKID	92
2.37.	CompanyActivityData	93
2.38.	CompanyActivityType	94
2.39.	CompanyCardApplicationIdentification	94
2.40.	CompanyCardHolderIdentification	95
2.41.	ControlCardApplicationIdentification	95
2.42.	ControlCardControlActivityData	95
2.43.	ControlCardHolderIdentification	96
2.44.	ControlType	97
2.45.	CurrentDateTime	97
2.46.	DailyPresenceCounter	98
2.47.	Datef	98
2.48.	Distance	98
2.49.	DriverCardApplicationIdentification	98
2.50.	DriverCardHolderIdentification	99
2.51.	EntryTypeDailyWorkPeriod	100
2.52.	EquipmentType	100
2.53.	EuropeanPublicKey	101
2.54.	EventFaultType	101
2.55.	EventFaultRecordPurpose	102
2.56.	ExtendedSerialNumber	103
2.57.	FullCardNumber	104
2.58.	HighResOdometer	104
2.59.	HighResTripDistance	104
2.60.	HolderName	104
2.61.	K-ConstantOfRecordingEquipment	105

2.62.	KeyIdentifier	105
2.63.	L-TyreCircumference	105
2.64.	Language.....	105
2.65.	LastCardDownload	106
2.66.	ManualInputFlag.....	106
2.67.	ManufacturerCode	106
2.68.	MemberStateCertificate	108
2.69.	MemberStatePublicKey	108
2.70.	Name	108
2.71.	NationAlpha	108
2.72.	NationNumeric	110
2.73.	NoOfCalibrationRecords	113
2.74.	NoOfCalibrationsSinceDownload	113
2.75.	NoOfCardPlaceRecords.....	113
2.76.	NoOfCardVehicleRecords	113
2.77.	NoOfCompanyActivityRecords.....	113
2.78.	NoOfControlActivityRecords.....	114
2.79.	NoOfEventsPerType.....	114
2.80.	NoOfFaultsPerType	114
2.81.	OdometerValueMidnight	114
2.82.	OdometerShort.....	114
2.83.	OverspeedNumber	114
2.84.	PlaceRecord	115
2.85.	PreviousVehicleInfo	115
2.86.	PublicKey	115
2.87.	RegionAlpha	116
2.88.	RegionNumeric	117
2.89.	RSAPublicKeyModulus.....	117
2.90.	RSAPublicKeyPrivateExponent	118
2.91.	RSAPublicKeyPublicExponent	118
2.92.	SensorApprovalNumber	118
2.93.	SensorIdentification	118
2.94.	SensorInstallation	119
2.95.	SensorInstallationSecData	119
2.96.	SensorOSIdentifier	119

2.97.	SensorPaired	120
2.98.	SensorPairingDate	120
2.99.	SensorSerialNumber	120
2.100.	SensorSCIdentifier	120
2.101.	Signature	120
2.102.	SimilarEventsNumber	121
2.103.	SpecificConditionType	121
2.104.	SpecificConditionRecord	121
2.105.	Speed	121
2.106.	SpeedAuthorised	122
2.107.	SpeedAverage	122
2.108.	SpeedMax	122
2.109.	TDesSessionKey	122
2.110.	TimeReal	122
2.111.	TyreSize	122
2.112.	VehicleIdentificationNumber	123
2.113.	VehicleRegistrationIdentification	123
2.114.	VehicleRegistrationNumber	123
2.115.	VuActivityDailyData	123
2.116.	VuApprovalNumber	124
2.117.	VuCalibrationData	124
2.118.	VuCalibrationRecord	124
2.119.	VuCardIWData	126
2.120.	VuCardIWRecord	126
2.121.	VuCertificate	127
2.122.	VuCompanyLocksData	127
2.123.	VuCompanyLocksRecord	127
2.124.	VuControlActivityData	128
2.125.	VuControlActivityRecord	128
2.126.	VuDataBlockCounter	129
2.127.	VuDetailedSpeedBlock	129
2.128.	VuDetailedSpeedData	129
2.129.	VuDownloadablePeriod	130
2.130.	VuDownloadActivityData	130
2.131.	VuEventData	130

2.132.	VuEventRecord.....	131
2.133.	VuFaultData.....	132
2.134.	VuFaultRecord.....	132
2.135.	VuIdentification.....	133
2.136.	VuManufacturerAddress.....	133
2.137.	VuManufacturerName	134
2.138.	VuManufacturingDate	134
2.139.	VuOverSpeedingControlData.....	134
2.140.	VuOverSpeedingEventData.....	134
2.141.	VuOverSpeedingEventRecord.....	135
2.142.	VuPartNumber	135
2.143.	VuPlaceDailyWorkPeriodData.....	136
2.144.	VuPlaceDailyWorkPeriodRecord.....	136
2.145.	VuPrivateKey	136
2.146.	VuPublicKey.....	136
2.147.	VuSerialNumber	136
2.148.	VuSoftInstallationDate	137
2.149.	VuSoftwareIdentification.....	137
2.150.	VuSoftwareVersion	137
2.151.	VuSpecificConditionData.....	137
2.152.	VuTimeAdjustmentData.....	137
2.153.	VuTimeAdjustmentRecord.....	138
2.154.	W-VehicleCharacteristicConstant	138
2.155.	WorkshopCardApplicationIdentification	138
2.156.	WorkshopCardCalibrationData	139
2.157.	WorkshopCardCalibrationRecord	140
2.158.	WorkshopCardHolderIdentification	141
2.159.	WorkshopCardPIN	141
3.	DEFINICE ROZSAHU HODNOTY A VELIKOSTI.....	142
3.1.	Definice pro kartu řidiče:.....	143
3.2.	Definice pro dílenskou kartu:	143
3.3.	Definice pro kontrolní kartu:	143
3.4.	Definice pro kontrolní kartu:	143
4.	SOUBORY ZNAKŮ	144
5.	KÓDOVÁNÍ.....	144

1. ÚVOD

Tento dodatek určuje formáty dat, prvky dat a struktury dat pro použití v záznamovém zařízení a v kartách tachografů.

1.1. Podklad pro definice typů dat

Tento dodatek používá Abstract Syntax Notation One (ASN.1) k definování typů dat. To umožňuje, že jednoduchá a strukturovaná data jsou definována bez naznačující jakékoliv zvláštní přenosové skladby (kódovací pravidla), která budou závislá na aplikaci a systémovém prostředí.

ASN.1 uvádějící obecné zásady byly provedeny v souladu s ISO/IEC 8824-1. To znamená, že:

- tam, kde je to možné, význam typu dat je naznačen vybranými názvy,
- tam, kde typ dat je skladba jiných typů dat, název typu dat je jednoduchá posloupnost abecedních znaků začínající velkým písmenem, ačkoliv velká písmena jsou použita v názvu ke sdělení příslušného významu,
- názvy typů dat obvykle souvisejí s názvem typů dat od kterých jsou odvozeny, zařízením, v kterém jsou data uložena a funkcí vztahující se k datům.

Jestliže typ ASN.1 je již definován jako část jiné normy a jestliže je toto vhodné pro použití v záznamovém zařízení, pak tento typ ASN.1 bude definován v tomto dodatku.

K uvolnění několika typů kódovacích pravidel některé ASN.1 typy v tomto dodatku jsou vynuceny identifikátory hodnoty rozsahu. Identifikátory hodnoty rozsahu jsou definovány v odstavci 3.

1.2. Odkazy

V tomto dodatku jsou použity související normy:

ISO 639	Kód pro vyjádření názvů jazyků. První vydání: 1988
EN 726-3	Systémy s identifikačními kartami – Telekomunikační karty s integrovanými obvody a koncová zařízení – Část 3: Aplikačně nezávislé požadavky na karty. Prosinec 1994
ISO 3779	Silniční vozidla – Identifikační číslo vozidla (VIN) – Obsah a skladba. Třetí vydání: 1983
ISO/IEC 7816-5	Informační technika – Identifikační karty – Karty s integrovanými obvody a s kontakty – Část 5: Systém číslování a registrační postup identifikátorů aplikací. První vydání: 1994 + Změna 1: 1996

- ISO/IEC 8824-1 Informační technika – Abstraktní syntaktická notace jedna (ASN.1): Specifikace základní notace. Druhé vydání: 1998
- ISO/IEC 8824-2 Informační technika – ASN.1 kódovací pravidla: Specifikace zhuštěných kódovacích pravidel (PER – Packed Encoding Rules). Druhé vydání: 1998
- ISO/IEC 8859-1 Informační technika – Jedním 8-bitovým bytem kódované soubory grafických znaků – Část 1: Latinská abeceda č.1., První vydání: 1998
- ISO/IEC 8859-7 Informační technika – Jedním 8-bitovým bytem kódované soubory grafických znaků – Část 7: Latinská a řecká abeceda. První vydání
- ISO 16844-3 Silniční vozidla – systémy tachografů – Rozhraní snímače pohybu. WD 3-20/05/99.

2. DEFINICE TYPU DAT

Pro jakýkoliv z následujících typů dat standardní hodnota pro „neznámý“ nebo „nevhodný“ obsah bude spočívat v části dat s 'FF'- byty.

2.1. ActivityChangeInfo

Tento typ dat dává možnost kódovat uvnitř dvoubytového slova, status slotu v 00.00 a/nebo status řidiče v 00.00 a/nebo změny činnosti a/nebo změny statusu řízení a/nebo změny statusu karty řidiče nebo druhého řidiče. Tento typ dat se vztahuje k požadavkům 084, 109a, 199 a 219.

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

Přiřazení hodnoty – Osmibitové uspořádání: 'scpaatttttttttt' B (16 bitů)

Pro záznamy do paměti dat (nebo status slotu):

's' B Slot:

'0' B: ŘIDIČ,

'1' B: 2.ŘIDIČ,

'c' B Status řízení vozidla:

'0' B: JEDEN,

'1' B: POSÁDKA,

'p' B Status řidičovy (nebo dílenské) karty v příslušném slotu:

'0' B: VLOŽENA, karta je vložena,

'1'B: NENÍ VLOŽENA, není vložena žádná karta (nebo je karta vyjmuta),

'aa'B Činnost:

'00'B: PŘESTÁVKA/ODPOČINEK,

'01'B: POHOTOVOST,

'10'B: PRÁCE,

'11'B: ŘÍZENÍ,

'tttttttt'B: Čas změny: Počet minut od 00h00 daného dne.

Pro záznamy karty řidiče (nebo dílenské karty) (a status řidiče):

's'B Slot (netýká se jestliže 'p' = 1 kromě dále uvedené poznámky):

'0'B: ŘIDIČ,

'1'B: 2. ŘIDIČ,

'c'B Status řízení vozidla (v případě 'p' = 0) nebo následující status činnosti (v případě 'p' = 1):

'0'B: JEDEN,

'0'B: NEZNÁMÝ

'1'B: POSÁDKA,

'1'B: ZNÁMÝ (= ručně vložený)

'p'B Status karty:

'0'B: VLOŽENA, karta je vložena do záznamového zařízení,

'1'B: NENÍ VLOŽENA, karta není vložena (nebo je karta vyjmuta),

'aa'B Činnost (není důležité, jestliže 'p' = 1 a 'c' = 0 kromě dále uvedené poznámky):

'00'B: PŘESTÁVKA/ODPOČINEK,

'01'B: POHOTOVOST,

'10'B: PRÁCE,

'11'B: ŘÍZENÍ VOZIDLA,

'tttttttt'B Čas změny: Počet minut od 00h00 daného dne.

Poznámka pro případ "vyjmutí karty":

Je-li karta vyjmuta:

- ‘s’ je důležité a je určen slot, ze kterého je karta vyjmuta,
- ‘c’ musí být nastaveno na 0,
- ‘p’ musí být nastaveno na 1,
- ‘aa’ musí být kódována činnost, která v tu dobu probíhá,

Jako výsledek manuálního vstupu bity ‘c’ a ‘aa’ slova (uloženého na kartě) mohou být přepsány později s ohledem na vstup.

2.2. Address

Adresa.

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

codePage udává část ISO/IEC 8859, která je použita ke kódování adresy,

address je adresa kódovaná v souladu s ISO/IEC 8859-codePage.

2.3. BCDString

BCDString se použije pro vyjádření dekadických čísel binárním kódem (BCD). Tento typ dat se použije k vyjádření jedné dekadické číslice skupinou 4 bitů (poloviční oktet). BCDString je založen na ISO/IEC 8824-1 ‘CharacterStringType’.

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

BCDString používá ‘hstring’ notaci. Vnější levá hexadecimální číslice musí být skupinou 4 bitů s nejvyšší hodnotou prvního oktetu. K získání násobku oktetů se musí podle potřeby vložit od pozice levé vnější 4-bitové skupiny v prvním oktetu nulové 4-bitové skupiny.

Přípustné číslice jsou: 0, 1, ... 9.

2.4. CalibrationPurpose

Kód k objasnění, proč soubor kalibračních parametrů byl zaznamenán. Tento typ dat se vztahuje k požadavkům 097 a 098.

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

Přiřazení hodnoty:

‘00’H vyhrazená hodnota,

‘01’H aktivace: záznam známých kalibračních parametrů v okamžiku aktivace celku ve vozidle (VU),

‘02’H první instalace: první kalibrace VU po jeho aktivaci,

‘03’H instalace: první kalibrace VU v běžném vozidle,

‘04’H periodická kontrola.

2.5. CardActivityDailyRecord

Informace, uložené na kartě a vztahující se k činnostem řidiče po určitý kalendářní den. Tento typ dat se vztahuje k požadavkům 199 a 219.

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

activityPreviousRecordLength je celková délka záznamu předešlého dne v bytech. Nejvyšší hodnota je dána délkou OCTET STRING obsahující tyto záznamy (viz CardActivityLengthRange odstavec 3). Jestliže tento záznam je nejdelší denní záznam, potom hodnota activityPreviousRecordLength musí být nastavena na 0.

activityRecordLength je celková délka tohoto záznamu v bytech. Maximální hodnota je dána délkou OCTET STRING, který obsahuje tyto záznamy.

activityRecordDate je datum záznamu.

activityDailyPresenceCounter je denní prezentační čítač pro kartu toho dne.

activityDayDistance je celková vzdálenost ujetá toho dne.

activityChangeInfo je soubor ActivityChangeInfo dat toho dne pro řidiče. Může obsahovat maximálně 1 440 hodnot (jedna změna činnosti za minutu). Tento soubor vždy obsahuje activityChangeInfo pro status řidiče v 00.00.

2.6. CardActivityLengthRange

Počet bytů v kartě řidiče nebo v dílenské kartě, které jsou dostupné k uložení záznamů o činnosti řidiče.

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

Přiřazení hodnoty: viz odstavec 3.

2.7. CardApprovalNumber

Číslo schválení typu karty.

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

Přiřazení hodnoty: Nespecifikovaná.

2.8. CardCertificate

Certifikát veřejného klíče karty.

`CardCertificate ::= Certificate.`

2.9. CardChipIdentification

Informace uložené na kartě určené k identifikaci integrovaného obvodu karty (požadavek 191).

```
CardChipIdentification ::= SEQUENCE {  
    IcSerialNumber          OCTET STRING (SIZE(4)),  
    IcManufacturingReferences OCTET STRING (SIZE(4))  
}
```

icSerialNumber je pořadové číslo integrovaného obvodu dle EN 726-3.

icManufacturingReferences je označení výrobce integrovaného obvodu a výrobního článku dle EN 726-3.

2.10. CardConsecutiveIndex

Pořadový index karty (definice h)).

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

Přiřazení hodnoty: (viz tato příloha, kapitola VII)

Posloupnost: '0, ..., 9, A, ..., Z, a, ..., z'.

2.11. CardControlActivityDataRecord

Informace uložené na kartě řidiče nebo dílenské kartě týkající se poslední kontroly, které byl řidič podroben (požadavky 210 a 225).

```
CardControlActivityDataRecord ::= SEQUENCE {  
    ControlType          controlType,
```

```

ControlTime                TimeReal,

ControlCardNumber          FullCardNumber,

ControlVehicleRegistration  VehicleRegistrationIdentification,

ControlDownloadPeriodBegin TimeReal,

ControlDownloadPeriodEnd   TimeReal,

}

```

controlType je typ kontroly.

controlTime je datum a čas kontroly.

controlCardNumber je FullCardNumber kontrolní úřední osoby mající vykonat kontrolu.

controlVehicleRegistration je registrační číslo vozidla (VRN) a členský stát registrující vozidlo, v kterém byla kontrola provedena.

controlDownloadPeriodBegin and **controlDownloadPeriodEnd** je doba stahování dat v případě stahování.

2.12. CardCurrentUse

Informace o aktuálním použití karty (požadavek 212).

```

CardCurrentUse ::= SEQUENCE {

    SessionOpenTime        TimeReal,

    SessionOpenVehicle      VehicleRegistrationIdentification

}

```

sessionOpenTime je čas, kdy je karta vložena pro běžné použití. Tato položka se nastavuje na nulu při vyjmutí karty.

sessionOpenVehicle je identifikace běžného použití vozidla nastaveného při vložení karty. Tato položka se nastavuje na nulu při vyjmutí karty.

2.13. CardDriverActivity

Informace uložené na kartě řidiče nebo dílenské kartě týkající se činnosti řidiče (požadavky 199 a 219).

```

CardDriverActivity ::= SEQUENCE {

    ActivityPointerOldestDayRecord
        INTEGER(0..CardActivityLengthRange-1),

```

```

    ActivityPointerNewestRecord
        INTEGER (0..CardActivityLengthRange-1),

    ActivityDailyRecords    OCTET
                           STRING (SIZE (CardActivityLengthRange))

}

```

activityPointerOldestDayRecord je určení začátku paměťového místa (počet bytů od začátku řetězce) nejstaršího úplného denního záznamu v řetězci activityDailyRecords. Maximální hodnota je dána délkou řetězce.

activityPointerNewestRecord je určení začátku paměťového místa (počet bytů od začátku řetězce) nejmladšího denního záznamu v řetězci activityDailyRecords. Maximální hodnota je dána délkou řetězce

activityDailyRecords je prostor vhodný k uložení dat činnosti řidiče (struktura dat: CardActivityDailyRecord) pro každý kalendářní den, kdy byla karta použita.

Přiřazení hodnoty: tento osmibitový řetězec je cyklicky plněn záznamy CardActivityDailyRecord. Při prvním použití začíná ukládání do paměti na prvním bytu řetězce. Všechny nové záznamy jsou připojeny na konec předchozího. Když je řetězec plný, ukládání pokračuje na prvním bytu řetězce nezávisle na přerušení, které je uvnitř datového prvku. Před umístěním dat nové činnosti do řetězce (zvětšení běžné activityDailyRecord nebo umístění nové activityDailyRecord), která nahrazuje starší data činnosti, activityPointerOldestDayRecord musí být aktualizovány k vyjádření nového umístění nejstaršího úplného denního záznamu a activityPreviousRecordLength tohoto (nového) nejstaršího úplného denního záznamu musí být nastavena na nulu.

2.14. CardDrivingLicenceInformation

Informace uložené na kartě řidiče týkající se dat karty držitele řidičského oprávnění (požadavek 196).

```

CardDrivingLicenceInformation ::= SEQUENCE {

    drivingLicenceIssuingAuthority    Name,

    drivingLicenceIssuingNation       NationNumeric,

    drivingLicenceNumber              IA5String (SIZE (16))

}

```

drivingLicenceIssuingAuthority je správní orgán zodpovědný za vydání řidičského oprávnění.

drivingLicenceIssuingNation je národní správní orgán, který vydává řidičské oprávnění.

drivingLicenceNumber je číslo řidičského oprávnění.

2.15. CardEventData

Informace uložené na kartě řidiče nebo dílenské kartě týkající se událostí v souvislosti s kartou držitele (požadavky 204 a 223).

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

CardEventData je posloupnost hodnot **EventFaultType** uspořádaná vzestupně, hodnot **cardEventRecords** (kromě pokusů narušení spolehlivosti záznamů, které jsou seskupeny v posledním souboru posloupnosti).

2.16. CardEventRecord

Informace uložené na kartě řidiče nebo dílenské kartě týkající se události v souvislosti s kartou držitele (požadavky 205 a 223).

```
CardEventRecord ::= SEQUENCE {  
  
    EventType                  EventFaultType,  
  
    EventBeginTime             TimeReal,  
  
    EventEndTime               TimeReal,  
  
    EventVehicleRegistration   VehicleRegistrationIdentification  
  
}
```

eventType je typ události.

eventBeginTime je datum a čas začátku události.

eventEndTime je datum a čas konce události.

eventVehicleRegistration je registrační číslo vozidla (VRN) a členský stát registrující vozidlo, v kterém se událost stala.

2.17. CardFaultData

Informace uložené na kartě řidiče nebo dílenské kartě týkající se závad v souvislosti s kartou držitele (požadavky 207 a 223).

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

CardFaultData je posloupnost záznamů závad záznamového zařízení doprovázená záznamy závad karty.

cardFaultRecords je soubor záznamů závad určité kategorie závad (záznamové zařízení nebo karta).

2.18. CardFaultRecord

Informace uložené na kartě řidiče nebo dílenské kartě týkající se závad v souvislosti s kartou držitele (požadavky 208 a 223).

```
CardFaultRecord ::= SEQUENCE {
    FaultType                EventFaultType,
    FaultBeginTime           TimeReal,
    FaultEndTime             TimeReal,
    FaultVehicleRegistration VehicleRegistrationIdentification
}
```

faultType je typ závady.

faultBeginTime je datum a čas začátku závady.

faultEndTime je datum a čas konce závady.

faultVehicleRegistration je registrační číslo vozidla (VRN) členský stát registrující vozidlo, v kterém porucha nastala.

2.19. CardIccIdentification

Informace uložené na kartě týkající se označení karty s integrovaným obvodem (IC) (požadavek 192).

```
CardIccIdentification ::= SEQUENCE {
    ClockStop                OCTET STRING (SIZE(1)),
    CardExtendedSerialNumber ExtendedSerialNumber,
    CardApprovalNumber       CardApprovalNumber
    CardPersonaliserID       OCTET STRING (SIZE(1)),
    EmbedderIcAssemblerId    OCTET STRING (SIZE(5)),
    IccIdentifier             OCTET STRING (SIZE(2))
}
```

clockStop je Clockstop mód dle EN 726-3.

cardExtendedSerialNumber je pořadové číslo karty s integrovaným obvodem (IC) a výrobní údaj IC karty dle EN 726-3 a jak je dále specifikováno typem dat ExtendedSerialNumber.

cardApprovalNumber je číslo schválení typu karty.

cardPersonaliserID je karta personaliser - ID dle definice v EN 726-3.

embedderIcAssemblerId je výrobce karty/IC assembler identifikátor dle EN 726-3.

icIdentifier je identifikátor IC na kartě a výrobce IC dle EN 726-3.

2.20. CardIdentification

Informace uložené na kartě týkající se identifikace karty (požadavky 194, 215, 231, 235).

CardIdentification ::= SEQUENCE

```

    CardIssuingMemberState      NationNumeric,
    CardNumber                   CardNumber,
    CardIssuingAuthorityName     Name,
    CardIssueDate                TimeReal,
    cardValidityBegin            TimeReal,
    cardExpiryDate               TimeReal
}

```

cardIssuingMemberState je kód členského státu vydávajícího kartu.

cardNumber je číslo karty.

cardIssuingAuthorityName je název správního orgánu vydávajícího kartu.

cardIssueDate je datum vydání karty současnému držiteli.

cardValidityBegin je datum začátku platnosti karty.

cardExpiryDate je datum konce platnosti karty.

2.21. CardNumber

Číslo karty dle definice g).

CardNumber ::= CHOICE {

SEQUENCE {

DriverIdentification IA5String(SIZE(14)),

```

        CardReplacementIndex      CardReplacementIndex,
        CardRenewalIndex          CardRenewalIndex
    }

    SEQUENCE {
        OwnerIdentification        IA5String(SIZE(13)),
        CardConsecutiveIndex      CardConsecutiveIndex,
        CardReplacementIndex      CardReplacementIndex,
        CardRenewalIndex          CardRenewalIndex
    }
}

```

driverIdentification je jednoznačná identifikace řidiče v členském státě.

ownerIdentification je jednoznačná identifikace společnosti nebo dílny nebo kontrolního orgánu v členském státě.

cardConsecutiveIndex je pořadový index karty.

cardReplacementIndex je index náhrady karty.

cardRenewalIndex je index obnovy karty.

První posloupnost výběru je vhodná ke kódování čísla karty řidiče, druhá posloupnost výběru je vhodná ke kódování čísel dílenské karty, kontrolní karty a karty společnosti.

2.22. CardPlaceDailyWorkPeriod

Informace uložené na kartě řidiče nebo dílenské kartě týkající se míst, kde denní pracovní doba začíná a/nebo končí (požadavky 202 a 221).

```

CardPlaceDailyWorkPeriod ::= SEQUENCE {
    PlacePointerNewestRecord  INTEGER(0..NoOfCardPlaceRecords-1),
    placeRecords SET          SIZE(NoOfCardPlaceRecords) OF
                                PlaceRecord
}

```

placePointerNewestRecord je index posledně aktualizovaného záznamu o místě.

Přiřazení hodnoty: Číslo odpovídající čítači záznamu míst začínající '0' pro první výskyt záznamu místa ve struktuře.

placeRecords je soubor záznamů obsahující informaci týkající se vložených míst.

2.23. CardPrivateKey

Soukromý klíč karty.

`CardPrivateKey ::= RSAKeyPrivateExponent.`

2.24. CardPublicKey

Veřejný klíč karty.

`CardPublicKey ::= PublicKey.`

2.25. CardRenewalIndex

Index obnovy karty (definice i)).

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

Přiřazení hodnoty: (viz kapitola VII v této příloze).

‘0’ První vydání.

Pořadí pro zvýšení: ‘0, ..., 9, A, ..., Z’.

2.26. CardReplacementIndex

Index náhrady karty (definice j)).

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

Přiřazení hodnoty: (viz kapitola VII v této příloze).

‘0’ Původní karta.

Pořadí pro zvýšení: ‘0, ..., 9, A, ..., Z’.

2.27. CardSlotNumber

Kód pro rozlišení mezi dvěma sloty celku ve vozidle.

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

Přiřazení hodnoty: není dále specifikováno.

2.28. CardSlotsStatus

Kód k indikaci typu karet vložených do dvou slotů celku ve vozidle.

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

Přiřazení hodnoty – osmibitové uspořádání: 'ccccdddd' B:

'cccc' B Identifikace typu karty vložené do slotu druhého řidiče,

'dddd' B Identifikace typu karty vložené do slotu řidiče,

s následujícími identifikačními kódy:

'0000' B není vložena žádná karta,

'0001' B je vložena karta řidiče,

'0010' B je vložena dílenská karta,

'0011' B je vložena kontrolní karta,

'0100' B je vložena karta společnosti.

2.29. CardStructureVersion

Kód indikující verzi realizované struktury v kartě tachografu.

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

Přiřazení hodnoty: 'aabb' H:

'aa' H Index změn struktury,

'bb' H Index změn týkajících se použití prvků dat definovaných pro strukturu danou horním bytem.

2.30. CardVehicleRecord

Informace uložené na kartě řidiče nebo dílenské kartě týkající se doby použití vozidla během kalendářního dne (požadavky 197 a 217).

```
CardVehicleRecord ::= SEQUENCE {  
    VehicleOdometerBegin     OdometerShort,  
    VehicleOdometerEnd       OdometerShort,  
    VehicleFirstUse           TimeReal,  
    VehicleLastUse            TimeReal,  
    VehicleRegistration       VehicleRegistrationIdentification,  
    VuDataBlockCounter        VuDataBlockCounter  
}
```

vehicleOdometerBegin je hodnota měřiče ujeté vzdálenosti na začátku doby použití vozidla.

vehicleOdometerEnd je hodnota měřiče ujeté vzdálenosti na konci doby použití vozidla.

vehicleFirstUse je datum a čas začátku doby použití vozidla.

vehicleLastUse je datum a čas konce doby použití vozidla.

vehicleRegistration je registrační číslo vozidla (VRN) a členský stát registrující vozidlo.

vuDataBlockCounter je hodnota VuDataBlockCounter při posledním výpisu doby použití vozidla.

2.31. CardVehiclesUsed

Informace uložené na kartě řidiče nebo dílenské kartě týkající vozidel použitých držitelem karty (požadavky 197 a 217).

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

vehiclePointerNewestRecord je index posledního aktualizovaného záznamu vozidla.

Přiřazení hodnoty: Číslo odpovídající čítači záznamů vozidla začínající '0' pro první výskyt záznamu vozidla ve struktuře.

cardVehicleRecords je soubor záznamů obsahující informace o použití vozidla.

2.32. Certificate

Certifikát veřejného klíče vydaný certifikačním orgánem.

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

Přiřazení hodnoty: digitální podpis s částečnou obnovou CertificateContent podle dodatku 11 "společný bezpečnostní mechanismus": Signature (128 bytes) || Public Key remainder (58 Byte) || Certification Authority Reference (8 bytes).

2.33. CertificateContent

(Čistý) obsah certifikátu veřejného klíče podle dodatku 11 "společný bezpečnostní mechanismus".

```

CertificateContent ::= SEQUENCE {
    CertificateProfileIdentifier      INTEGER(0..255),
    CertificationAuthorityReference  KeyIdentifier,
    CertificateHolderAuthorisation   CertificateHolder
                                    Authorisation,
    CertificateEndOfValidity         TimeReal,
    CertificateHolderReference       KeyIdentifier,
    PublicKey                       PublicKey
}

```

certificateProfileIdentifier je verze odpovídajícího certifikátu.

Přiřazení hodnoty: '01h' pro tuto verzi.

CertificationAuthorityReference identifikuje certifikační orgán vydávající certifikát a zároveň obsahuje odkaz na veřejný klíč tohoto certifikačního orgánu.

certificateHolderAuthorisation identifikuje práva držitele certifikátu.

certificateEndOfValidity je datum, kdy platnost certifikátu končí.

certificateHolderReference identifikuje držitele certifikátu a obsahuje zároveň odkaz na jeho veřejný klíč.

publicKey je veřejný klíč, který je certifikován tímto certifikátem.

2.34. CertificateHolderAuthorisation

Identifikace práv držitele certifikátu.

```

CertificateHolderAuthorisation ::= SEQUENCE {
    TachographApplicationID      OCTET STRING(SIZE(6))
    EquipmentType                 EquipmentType
}

```

tachographApplicationID je identifikátor použití pro použití tachografu.

Přiřazení hodnoty: 'FFh' '54h' '41h' '43h' '48h' '4Fh'. Tento AID je vlastnický neregistrovaný identifikátor použití v souladu s ISO/IEC 7816-5.

equipmentType je identifikace typu zařízení, pro které je certifikát určen.

Přiřazení hodnoty: ve shodě s typem dat EquipmentType. 0 jestliže se jedná o certifikát jednoho z členských států.

2.35. CertificateRequestID

Jednoznačná identifikace žádosti o certifikát. Může být použita také jako identifikátor veřejného klíče celku ve vozidle, jestliže pořadové číslo celku ve vozidle, ke kterému je určený klíč, není známo v době vystavení certifikátu.

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

requestSerialNumber je pořadové číslo žádosti o certifikát pro dále jednoznačně určeného výrobce a měsíce.

requestMonthYear je identifikace měsíce a roku žádosti o certifikát.

Přiřazení hodnoty: BCD kód měsíce (dvě číslice) a roku (poslední dvě číslice).

crIdentifier je identifikátor k rozlišení žádosti o certifikát od rozšířeného pořadového čísla.

Přiřazení hodnoty: 'FFh'.

manufacturerCode je číselný kód výrobce žádajícího o certifikát.

2.36. CertificationAuthorityKID

Identifikátor veřejného klíče orgánu, který vydává certifikát (členský stát nebo Evropský certifikační orgán).

```
CertificationAuthorityKID ::= SEQUENCE {
    NationNumeric             NationNumeric
    NationAlpha               NationAlpha
    KeySerialNumber           INTEGER(0..255)
    AdditionalInfo            OCTET STRING(SIZE(2))
    CaIdentifier               OCTET STRING(SIZE(1))
}
```

nationNumeric je číselný kód státu certifikačního orgánu.

nationAlpha je alfanumerický kód státu certifikačního orgánu.

keySerialNumber je pořadové číslo k rozlišení různých klíčů certifikačního orgánu v případě, že se klíče mění.

additionalInfo je dvoubytové pole pro dodatečné kódování (podle certifikačního orgánu).

caIdentifier je identifikátor k rozlišení identifikátoru klíče certifikačního orgánu od identifikátorů klíče.

Přiřazení hodnoty: '01h'.

2.37. CompanyActivityData

Informace uložené na kartě společnosti týkající se činností vykonaných s kartou (požadavek 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 je index poslední aktualizace companyActivityRecord.

Přiřazení hodnoty: Číslo odpovídající čítači záznamu činnosti společnosti, začínající '0' pro první výskyt záznamu činnosti společnosti ve struktuře.

companyActivityRecords je soubor všech záznamů o činnosti společnosti.

companyActivityRecord je posloupnost informací vztahujících se k jedné činnosti společnosti.

companyActivityType je typ činnosti společnosti.

companyActivityTime je datum a čas činnosti společnosti.

cardNumberInformation je číslo karty a členského státu vydávajícího kartu, z které jsou stažena data.

vehicleRegistrationInformation je registrační číslo vozidla (VRN) a registrace členského státu, jejichž data jsou stažena, zablokována nebo odblokována.

downloadPeriodBegin and **downloadPeriodEnd** je začátek a konec doby stahování dat z celku ve vozidle.

2.38. CompanyActivityType

Kód indikující činnost provedenou společnostmi používající karu společnosti.

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

2.39. CompanyCardApplicationIdentification

Informace uložené na kartě společnosti týkající se identifikace žádosti o kartu (požadavek 190).

```
CompanyCardApplicationIdentification ::= SEQUENCE {
    TypeOfTachographCardId      EquipmentType,
    CardStructureVersion         CardStructureVersion,
    NoOfCompanyActivityRecords   NoOfCompanyActivityRecords
}
```

typeOfTachographCardId udává implementovaný typ karty.

cardStructureVersion udává verzi struktury, která je do karty implementována.

noOfCompanyActivityRecords je počet záznamů činnosti společnosti, které lze na kartu uložit.

2.40. CompanyCardHolderIdentification

Informace uložené na kartě společnosti týkající se identifikace držitele karty (požadavek 236).

```
CompanyCardHolderIdentification ::= SEQUENCE {  
    CompanyName                Name,  
    CompanyAddress             Address,  
    CardHolderPreferredLanguage Language  
}
```

companyName je název majitele společnosti.

companyAddress je adresa majitele společnosti.

cardHolderPreferredLanguage je mateřský jazyk držitele karty

2.41. ControlCardApplicationIdentification

Informace uložené na kontrolní kartě týkající se identifikace žádosti o kartu (požadavek 190).

```
ControlCardApplicationIdentification ::= SEQUENCE {  
    TypeOfTachographCardId      EquipmentType,  
    CardStructureVersion         CardStructureVersion,  
    NoOfControlActivityRecords   NoOfControlActivityRecords  
}
```

typeOfTachographCardId udává implementovaný typ karty.

cardStructureVersion udává verzi struktury, která je v kartě implementována.

noOfControlActivityRecords je počet záznamů kontrol činnosti, které mohou být na kartu uloženy.

2.42. ControlCardControlActivityData

Informace uložené na kontrolní kartě týkající se kontrol činnosti vykonaných s kartou (požadavek 223).

```
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 je index posledně aktualizovaného záznamu kontroly činnosti.

Přiřazení hodnoty: Číslo odpovídající čítači záznamu kontrol činnosti., začínající '0' pro první výskyt záznamu kontrol činnosti ve struktuře.

controlActivityRecords je soubor všech záznamů kontrol činnosti.

controlActivityRecord je posloupnost informací vztahující se k jedné kontrole.

controlType je typ kontroly.

controlTime je datum a čas kontroly.

controlledCardNumber je číslo karty a členského státu vydávajícího kartu a kontrolujícího kartu.

controlledVehicleRegistration je registrační číslo vozidla (VRN) a členský stát registrující vozidlo v kterém byla karta kontrolována.

controlDownloadPeriodBegin a **controlDownloadPeriodEnd** je začátek a konec doby během které byla stahována data.

2.43. ControlCardHolderIdentification

Informace uložené na kontrolní kartě týkající se identifikace držitele karty (požadavek 232).

```

ControlCardHolderIdentification ::= SEQUENCE {
    ControlBodyName          Name,
    ControlBodyAddress       Address,
    CardHolderName           HolderName,

```



```

        CardHolderPreferredLanguage    Language
    }

```

controlBodyName je název kontrolního orgánu držitele karty.

controlBodyAddress je adresa kontrolního orgánu držitele karty.

cardHolderName je příjmení a jméno držitele kontrolní karty.

cardHolderPreferredLanguage je mateřský jazyk držitele karty.

2.44. ControlType

Kód indikující činnosti provedené během kontroly. Tento typ dat se vztahuje k požadavkům 102, 210 a 225.

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

Přiřazení hodnoty – Osmibitové uspořádání: 'cvpdx' B (8 bitů)

'c' B	stahování dat z karty
'0' B:	data se nestahují z karty během této kontrolní činnosti,
'1' B:	data se stahují z karty během této kontrolní činnosti,
'v' B	stahování dat z celku ve vozidle (VU):
'0' B:	data se nestahují z VU během této kontrolní činnosti,
'1' B:	data se stahují z VU během této kontrolní činnosti
'p' B	tisk:
'0' B:	netiskne se během této kontrolní činnosti,
'1' B:	tiskne se během této kontrolní činnosti
'd' B	zobrazení:
'0' B:	nepoužije se zobrazení během této kontrolní činnosti,
'1' B:	použije se zobrazení během této kontrolní činnosti,
'xxxx' B	nepoužije se.

2.45. CurrentDateTime

Aktuální datum a čas záznamového zařízení.

```
CurrentDateTime ::= TimeReal
```

Přiřazení hodnoty: žádná další specifikace.

2.46. DailyPresenceCounter

Čítač uložený v kartě řidiče a dílenské kartě přičítající jedničku pro každý kalendářní den, karta byla vložena do celku ve vozidle (VU). Tato data se vztahují k požadavkům 199 a 219.

DailyPresenceCounter ::= BCDString(SIZE(2))

Přiřazení hodnoty: Pořadové číslo s maximální hodnotou = 9 999, začínající 0. V okamžiku prvního vydání karty se číslo nastavuje na 0.

2.47. Datef

Datum vyjádřený v číselném tvaru, který lze snadno tisknout.

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

Přiřazení hodnoty:

YYYY	rok
mm	měsíc
dd	den

'00000000'H nezobrazuje explicitně žádný datum.

2.48. Distance

Ujetá vzdálenost (výsledek rozdílu mezi dvěma údaji měřiče ujeté vzdálenosti v kilometrech).

Distance ::= INTEGER(0..2¹⁶-1)

Přiřazení hodnoty: Binární číslo bez znaménka. Hodnota v km v provozním rozsahu 0 až 9 999 km.

2.49. DriverCardApplicationIdentification

Informace uložené na kartě řidiče týkající se identifikace žádosti o kartu (požadavek 190).

DriverCardApplicationIdentification ::= SEQUENCE {

```

        TypeOfTachographCardId      EquipmentType,
        CardStructureVersion         CardStructureVersion,
        NoOfEventsPerType            NoOfEventsPerType,
        NoOfFaultsPerType            NoOfFaultsPerType,
        ActivityStructureLength       CardActivityLengthRange,
        NoOfCardVehicleRecords       NoOfCardVehicleRecords,
        NoOfCardPlaceRecords         NoOfCardPlaceRecords
    }

```

typeOfTachographCardId udává implementovaný typ karty.

cardStructureVersion udává verzi struktury, která je implementována v kartě.

noOfEventsPerType je počet událostí od každého typu události, který může karta zaznamenat.

noOfFaultsPerType je počet závad od každého typu závady, který může karta zaznamenat.

activityStructureLength udává počet bytů, které jsou k dispozici pro uložení záznamů činnosti.

noOfCardVehicleRecords je počet záznamů vozidla, které karta může obsahovat.

noOfCardPlaceRecords je počet míst, který může karta zaznamenat.

2.50. DriverCardHolderIdentification

Informace uložené na kartě řidiče týkající se identifikace držitele karty (požadavek 195).

```

DriverCardHolderIdentification ::= SEQUENCE {
    CardHolderName          HolderName,
    CardHolderBirthDate     Datef,
    CardHolderPreferredLanguage Language
}

```

cardHolderName je příjmení a jméno držitele karty řidiče.

cardHolderBirthDate je datum narození držitele karty řidiče.

cardHolderPreferredLanguage je mateřský jazyk držitele karty.

2.51. EntryTypeDailyWorkPeriod

Kód k rozlišení mezi začátkem a koncem zápisu pracovních dnů a vstupních podmínek.

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)

}

Přiřazení hodnoty: dle ISO/IEC8824-1.

2.52. EquipmentType

Kód k rozlišení různých typů zařízení pro aplikaci jako tachograf.

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)

Přiřazení hodnoty: dle ISO/IEC 8824-1.

Hodnota 0 je vyhrazena pro účely označení členského státu nebo Evropy v CHA poli certifikátů.

2.53. EuropeanPublicKey

Evropský veřejný klíč.

EuropeanPublicKey ::= PublicKey.

2.54. EventFaultType

Kód blíže určující událost nebo závadu.

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

Přiřazení hodnoty:

'0x' H	všeobecné události,
'00' H	žádné další podrobnosti,
'01' H	vložení neplatné karty,
'02' H	konflikt karty,
'03' H	časové překrytí,
'04' H	řízení bez vhodné karty,
'05' H	vložení karty během řízení,
'06' H	poslední případ nebyl správně uzavřen,
'07' H	překročení rychlosti,
'08' H	přerušování napájení,
'09' H	chyba dat dráhy a rychlosti,
'0A' H to '0F' H	RFU, (vyhrazeno pro budoucí funkce)
'1x' H	narušení spolehlivosti celku ve vozidle,
'10' H	žádné další podrobnosti,
'11' H	porucha snímače pohybu (dráhy a rychlosti),
'12' H	porucha karty tachografu,
'13' H	neoprávněná výměna snímače pohybu,
'14' H	chyba celistvosti vstupních dat karty,
'15' H	chyba celistvosti dat uložených uživatelem,
'16' H	chyba přenosu interních dat,

'17' H	neoprávněné otevření pouzdra,
'18' H	hardwarové záškodnictví,
'19' H to '1F' H	RFU,
'2x' H	narušení spolehlivosti snímače dráhy a/nebo rychlosti,
'20' H	žádné další podrobnosti,
'21' H	ověření poruchy,
'22' H	chyba celistvosti uložených dat,
'23' H	chyba přenosu interních dat,
'24' H	neoprávněné otevření pouzdra,,
'25' H	hardwarové záškodnictví,
'26' H to '2F' H	RFU,
'3x' H	závady záznamového zařízení,
'30' H	žádné další podrobnosti,
'31' H	interní závada celku ve vozidle (VU),
'32' H	závada tisku,
'33' H	závada zobrazení,
'34' H	závada stahování dat,
'35' H	závada snímače,
'36' H to '3F' H	RFU,
'4x' H	závady karty,
'40' H	žádné další podrobnosti,
'41' H to '4F' H	RFU,
'50' H to '7F' H	RFU,
'80' H to 'FF' H	týkající se výrobce,

2.55. EventFaultRecordPurpose

Kód vysvětlující, proč událost nebo závada byla zaznamenána.

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

Přiřazení hodnoty:

'00'H	jedna z 10 nejmladších událostí nebo závad,
'01'H	nejdelší událost, která se vyskytla během jednoho z 10 posledních dnů,
'02'H	jedna z 5 nejdelších událostí během posledních 365 dní,
'03'H	poslední událost, která se vyskytla během jednoho z 10 posledních dnů,
'04'H	nejvážnější událost, která se vyskytla během jednoho z posledních 10 dnů,
'05'H	jedna z 5 nejvážnějších událostí během posledních 365 dní,
'06'H	první událost nebo závada, která se vyskytla po poslední kalibraci,
'07'H	působící/pokračující událost nebo závada,
'08'H to '7F'H	RFU,
'80'H to 'FF'H	týkající se výrobce.

2.56. ExtendedSerialNumber

Jednoznačná identifikace zařízení. Může také být použito jako identifikátor veřejného klíče.

```
ExtendedSerialNumber ::= SEQUENCE {
    SerialNumber          INTEGER(0..232-1)
    MonthYear             BCDString(SIZE(2))
    type OCTET            STRING(SIZE(1))
    manufacturerCode      ManufacturerCode
}
```

serialNumber je pořadové číslo zařízení, jednoznačné pro výrobce, typ zařízení a dále uvedený měsíc.

monthYear je identifikace měsíce a roku výroby (nebo pořadové číslo přiřazení).

Přiřazení hodnoty: BCD kód měsíce (dvě číslice) a rok (dvě poslední číslice).

type je identifikátor typu zařízení.

Přiřazení hodnoty: týká se výrobce, s vyhrazenou hodnotou FFh'.

manufacturerCode: je číselný kód výrobce zařízení.

2.57. FullCardNumber

Kód plně identifikující kartu tachografu.

```
FullCardNumber ::= SEQUENCE {  
    CardType                               EquipmentType,  
    CardIssuingMemberState                 NationNumeric,  
    CardNumber                             CardNumber  
}
```

cardType je typ karty tachografu.

cardIssuingMemberState je kód členského státu vydávajícího kartu.

cardNumber je číslo karty.

2.58. HighResOdometer

Údaj měřiče ujeté vzdálenosti: Akumulovaná ujetá vzdálenost vozidlem během jeho činnosti.

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

Přiřazení hodnoty Binární číslo bez znaménka. Hodnota v 1/200 km v provozním rozsahu 0 až 21 055 406 km.

2.59. HighResTripDistance

Vzdálenost ujetá během všech částí cesty.

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

Přiřazení hodnoty Binární číslo bez znaménka. Hodnota v 1/200 km v provozním rozsahu 0 až 21 055 406 km.

2.60. HolderName

Příjmení a jméno držitele karty.

```
HolderName ::= SEQUENCE {  
    HolderSurname                Name,  
    HolderFirstNames             Name  
}
```


holderSurname je příjmení držitele. Toto příjmení neobsahuje titul.

Přiřazení hodnoty: Jestliže karta není osobní, holderSurname obsahuje stejné informace jako companyName nebo workshopName nebo controlBodyName.

holderFirstNames je jméno a iniciály držitele.

2.61. K-ConstantOfRecordingEquipment

Konstanta záznamového zařízení (definice m)).

`K-ConstantOfRecordingEquipment ::= INTEGER(0..216-1)`

Přiřazení hodnoty: Impulzy na kilometr v provozním rozsahu 0 až 64 255 impulz/km.

2.62. KeyIdentifier

Jednoznačný identifikátor veřejného klíče použitý k odkazu a výběru klíče. Ten také identifikuje držitele klíče.

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

První výběr je vhodný k odkazu na veřejný klíč celku ve vozidle nebo kartu tachografu.

Druhý výběr je vhodný k odkazu na veřejný klíč celku ve vozidle (pokud pořadové číslo celku ve vozidle nemůže být známé v čase vydání certifikátu).

Třetí výběr je vhodný k odkazu na veřejný klíč členského státu.

2.63. L-TyreCircumference

Efektivní obvod pneumatik kol (definice u)).

`L-TyreCircumference ::= INTEGER(0..216-1)`

Přiřazení hodnoty: : Binární číslo bez znaménka, hodnota v 1/8 mm v provozním rozsahu 0 až 8 031 mm.

2.64. Language

Kód identifikující jazyk.

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

Přiřazení hodnoty: Dvě malá písmena kódovaná dle ISO 639.

2.65. LastCardDownload

Datum a čas uložené na kartě řidiče, posledně stažená data z karty (pro jiné účely jako kontrola). Tento datum může být aktualizován libovolným celkem ve vozidle nebo čtečkou karet.

LastCardDownload ::= TimeReal

Přiřazení hodnoty: není blíže specifikováno.

2.66. ManualInputFlag

Kód udávající, zda držitel karty ručně vložil činnosti řidiče při zasunutí karty nebo ne (požadavek 081).

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

Přiřazení hodnoty: není blíže specifikováno.

2.67. ManufacturerCode

Kód identifikující výrobce.

ManufacturerCode ::= INTEGER(0..255)

Přiřazení hodnoty:

'00'H	žádné informace k dispozici
'01'H	vyhrazená hodnota
'02'H .. '0F'H	vyhrazeno pro budoucí použití
'10'H	ACTIA
'11'H .. '17'H	vyhrazeno pro výrobce, jehož název začíná 'A'
'18'H .. '1F'H	vyhrazeno pro výrobce, jehož název začíná 'B'
'20'H .. '27'H	vyhrazeno pro výrobce, jehož název začíná 'C'
'28'H .. '2F'H	vyhrazeno pro výrobce, jehož název začíná 'D'
'30'H .. '37'H	vyhrazeno pro výrobce, jehož název začíná 'E'

'38' H .. '3F' H	vyhrazeno pro výrobce, jehož název začíná 'F'
'40' H	Giesecke & Devrient GmbH
'41' H	GEM plus
'42' H .. '47' H	vyhrazeno pro výrobce, jehož název začíná 'G'
'48' H .. '4F' H	vyhrazeno pro výrobce, jehož název začíná 'H'
'50' H .. '57' H	vyhrazeno pro výrobce, jehož název začíná 'I'
'58' H .. '5F' H	vyhrazeno pro výrobce, jehož název začíná 'J'
'60' H .. '67' H	vyhrazeno pro výrobce, jehož název začíná 'K'
'68' H .. '6F' H	vyhrazeno pro výrobce, jehož název začíná 'L'
'70' H .. '77' H	vyhrazeno pro výrobce, jehož název začíná 'M'
'78' H .. '7F' H	vyhrazeno pro výrobce, jehož název začíná 'N'
'80' H	OSCARD
'81' H .. '87' H	vyhrazeno pro výrobce, jehož název začíná 'O'
'88' H .. '8F' H	vyhrazeno pro výrobce, jehož název začíná 'P'
'90' H .. '97' H	vyhrazeno pro výrobce, jehož název začíná 'Q'
'98' H .. '9F' H	vyhrazeno pro výrobce, jehož název začíná 'R'
'A0' H	SETEC
'A1' H	SIEMENS VDO
'A2' H	STONERIDGE
'A3' H .. 'A7' H	vyhrazeno pro výrobce, jehož název začíná 'S'
'AA' H	TACHOCONTROL
'AB' H .. 'AF' H	vyhrazeno pro výrobce, jehož název začíná 'T'
'B0' H .. 'B7' H	vyhrazeno pro výrobce, jehož název začíná 'U'
'B8' H .. 'BF' H	vyhrazeno pro výrobce, jehož název začíná 'V'
'C0' H .. 'C7' H	vyhrazeno pro výrobce, jehož název začíná 'W'
'C8' H .. 'CF' H	vyhrazeno pro výrobce, jehož název začíná 'X'

`'D0'H .. 'D7'H` vyhrazeno pro výrobce, jehož název začíná 'Y'

`'D8'H .. 'DF'H` vyhrazeno pro výrobce, jehož název začíná 'Z'

2.68. MemberStateCertificate

Certifikát veřejného klíče členského státu vydaný Evropským certifikačním orgánem.

`MemberStateCertificate ::= Certificate`

2.69. MemberStatePublicKey

Veřejný klíč členského státu.

`MemberStatePublicKey ::= PublicKey.`

2.70. Name

Název.

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

codePage určuje část ISO/IEC 8859 používané ke kódování názvu,

name je název kódovaný v souladu s ISO/IEC 8859-codePage.

2.71. NationAlpha

Abecední označení státu, odpovídající obvyklé poznávací značce státu na nárazníku vozidla a/nebo použité v mezinárodním dokladu o pojištění motorového vozidla (zelená karta).

`NationAlpha ::= IA5String(SIZE(3))`

Přiřazení hodnoty:

<code>' '</code>	žádné informace k dispozici
<code>'A'</code>	Rakousko
<code>'AL'</code>	Albánie
<code>'AND'</code>	Andorra
<code>'ARM'</code>	Arménie
<code>'AZ'</code>	Azerbájdžán

'B'	Belgie
'BG'	Bulharsko
'BIH'	Bosna a Hercegovina
'BY'	Bělorusko
'CH'	Švýcarsko
'CY'	Kypr
'CZ'	Česká republika
'D'	Německo
'DK'	Dánsko
'E'	Španělsko
'EST'	Estonsko
'F'	Francie
'FIN'	Finsko
'FL'	Lichtenštejnsko
'FR'	Faerské ostrovy
'UK'	Spojené království, Alderney, Guernsey, Jersey, Ostrov Man, Gibraltar
'GE'	Gruzie
'GR'	Řecko
'H'	Maďarsko
'HR'	Chorvatsko
'I'	Itálie
'IRL'	Irsko
'IS'	Island
'KZ'	Kazachstán
'L'	Lucembursko
'LT'	Litva

'LV'	Lotyšsko
'M'	Malta
'MC'	Monako
'MD'	Moldávie
'MK'	Makedonie
'N'	Norsko
'NL'	Nizozemsko
'P'	Portugalsko
'PL'	Polsko
'RO'	Rumunsko
'RSM'	San Marino
'RUS'	Ruská federace
'S'	Švédsko
'SK'	Slovensko
'SLO'	Slovinsko
'TM'	Turkmenistán
'TR'	Turecko
'UA'	Ukrajina
'V'	Vatikán
'YU'	Jugoslávie
'UNK'	neznámý
'EC'	Evropské společenství
'EUR'	zbytek Evropy
'WLD'	zbytek světa

2.72. NationNumeric

Číselné označení státu.

NationNumeric ::= INTEGER(0..255)

Přiřazení hodnoty:

-- žádné informace k dispozici	(00) H,
-- Rakousko	(01) H,
-- Albánie	(02) H,
-- Andorra	(03) H,
-- Arménie	(04) H,
-- Azerbájdžán	(05) H,
-- Belgie	(06) H,
-- Bulharsko	(07) H,
-- Bosna a Hercegovina	(08) H,
-- Bělorusko	(09) H,
-- Švýcarsko	(0A) H,
-- Kypr	(0B) H,
-- Česká republika	(0C) H,
-- Německo	(0D) H,
-- Dánsko	(0E) H,
-- Španělsko	(0F) H,
-- Estonsko	(10) H,
-- Francie	(11) H,
-- Finsko	(12) H,
-- Lichtenštejsko	(13) H,
-- Faerské ostrovy	(14) H,
-- Spojené království	(15) H,
-- Gruzie	(16) H,
-- Řecko	(17) H,

--	Maďarsko	(18) H,
--	Chorvatsko	(19) H,
--	Itálie	(1A) H,
--	Irsko	(1B) H,
--	Island	(1C) H,
--	Kazachstán	(1D) H,
--	Lucembursko	(1E) H,
--	Litva	(1F) H,
--	Lotyšsko	(20) H,
--	Malta	(21) H,
--	Monako	(22) H,
--	Moldávie	(23) H,
--	Makedonie	(24) H,
--	Norsko	(25) H,
--	Nizozemsko	(26) H,
--	Portugalsko	(27) H,
--	Polsko	(28) H,
--	Rumunsko	(29) H,
--	San Marino	(2A) H,
--	Ruská federace	(2B) H,
--	Švédsko	(2C) H,
--	Slovensko	(2D) H,
--	Slovinsko	(2E) H,
--	Turkmenistán	(2F) H,
--	Turecko	(30) H,
--	Ukrajina	(31) H,

--	Vatikán	(32) H,
--	Jugoslávie	(33) H,
--	RFU	(34..FC) H,
--	Evropské společenství	(FD) H,
--	zbytek Evropy	(FE) H,
--	zbytek světa	(FF) H

2.73. NoOfCalibrationRecords

Počet kalibračních záznamů, které může dílenská karta uložit.

NoOfCalibrationRecords ::= INTEGER(0..255)

Přiřazení hodnoty: viz odstavec 3.

2.74. NoOfCalibrationsSinceDownload

Čítač indikující počet kalibrací provedených s dílenskou kartou od posledního stahování dat z ní (požadavek 230).

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

Přiřazení hodnoty: není blíže specifikováno.

2.75. NoOfCardPlaceRecords

Počet záznamů místa, které mohou karta řidiče nebo dílenská karta uložit.

NoOfCardPlaceRecords ::= INTEGER(0..255)

Přiřazení hodnoty: viz odstavec 3.

2.76. NoOfCardVehicleRecords

Počet záznamů o použitých vozidlech, které karta řidiče nebo dílenská karta mohou uložit.

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

Přiřazení hodnoty: viz odstavec 3.

2.77. NoOfCompanyActivityRecords

Počet záznamů činnosti společnosti, které karta společnosti může uložit.

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

Přiřazení hodnoty: viz odstavec 3.

2.78. NoOfControlActivityRecords

Počet záznamů kontrol činnosti, které kontrolní karta může uložit.

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

Přiřazení hodnoty: viz odstavec 3.

2.79. NoOfEventsPerType

Počet událostí každého typu události, které karta může uložit.

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

Přiřazení hodnoty: viz odstavec 3.

2.80. NoOfFaultsPerType

Počet závad každého typu závady, které karta může uložit.

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

Přiřazení hodnoty: viz odstavec 3.

2.81. OdometerValueMidnight

Údaj měřiče ujeté vzdálenosti o půlnoci daného dne (požadavek 090).

`OdometerValueMidnight ::= OdometerShort`

Přiřazení hodnoty: není blíže specifikováno

2.82. OdometerShort

Údaj měřiče ujeté vzdálenosti vozidla ve zkrácené formě.

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

Přiřazení hodnoty: Binární číslo bez znaménka. Hodnota v km v provozním rozsahu 0 až 9 999 999 km.

2.83. OverspeedNumber

Počet událostí překročení rychlosti od poslední kontroly překročení rychlosti.

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

Přiřazení hodnoty: 0 znamená, že se nevyskytlo žádné překročení rychlosti od poslední kontroly překročení rychlosti, 1 znamená, že se vyskytla událost jednoho překročení rychlosti od poslední kontroly překročení rychlosti ... 255 znamená, že 255 nebo více událostí překročení rychlosti se vyskytlo od poslední kontroly překročení rychlosti.

2.84. PlaceRecord

Informace týkající se místa, kde denní pracovní doba začíná nebo končí (požadavky 087, 202, 221).

```
PlaceRecord ::= SEQUENCE {  
    EntryTime                TimeReal,  
    EntryTypeDailyWorkPeriod EntryTypeDailyWorkPeriod,  
    DailyWorkPeriodCountry   NationNumeric,  
    DailyWorkPeriodRegion    RegionNumeric,  
    VehicleOdometerValue     OdometerShort  
}
```

entryTime je datum a čas vztahující se ke vstupu.

entryTypeDailyWorkPeriod je typ vstupu.

dailyWorkPeriodCountry je vložený kraj.

dailyWorkPeriodRegion je vložený region.

vehicleOdometerValue je údaj měřiče ujeté vzdálenosti vztažený k času a vloženému místu.

2.85. PreviousVehicleInfo

Informace vztažená k vozidlu předtím použitým řidičem, když vkládal svoji kartu do celku ve vozidle (požadavek 081).

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

vehicleRegistrationIdentification je registrační číslo vozidla a členský stát registrující vozidlo.

cardWithdrawalTime je datum a čas vyjmutí karty.

2.86. PublicKey

Veřejný RSA klíč.

```
PublicKey ::= SEQUENCE {
```

```

RsaKeyModulus          RSAKeyModulus,
RsaKeyPublicExponent   RSAKeyPublicExponent
}

```

rsaKeyModulus je modul páru klíčů.

rsaKeyPublicExponent je veřejný činitel (exponent) páru klíčů.

2.87. RegionAlpha

Abecední odkaz na region uvnitř určitého státu.

RegionAlpha ::= IA5STRING(SIZE(3))

Přiřazení hodnoty:

‘ ’ žádné informace k dispozici

Španělsko:

‘AN’	Andalucia
‘AR’	Aragón
‘AST’	Asturias
‘C’	Cantabria
‘CAT’	Cataluña
‘CL’	Castilla-León
‘CM’	Castilla-La-Mancha
‘CV’	Valencia
‘EXT’	Extremadura
‘G’	Galicia
‘IB’	Baleares
‘IC’	Canarias
‘LR’	La Rioja
‘M’	Madrid
‘MU’	Murcia
‘NA’	Navarra

'PV' País Vasco.

2.88. RegionNumeric

Číselný odkaz na region uvnitř určitého státu.

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

Přiřazení hodnoty:

'00' H řádné informace k dispozici

Španělsko:

'01' H Andalucia

'02' H Aragón

'03' H Asturias

'04' H Cantabria

'05' H Cataluña

'06' H Castilla-León

'07' H Castilla-La-Mancha

'08' H Valencia

'09' H Extremadura

'0A' H Galicia

'0B' H Balears

'0C' H Canarias

'0D' H La Rioja

'0E' H Madrid

'0F' H Murcia

'10' H Navarra

'11' H País Vasco.

2.89. RSAKeyModulus

Modul RSA páru klíčů.

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

Přiřazení hodnoty: není specifikováno.

2.90. RSAKeyPrivateExponent

Soukromý činitel RSA páru klíčů.

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

Přiřazení hodnoty: není specifikováno.

2.91. RSAKeyPublicExponent

Veřejný činitel RSA páru klíčů.

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

Přiřazení hodnoty: není specifikováno.

2.92. SensorApprovalNumber

Číslo schválení snímače.

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

Přiřazení hodnoty: není specifikováno.

2.93. SensorIdentification

Informace uložená ve snímači pohybu a týkající se identifikace snímače pohybu (požadavek 077).

```
SensorIdentification ::= SEQUENCE {  
    SensorSerialNumber      SensorSerialNumber,  
    SensorApprovalNumber    SensorApprovalNumber,  
    SensorSCIdentifier       SensorSCIdentifier,  
    SensorOSIdentifier       SensorOSIdentifier  
}
```

sensorSerialNumber je rozšířené pořadové číslo snímače pohybu (obsahuje číslo dílu a kód výrobce).

sensorApprovalNumber je číslo schválení snímače pohybu.

sensorSCIdentifier je identifikátor spolehlivosti dílu snímače pohybu.

sensorOSIdentifier je identifikátor provozního systému snímače pohybu.

2.94. SensorInstallation

Informace uložená ve snímači pohybu týkající se instalace snímače pohybu (požadavek 099).

```
SensorInstallation ::= SEQUENCE {  
    SensorPairingDateFirst      SensorPairingDate,  
    FirstVuApprovalNumber      VuApprovalNumber,  
    FirstVuSerialNumber        VuSerialNumber,  
    SensorPairingDateCurrent    SensorPairingDate,  
    CurrentVuApprovalNumber     VuApprovalNumber,  
    CurrentVUSerialNumber       VuSerialNumber  
}
```

sensorPairingDateFirst je datum prvního spojení snímače pohybu s celkem ve vozidle.

firstVuApprovalNumber je číslo schválení prvního celku ve vozidle spojeného se snímačem pohybu.

firstVuSerialNumber je pořadové číslo prvního celku ve vozidle spojeného se snímačem pohybu.

sensorPairingDateCurrent je datum současného spojení snímače pohybu s celkem ve vozidle.

currentVuApprovalNumber je číslo schválení celku ve vozidle nyní spojeného se snímačem pohybu.

currentVUSerialNumber je pořadové číslo celku ve vozidle nyní spojeného se snímačem pohybu.

2.95. SensorInstallationSecData

Informace uložená na dílenské kartě týkající se dat spolehlivosti potřebných pro spojení snímačů pohybu s celky ve vozidlech (požadavek 214).

```
SensorInstallationSecData ::= TDesSessionKey
```

Přiřazení hodnoty: dle ISO 16844-3.

2.96. SensorOSIdentifier

Identifikátor provozního systému snímače pohybu.

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

Přiřazení hodnoty: týkající se výrobce.

2.97. SensorPaired

Informace uložená v celku ve vozidle týkající se identifikace snímače pohybu spojeného s celkem ve vozidle (požadavek 079).

```
SensorPaired ::= SEQUENCE {  
    SensorSerialNumber      SensorSerialNumber,  
    SensorApprovalNumber    SensorApprovalNumber,  
    SensorPairingDateFirst  SensorPairingDate  
}
```

sensorSerialNumber je pořadové číslo snímače pohybu nyní spojeného s celkem ve vozidle.

sensorApprovalNumber je číslo schválení snímače pohybu nyní spojeného s celkem ve vozidle.

SensorPairingDateFirst je datum prvního spojení s celkem ve vozidle nyní spojeného snímače pohybu s celkem ve vozidle.

2.98. SensorPairingDate

Datum spojení snímače pohybu s celkem ve vozidle.

```
SensorPairingDate ::= TimeReal
```

Přiřazení hodnoty: není specifikováno.

2.99. SensorSerialNumber

Pořadové číslo snímače pohybu.

```
SensorSerialNumber ::= ExtendedSerialNumber:
```

2.100. SensorSCIdentifier

Identifikátor spolehlivosti součásti snímače pohybu.

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

Přiřazení hodnoty: součást týkající se výrobce.

2.101. Signature

Digitální podpis.

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


Přiřazení hodnoty: v souladu s dodatkem 11, “Společný bezpečnostní mechanismus”.

2.102. SimilarEventsNumber

Počet podobných událostí během daného dne (požadavek 094).

SimilarEventsNumber ::= INTEGER(0..255)

Přiřazení hodnoty: 0 se nepoužije, 1 znamená, že se vyskytla pouze jedna událost toho typu a byla uložena toho dne, 2 znamená, že se vyskytly dvě události toho typu toho dne (pouze jedna byla uložena), 255 znamená, že 255 nebo více událostí toho typu se vyskytlo toho dne.

2.103. SpecificConditionType

Kód identifikující zvláštní podmínku (požadavky 050b, 105a, 212a a 230a).

SpecificConditionType ::= INTEGER(0..255)

Přiřazení hodnoty:

'00'H	RFU
'01'H	mimo rozsah platnosti - začátek
'02'H	mimo rozsah platnosti - konec
'03'H	cesta přes trajekt/vlak
'04'H .. 'FF'H	RFU.

2.104. SpecificConditionRecord

Informace uložená na kartě řidiče, dílenské kartě nebo v celku ve vozidle týkající se zvláštní podmínky (požadavky 105a, 212a a 230a).

```
SpecificConditionRecord ::= SEQUENCE {
    EntryTime                TimeReal,
    SpecificConditionType     SpecificConditionType
}
```

entryTime je datum a čas vstupu.

specificConditionType je kód identifikující zvláštní podmínku.

2.105. Speed

Rychlost vozidla (km/h).

Speed ::= INTEGER(0..255)

Přiřazení hodnoty: kilometry za hodinu v provozním rozsahu 0 až 220 km/h.

2.106. SpeedAuthorised

Maximální dovolená rychlost vozidla (definice bb)).

SpeedAuthorised ::= Speed.

2.107. SpeedAverage

Průměrná rychlost v dříve určené době trvání (km/h).

SpeedAverage ::= Speed.

2.108. SpeedMax

Nejvyšší rychlost v dříve určené době trvání.

SpeedMax ::= Speed.

2.109. TDesSessionKey

Triple-DES klíč zasedání.

```
TDesSessionKey ::= SEQUENCE {  
    TDesKeyA          OCTET STRING (SIZE(8))  
    TDesKeyB          OCTET STRING (SIZE(8))  
}
```

Přiřazení hodnoty: není blíže specifikováno.

2.110. TimeReal

Kód pro kombinovaný datum a časové pole, kde datum a čas jsou vyjádřeny jako sekundy 00h.00m.00s po 1.lednu 1970 času GMT.

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

Přiřazení hodnoty – osmibitové uspořádání: Počet sekund od půlnoci 1.ledna 1970, 0.00 hod času GMT.

Nejvyšší možný údaj datum/čas je v roce 2106.

2.111. TyreSize

Označení rozměrů pneumatik.

TyreSize ::= IA5String(SIZE(15))

Přiřazení hodnoty: podle směrnice 92/23 (EHS), 31.3.1992, Úřední věstník ES L 129, str. 95.

2.112. VehicleIdentificationNumber

Identifikační číslo vozidla (VIN) odkazující se na vozidlo jako celek, obvykle pořadové číslo karosérie nebo rámu.

```
VehicleIdentificationNumber ::= IA5String(SIZE(17))
```

Přiřazení hodnoty: jak je definováno v ISO 3779.

2.113. VehicleRegistrationIdentification

Jednoznačná identifikace vozidla pro Evropu (registrační číslo vozidla a členský stát).

```
VehicleRegistrationIdentification ::= SEQUENCE {  
    VehicleRegistrationNation      NationNumeric,  
    VehicleRegistrationNumber      VehicleRegistrationNumber  
}
```

vehicleRegistrationNation je stát, v kterém je vozidlo registrováno.

vehicleRegistrationNumber je registrační číslo vozidla (VRN).

2.114. VehicleRegistrationNumber

Registrační číslo vozidla (VRN). Registrační číslo vozidla je přiděleno orgánem registrujícím vozidlo.

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

codePage určuje část ISO/IEC 8859, která je použita ke kódování **vehicleRegNumber**,

vehicleRegNumber je registrační číslo vozidla kódované podle ISO/IEC 8859-codePage.

Přiřazení hodnoty: kód země.

2.115. VuActivityDailyData

Informace uložené v celku ve vozidle, související se změnami činnosti a/nebo změnami statusu řízení a/nebo změnami statusu karty pro daný kalendářní den (požadavek 084) a související se statusem slotů v 00.00 toho dne.

```
VuActivityDailyData ::= SEQUENCE {
```

```

        NoOfActivityChanges      INTEGER SIZE(0..1440),

        ActivityChangeInfos      SET  SIZE(noOfActivityChanges)  OF
                                ActivityChangeInfo

    }

```

noOfActivityChanges je počet ActivityChangeInfo slov v souboru activityChangeInfos.

activityChangeInfos je soubor ActivityChangeInfo slov, uložený v celku ve vozidle pro den. Vždy obsahuje dvě ActivityChangeInfo slova dávající status dvou slotů v 00.00 toho dne.

2.116. VuApprovalNumber

Číslo schválení typu celku ve vozidle.

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

Přiřazení hodnoty: není specifikováno.

2.117. VuCalibrationData

Informace uložené v celku ve vozidle týkající se kalibrací záznamového zařízení (požadavek 098).

```

VuCalibrationData ::= SEQUENCE {

    NoOfVuCalibrationRecords  INTEGER(0..255),

    VuCalibrationRecords      SET  SIZE(noOfVuCalibrationRecords)
                                OF VuCalibrationRecord

}

```

noOfVuCalibrationRecords je počet záznamů obsažených v souboru vuCalibrationRecords.

vuCalibrationRecords je soubor kalibračních záznamů.

2.118. VuCalibrationRecord

Informace uložené v celku ve vozidle týkající se kalibrace záznamového zařízení (požadavek 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 je účel kalibrace.

workshopName, workshopAddress jsou název dílny a adresa.

workshopCardNumber identifikuje dílenskou kartu použitou během kalibrace.

workshopCardExpiryDate je prošlé datum platnosti karty.

vehicleIdentificationNumber je identifikační číslo vozidla (VIN).

vehicleRegistrationIdentification obsahuje registrační číslo vozidla a registrující členský stát.

wVehicleCharacteristicConstant je charakteristický koeficient vozidla.

kConstantOfRecordingEquipment je konstanta záznamového zařízení.

LTyreCircumference je efektivní obvod pneumatik kol.

tyreSize je označení rozměrů pneumatik namontovaných na vozidle.

authorisedSpeed je dovolená rychlost vozidla.

oldOdometerValue, **newOdometerValue** jsou staré a nového údaje měřiče ujeté vzdálenosti.

oldTimeValue, **newTimeValue** jsou staré a nové hodnoty datumu a času.

nextCalibrationDate je datum příští kalibrace typu stanoveného v CalibrationPurpose, kterou provede oprávněný kontrolní orgán.

2.119. VuCardIWData

Informace uložené v celku ve vozidle týkající se cyklů vkládání a vyjímání karet řidiče nebo dílenských karet v celku ve vozidle (požadavek 081).

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

noOfIWRecords je počet záznamů v souboru vuCardIWRecords.

vuCardIWRecords je soubor záznamů týkajících se cyklů vkládání a vyjímání karty.

2.120. VuCardIWRecord

Informace uložené v celku ve vozidle týkající se cyklu vložení a vyjmutí karty řidiče nebo dílenské karty v celku ve vozidle (požadavek 081).

```
VuCardIWRecord ::= SEQUENCE {
    CardHolderName          HolderName,
    FullCardNumber          FullCardNumber,
    CardExpiryDate          TimeReal,
    CardInsertionTime       TimeReal,
    VehicleOdometerValueAtInsertion OdometerShort,
    CardSlotNumber          CardSlotNumber,
    CardWithdrawalTime      TimeReal,
    VehicleOdometerValueAtWithdrawal OdometerShort,
    PreviousVehicleInfo     PreviousVehicleInfo
    ManualInputFlag         ManualInputFlag
}
```

cardHolderName jsou příjmení a jméno držitele karty řidiče nebo dílenské karty ve tvaru, jak jsou uloženy na kartě.

fullCardNumber je typ karty vystavené členským státem a číslo karty ve tvaru, jak jsou uloženy na kartě.

cardExpiryDate je prošílé datum platnosti karty ve tvaru, jak jsou uloženy na kartě.

cardInsertionTime je datum a čas vložení karty.

vehicleOdometerValueAtInsertion je údaj měřiče ujeté vzdálenosti při vložení karty.

cardSlotNumber je slot, ve kterém je karta vložena.

cardWithdrawalTime je datum a čas vyjmutí karty.

vehicleOdometerValueAtWithdrawal je údaj měřiče ujeté vzdálenosti při vyjmutí karty.

previousVehicleInfo obsahuje informaci o předchozím použití vozidla řidičem ve tvaru, jak je uložena na kartě.

manualInputFlag je příznak udávající, zda držitel karty při jejím vložení manuálně vložil činnosti řidiče.

2.121. VuCertificate

Certifikát veřejného klíče celku ve vozidle.

`VuCertificate ::= Certificate`

2.122. VuCompanyLocksData

Informace uložené v celku ve vozidle týkající se zámků společnosti (požadavek 104).

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

noOfLocks je počet zámků uvedených v `vuCompanyLocksRecords`.

vuCompanyLocksRecords je soubor záznamů zámků společnosti.

2.123. VuCompanyLocksRecord

Informace uložená v celku ve vozidle týkající se jednoho zámku společnosti (požadavek 104).

```

VuCompanyLocksRecord ::= SEQUENCE {
    LockInTime                TimeReal,
    LockOutTime               TimeReal,
    CompanyName               Name,
    CompanyAddress            Address,
    CompanyCardNumber         FullCardNumber
}

```

lockInTime, lockOutTime jsou datum a čas zamčeného a odemčeného zámku.

companyName, companyAddress jsou název a adresa společnosti vztahující se k zamčenému zámku.

companyCardNumber identifikuje kartu použitou v zamčeném zámku.

2.124. VuControlActivityData

Informace uložené v celku ve vozidle týkající se kontrol vykonaných použitím tohoto celku ve vozidle (požadavek 102).

```

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

```

noOfControls je počet kontrol uvedených v vuControlActivityRecords.

vuControlActivityRecords je soubor záznamů kontrol činnosti.

2.125. VuControlActivityRecord

Informace uložené v celku ve vozidle týkající se kontroly vykonané použitím tohoto celku ve vozidle (požadavek 102).

```

VuControlActivityRecord ::= SEQUENCE {
    ControlType                ControlType,
    ControlTime                TimeReal,
    ControlCardNumber          FullCardNumber,
    DownloadPeriodBeginTime    TimeReal,
    DownloadPeriodEndTime      TimeReal
}

```


}

controlType je typ kontroly.

controlTime je datum a čas kontroly.

ControlCardNumber identifikuje kontrolní kartu použitou pro kontrolu.

downloadPeriodBeginTime je začátek doby stahování dat, v případě stahování dat.

downloadPeriodEndTime je konec doby stahování dat, v případě stahování dat.

2.126. VuDataBlockCounter

Čítač uložený na kartě, identifikující postupně cykly vkládání a vyjímání karty v celku ve vozidle.

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

Přiřazení hodnoty: Pořadové číslo s maximální hodnotou 9 999, začínající zase 0.

2.127. VuDetailedSpeedBlock

Informace uložené v celku ve vozidle týkající se přesné rychlosti vozidla během jedné minuty, v které se vozidlo pohybovalo (požadavek 093).

```
VuDetailedSpeedBlock ::= SEQUENCE {
    SpeedBlockBeginDate      TimeReal,
    SpeedsPerSecond          SEQUENCE SIZE(60) OF Speed
}
```

speedBlockBeginDate je datum a čas první hodnoty rychlosti uvnitř bloku.

speedsPerSecond je chronologická posloupnost měřených rychlostí každou sekundu během minuty začínající v **speedBlockBeginDate**.

2.128. VuDetailedSpeedData

Informace uložené v celku ve vozidle týkající se přesné rychlosti vozidla.

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

noOfSpeedBlocks je počet bloků rychlosti v souboru **vuDetailedSpeedBlocks**.

VuDetailedSpeedBlocks je soubor bloků přesné rychlosti.

2.129. VuDownloadablePeriod

Nejstarší a nejmladší datum pro které celek ve vozidle uchovává data týkající se činností řidičů (požadavky 081, 084 nebo 087).

```
VuDownloadablePeriod ::= SEQUENCE {
    MinDownloadableTime      TimeReal
    MaxDownloadableTime      TimeReal
}
```

minDownloadableTime je nejstarší vložení karty nebo změny činnosti nebo místo vstupu datumu a času uložených v celku ve vozidle.

maxDownloadableTime je nejmladší vyjmutí karty nebo změny činnosti nebo místo vstupu datumu a času uložených v celku ve vozidle.

2.130. VuDownloadActivityData

Informace uložené v celku ve vozidle týkající se jeho posledního stažení dat (požadavek 105).

```
VuDownloadActivityData ::= SEQUENCE {
    DownloadingTime          TimeReal,
    FullCardNumber           FullCardNumber,
    CompanyOrWorkshopName    Name
}
```

downloadingTime je datum a čas stažení dat.

fullCardNumber identifikuje kartu použitou ke schválení stažení dat.

companyOrWorkshopName je název společnosti nebo dílny.

2.131. VuEventData

Informace uložené v celku ve vozidle týkající se událostí (požadavek 094 kromě události překročení rychlosti).

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

noOfVuEvents je počet událostí uvedených v souboru vuEventRecords.

vuEventRecords je soubor záznamů událostí.

2.132. VuEventRecord

Informace uložené v celku ve vozidle týkající se události (požadavek 094 kromě události překročení rychlosti).

```
VuEventRecord ::= SEQUENCE {  
    EventType                      EventFaultType,  
    EventRecordPurpose             EventFaultRecordPurpose,  
    EventBeginTime                 TimeReal,  
    EventEndTime                   TimeReal,  
    CardNumberDriverSlotBegin      FullCardNumber,  
    CardNumberCodriverSlotBegin    FullCardNumber,  
    CardNumberDriverSlotEnd        FullCardNumber,  
    CardNumberCodriverSlotEnd      FullCardNumber,  
    SimilarEventsNumber            SimilarEventsNumber  
}
```

eventType je typ události.

eventRecordPurpose je účel, pro který byla tato událost zaznamenána.

eventBeginTime je datum a čas začátku události.

eventEndTime je datum a čas konce události.

cardNumberDriverSlotBegin identifikuje kartu vloženou do slotu řidiče v začátku události.

cardNumberCodriverSlotBegin identifikuje kartu vloženou do slotu druhého řidiče v začátku události.

cardNumberDriverSlotEnd identifikuje kartu vloženou do slotu řidiče na konci události.

cardNumberCodriverSlotEnd identifikuje kartu vloženou do slotu druhého řidiče na konci události.

similarEventsNumber je počet podobných událostí toho dne.

Tato posloupnost může být použita pro všechny události s výjimkou události překročení rychlosti.

2.133. VuFaultData

Informace uložené v celku ve vozidle týkající se závad (požadavek 096).

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

noOfVuFaults je počet závad uvedených v souboru vuFaultRecords,

vuFaultRecords je soubor záznamů závad.

2.134. VuFaultRecord

Informace uložené v celku ve vozidle týkající se závady (požadavek 096).

```
VuFaultRecord ::= SEQUENCE {
    FaultType                EventFaultType,
    FaultRecordPurpose       EventFaultRecordPurpose,
    FaultBeginTime           TimeReal,
    FaultEndTime             TimeReal,
    CardNumberDriverSlotBegin FullCardNumber,
    CardNumberCodriverSlotBegin FullCardNumber,
    CardNumberDriverSlotEnd   FullCardNumber,
    CardNumberCodriverSlotEnd FullCardNumber
}
```

faultType je typ závady záznamového zařízení.

faultRecordPurpose je účel, pro který byla tato závada zaznamenána.

faultBeginTime je datum a čas začátku závady.

faultEndTime je datum a čas konce závady.

cardNumberDriverSlotBegin identifikuje kartu vloženou do slotu řidiče v začátku závady.

cardNumberCodriverSlotBegin identifikuje kartu vloženou do slotu druhého řidiče v začátku závady.

cardNumberDriverSlotEnd identifikuje kartu vloženou do slotu řidiče na konci závady.

cardNumberCodriverSlotEnd identifikuje kartu vloženou do slotu druhého řidiče na konci závady.

2.135. VuIdentification

Informace uložené v celku ve vozidle týkající se identifikace celku ve vozidle (požadavek 075).

```
VuIdentification ::= SEQUENCE {  
    VuManufacturerName      VuManufacturerName,  
    VuManufacturerAddress    VuManufacturerAddress,  
    VuPartNumber             VuPartNumber,  
    VuSerialNumber           VuSerialNumber,  
    VuSoftwareIdentification  VuSoftwareIdentification,  
    VuManufacturingDate      VuManufacturingDate,  
    VuApprovalNumber         VuApprovalNumber  
}
```

vuManufacturerName je název výrobce celku ve vozidle.

vuManufacturerAddress je adresa výrobce celku ve vozidle.

vuPartNumber je číslo dílu celku ve vozidle.

vuSerialNumber je pořadové číslo celku ve vozidle.

vuSoftwareIdentification identifikuje software implementované do celku ve vozidle.

vuManufacturingDate je datum výroby celku ve vozidle.

vuApprovalNumber je číslo schválení typu celku ve vozidle.

2.136. VuManufacturerAddress

Adresa výrobce celku ve vozidle.

```
VuManufacturerAddress ::= Address
```

Přiřazení hodnoty: není specifikováno.

2.137. VuManufacturerName

Název výrobce celku ve vozidle.

VuManufacturerName ::= Name

Přiřazení hodnoty: není specifikováno.

2.138. VuManufacturingDate

Datum výroby celku ve vozidle.

VuManufacturingDate ::= TimeReal

Přiřazení hodnoty: není specifikováno.

2.139. VuOverSpeedingControlData

Informace uložené v celku ve vozidle týkající se událostí překročení rychlosti od poslední kontroly překročení rychlosti (požadavek 095).

```
VuOverSpeedingControlData ::= SEQUENCE {  
    LastOverspeedControlTime      TimeReal,  
    FirstOverspeedSince           TimeReal,  
    NumberOfOverspeedSince       OverspeedNumber  
}
```

lastOverspeedControlTime je datum a čas poslední kontroly překročení rychlosti.

firstOverspeedSince je datum a čas prvního překročení rychlosti po této kontrole překročení rychlosti.

numberOfOverspeedSince je počet událostí překročení rychlosti od poslední kontroly překročení rychlosti.

2.140. VuOverSpeedingEventData

Informace uložené v celku ve vozidle týkající se událostí překročení rychlosti (požadavek 094).

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

noOfVuOverSpeedingEvents je počet událostí uvedených v souboru **vuOverSpeedingEventRecords**.

vuOverSpeedingEventRecords je soubor záznamů událostí překročení rychlosti.

2.141. VuOverSpeedingEventRecord

Informace uložené v celku ve vozidle týkající se událostí překročení rychlosti (požadavek 094).

```
VuOverSpeedingEventRecord ::= SEQUENCE {
    EventType                      EventFaultType,
    EventRecordPurpose             EventFaultRecordPurpose,
    EventBeginTime                 TimeReal,
    EventEndTime                   TimeReal,
    MaxSpeedValue                  SpeedMax,
    AverageSpeedValue              SpeedAverage,
    CardNumberDriverSlotBegin      FullCardNumber,
    SimilarEventsNumber            SimilarEventsNumber
}
```

eventType je typ události.

eventRecordPurpose je účel, pro který byla tato událost zaznamenána.

eventBeginTime je datum a čas začátku události.

eventEndTime je datum a čas konce události.

maxSpeedValue je nejvyšší rychlost měřená během události.

averageSpeedValue je průměrná rychlost měřená během události.

cardNumberDriverSlotBegin identifikuje kartu vloženou do slotu řidiče na začátku události.

similarEventsNumber je počet podobných událostí během toho dne.

2.142. VuPartNumber

Číslo dílu celku ve vozidle.

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

Přiřazení hodnoty: týkající se výrobce.

2.143. VuPlaceDailyWorkPeriodData

Informace uložené v celku ve vozidle týkající se míst, kde řidiči začínají nebo končí denní pracovní doby (požadavek 087).

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

noOfPlaceRecords je počet záznamů uvedených v souboru vuPlaceDailyWorkPeriodRecords.

vuPlaceDailyWorkPeriodRecords je soubor záznamů vztahujících se k místu.

2.144. VuPlaceDailyWorkPeriodRecord

Informace uložené v celku ve vozidle týkající se místa, kde řidič začíná nebo končí denní pracovní dobu (požadavek 087).

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

fullCardNumber je typ karty řidiče, kartu vydávající členský stát a číslo karty.

placeRecord obsahuje informace týkající se vloženého místa.

2.145. VuPrivateKey

Soukromý klíč celku ve vozidle.

```
VuPrivateKey ::= RSAKeyPrivateExponent
```

2.146. VuPublicKey

Veřejný klíč celku ve vozidle.

```
VuPublicKey ::= PublicKey
```

2.147. VuSerialNumber

Pořadové číslo celku ve vozidle (požadavek 075).

```
VuSerialNumber ::= ExtendedSerialNumber
```


2.148. VuSoftInstallationDate

Datum instalace softwarové verze celku ve vozidle.

`VuSoftInstallationDate ::= TimeReal`

Přiřazení hodnoty: není specifikováno.

2.149. VuSoftwareIdentification

Informace uložená v celku ve vozidle týkající se instalovaného software.

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

vuSoftwareVersion je číslo verze software v celku ve vozidle.

vuSoftInstallationDate je datum instalace verze software.

2.150. VuSoftwareVersion

Číslo verze software celku ve vozidle.

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

Přiřazení hodnoty: není specifikováno.

2.151. VuSpecificConditionData

Informace uložené v celku ve vozidle týkající se zvláštních podmínek.

```
VuSpecificConditionData ::= SEQUENCE {
    NoOfSpecificConditionRecords INTEGER(0..216-1)
    SpecificConditionRecords     SET SIZE (noOfSpecificCondition
                                     Records) OF SpecificConditionRecord
}
```

noOfSpecificConditionRecords je počet záznamů uložených v souboru `specificConditionRecords`.

specificConditionRecords je soubor zvláštních podmínek týkajících se záznamů.

2.152. VuTimeAdjustmentData

Informace uložené v celku ve vozidle týkající se nastavení času mimo normální kalibraci (požadavek 101).

```

VuTimeAdjustmentData ::= SEQUENCE {
    NoOfVuTimeAdjRecords      INTEGER(0..6),
    VuTimeAdjustmentRecords   SET  SIZE(noOfVuTimeAdjRecords)  OF
                                VuTimeAdjustmentRecords
}

```

noOfVuTimeAdjRecords je počet záznamů v **vuTimeAdjustmentRecords**.

vuTimeAdjustmentRecords je soubor záznamů nastavení času.

2.153. VuTimeAdjustmentRecord

Informace uložené v celku ve vozidle týkající se nastavení času mimo normální kalibraci (požadavek 101).

```

VuTimeAdjustmentRecord ::= SEQUENCE {
    OldTimeValue              TimeReal,
    OldTimeValue              TimeReal,
    NewTimeValue              TimeReal,
    WorkshopName              Name,
    WorkshopAddress           Address,
    WorkshopCardNumber        FullCardNumber
}

```

oldTimeValue, **newTimeValue** jsou staré a nové hodnoty datumu a času.

workshopName, **workshopAddress** jsou název dílny a adresa.

workshopCardNumber identifikuje kartu dílny použitou k nastavení času.

2.154. W-VehicleCharacteristicConstant

Charakteristický koeficient vozidla (definice k).

```

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

```

Přiřazení hodnoty: Impulzy na kilometr v provozním rozsahu 0 až 64 255 impulz/km.

2.155. WorkshopCardApplicationIdentification

Informace uložené na dílenské kartě, které se týkají identifikace použití karty (požadavek 190).

```

WorkshopCardApplicationIdentification ::= SEQUENCE {

```

```

    TypeOfTachographCardId      EquipmentType,
    CardStructureVersion         CardStructureVersion,
    NoOfEventsPerType            NoOfEventsPerType,
    NoOfFaultsPerType            NoOfFaultsPerType,
    ActivityStructureLength       CardActivityLengthRange,
    NoOfCardVehicleRecords        NoOfCardVehicleRecords,
    NoOfCardPlaceRecords          NoOfCardPlaceRecords,
    NoOfCalibrationRecords        NoOfCalibrationRecords
}

```

typeOfTachographCardId udává typ implementované karty.

cardStructureVersion udává verzi struktury implementované v kartě.

noOfEventsPerType je počet událostí každého druhu události, které mohou být na kartu uloženy.

noOfFaultsPerType je počet závad každého druhu závady, které mohou být na kartu uloženy.

activityStructureLength udává počet bytů, které jsou k dispozici pro uložení záznamů činnosti.

noOfCardVehicleRecords je počet záznamů vozidla, které může karta obsahovat.

noOfCardPlaceRecords je počet míst, které může karta zaznamenat.

noOfCalibrationRecords je počet záznamů kalibrace, které může karta uložit.

2.156. WorkshopCardCalibrationData

Informace uložené na dílenské kartě týkající se činnosti dílny, která byla provedena s kartou (požadavky 227 a 229).

```

WorkshopCardCalibrationData ::= SEQUENCE {
    CalibrationTotalNumber    INTEGER(0..216-1),
    CalibrationPointerNewestRecord
                                INTEGER(0..NoOfCalibrationRecords-1),
    CalibrationRecords         SET SIZE(NoOfCalibrationRecords) OF
                                WorkshopCardCalibrationRecord
}

```

calibrationTotalNumber je celkový počet kalibrací provedených s kartou.

calibrationPointerNewestRecord je index posledního aktualizovaného záznamu kalibrace.

Přiřazení hodnoty: Číslo odpovídající čítači záznamů kalibrace, začínající "0" pro první výskyt záznamu kalibrace ve struktuře.

calibrationRecords je soubor záznamů obsahujících kalibraci a/nebo informace o nastavení času.

2.157. WorkshopCardCalibrationRecord

Informace uložené na dílenské kartě týkající se kalibrace, která byla provedena s kartou (požadavek 227).

```
WorkshopCardCalibrationRecord ::= SEQUENCE {
    CalibrationPurpose           CalibrationPurpose,
    VehicleIdentificationNumber   VehicleIdentificationNumber,
    VehicleRegistration           VehicleRegistration
                                Identification,
    WVehicleCharacteristicConstant W-VehicleCharacteristic
                                Constant,
    KConstantOfRecordingEquipment K-ConstantOfRecording
                                Equipment,
    LTyreCircumference           L-TyreCircumference,
    TyreSize                     TyreSize,
    AuthorisedSpeed              SpeedAuthorised,
    OldOdometerValue             OdometerShort,
    NewOdometerValue             OdometerShort,
    OldTimeValue                 TimeReal,
    NewTimeValue                 TimeReal,
    NextCalibrationDate          TimeReal,
    VuPartNumber                 VuPartNumber,
    VuSerialNumber               VuSerialNumber,
    SensorSerialNumber           SensorSerialNumber
}
```

calibrationPurpose je účel kalibrace.

vehicleIdentificationNumber je identifikační číslo vozidla (VIN).

vehicleRegistration obsahuje registrační číslo vozidla (VRN) a registrující členský stát.

wVehicleCharacteristicConstant je charakteristický koeficient vozidla.

kConstantOfRecordingEquipment je konstanta záznamového zařízení.

ITyreCircumference je efektivní obvod pneumatiky kol.

tyreSize je označení rozměrů pneumatik montovaných na vozidlo.

authorisedSpeed je maximální dovolená rychlost vozidla.

oldOdometerValue, **newOdometerValue** jsou staré a nové hodnoty měřiče ujeté vzdálenosti.

oldTimeValue, **newTimeValue** jsou staré a nové hodnoty datumu a času.

nextCalibrationDate je datum příští kalibrace typu určeného v CalibrationPurpose, provedené pověřeným kontrolním orgánem.

vuPartNumber, **vuSerialNumber** and **sensorSerialNumber** jsou prvky dat pro identifikaci záznamového zařízení.

2.158. WorkshopCardHolderIdentification

Informace uložené na dílenské kartě týkající se identifikace držitele karty (požadavek 216).

```
WorkshopCardHolderIdentification ::= SEQUENCE {  
    WorkshopName                Name,  
    WorkshopAddress             Address,  
    CardHolderName              HolderName,  
    CardHolderPreferredLanguage Language  
}
```

workshopName je název dílny držitele karty.

workshopAddress je adresa dílny držitele karty.

cardHolderName je příjmení a jméno držitele (např. jméno mechanika).

cardHolderPreferredLanguage je mateřský jazyk držitele karty.

2.159. WorkshopCardPIN

Osobní identifikační číslo dílenské karty (požadavek 213).

WorkshopCardPIN ::= IA5String(SIZE(8))

Přiřazení hodnoty: Osobní identifikační číslo (PIN) známé držiteli karty, vpravo vyplněné “FF” byty do 8 bytů.

3. DEFINICE ROZSAHU HODNOTY A VELIKOSTI

Definice proměnných hodnot použitých pro definice v odstavci 2.

TimeRealRange ::= $2^{32} - 1$

3.1. Definice pro kartu řidiče:

Jméno proměnné hodnoty	min.	max.
CardActivityLengthRange	5 544 byte (28 dní 93 změn činnosti za den)	5 544 byte (28 dní 93 změn činnosti za den)
NoOfCardPlaceRecords	84	112
NoOfCardVehicleRecords	84	200
NoOfEventsPerType	6	12
NoOfFaultsPerType	12	24

3.2. Definice pro dílenskou kartu:

Jméno proměnné hodnoty	min.	max.
CardActivityLengthRange	198 byte (1 den 93 změn činnosti za den)	492 byte (1 den 240 změn činnosti za den)
NoOfCardPlaceRecords	6	8
NoOfCardVehicleRecords	4	8
NoOfEventsPerType	3	3
NoOfFaultsPerType	6	6
NoOfCalibrationRecords	88	255

3.3. Definice pro kontrolní kartu:

Jméno proměnné hodnoty	min.	max.
NoOfControlActivityRecords	230	520

3.4. Definice pro kartu společnosti:

Jméno proměnné hodnoty	min.	max.
NoOfCompanyActivityRecords	230	520

4. SOUBORY ZNAKŮ

V IA5Strings jsou použity ASCII znaky dle definice v ISO/IEC 8824-1. Pro čitelnost a snadný odkaz je přiřazení hodnoty uvedeno dále. V případě nesrovnalostí norma ISO/IEC 8824-1 nahrazuje tuto informativní poznámku.

! " # \$ % & ' () * + , - . / 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 { | } p

Jiné řetězce znaků (adresa, jméno, registrační číslo vozidla) používají navíc znaky, které jsou definovány kódy 192 až 255 normy ISO/IEC 8859-1 (soubor znaků Latin 1) nebo normy ISO/IEC 8859-7 (řecký soubor znaků).

5. KÓDOVÁNÍ

Při kódování dle ASN.1 musí být všechny typy dat kódovány podle ISO/IEC 8825-2.

DODATEK 2

SPECIFIKACE KARET TACHOGRAFU

OBSAH

SPECIFIKACE KARET TACHOGRAFU	145
1. ÚVOD	147
1.1. Zkratky	147
1.2. Odkazy	148
2. ELEKTRICKÉ A FYZIKÁLNÍ VLASTNOSTI	149
2.1. Napájecí napětí a spotřeba proudu	149
2.2. Programovací napětí U_{pp}	149
2.3. Generátor hodinových impulzů a frekvence	149
2.4. Kontakt vstup/výstup (I/O)	150
2.5. Stavy karty	150
3. HARDWARE A PŘENOS DAT	150
3.1. Úvod	150
3.2. Protokol přenosu	150
3.2.1. Protokoly	151
3.2.2. ATR	152
3.2.3. PTS	152
3.3. Podmínky přístupu (AC)	153
3.4. Kódování dat	154
3.5. Příkazy a kódy chyb - přehled	154
3.6. Popis příkazů	156
3.6.1. Select File	156
3.6.1.1. Výběr podle názvu (AID)	156
3.6.1.2. Výběr elementárního souboru na základě jeho identifikátoru souboru	157
3.6.2. Read Binary	158
3.6.2.1. Příkaz bez Secure Massaging	158
3.6.2.2. Příkaz s Secure Messaging	159
3.6.3. Update Binary	162
3.6.3.1. Příkaz bez Secure Messaging	162
3.6.3.2. Příkaz s Secure Messaging	163
3.6.4. Get Challenge	165

3.6.5.	Verify	165
3.6.6.	Get Response	166
3.6.7.	PSO: Verify Certificate.....	167
3.6.8.	Internal Authenticate	168
3.6.9.	External Authenticate	170
3.6.10.	Manage Security Environment	171
3.6.11.	PSO: Hash.....	172
3.6.12.	Perform Hash of File	173
3.6.13.	PSO: Compute Digital Signature	174
3.6.14.	PSO: Verify Digital Signature	174
4.	STRUKTURA KARET TACHOGRAFU.....	176
4.1.	Struktura karty řidiče	176
4.2.	Struktura dílenské karty	179
4.3.	Struktura kontrolní karty.....	183
4.4.	Struktura karty společnosti	185

1. ÚVOD

1.1. Zkratky

Pro účely tohoto dodatku platí následující zkratky:

AC	access conditions (podmínky přístupu)
AID	application identifier (identifikátor aplikace)
ALW	always (vždy)
APDU	application protocol data unit (struktura příkazu)
ATR	answer to reset (odpověď na reset)
AUT	authenticated (prokázaný)
C6, C7	kontakty č.6 a 7 karty, jak se uvedeno v normě ISO/IEC 7816-2
cc	clock cycles (hodinové impulzy)
CHV	card holder verification information (informace k ověření držitele karty)
CLA	class byte of an APDU command (byte třídy příkazu APDU)
DF	dedicated file (soubor). DF může obsahovat jiné soubory (EF nebo DF)
EF	elementary file (elementární soubor dat)
ENC	encrypted: access is possible only by encoding data (zakódovaný: přístup je možný pouze kódováním dat)
etu	elementary time unit (základní časová jednotka)
IC	integrated circuit (integrovaný obvod)
ICC	integrated circuit card (karta s integrovaným obvodem – čipová karta)
ID	identifier (identifikátor)
IFD	interface device (zařízení rozhraní, terminál karty)
IFS	information field size (velikost informačního pole)
IFSC	information field size for the card (velikost informačního pole karty)
IFSD	information field size device (velikost informačního pole terminálu)
INS	instruction byte of an APDU command (příkazový byte APDU příkazu)

Lc	length of the input data for a APDU command (délka vstupních dat pro APDU příkaz)
Le	length of the expected data (délka očekávaných dat, výstupní data pro jeden příkaz)
MF	master file (kořen DF)
P1-P2	parameter bytes (byty proměnné)
NAD	node address used in T=1 protocol (uzlová adresa použitá v protokole T = 1)
NEV	never (nikdy)
PIN	personal identification number (osobní identifikační číslo)
PRO SM	protected with secure messaging (chráněno Secure Messaging)
PTS	protocol transmission selection (výběr protokolu přenosu)
RFU	reserved for future use (vyhrazeno pro budoucí použití)
RST	reset (reset karty)
SM	secure messaging (Secure Messaging)
SW1-SW2	status bytes (stavové byty)
TS	initial ATR character (počáteční ATR znak)
VPP	programming voltage (programovací napětí)
XXh	value XX in hexadecimal notation (hodnota XX v hexadecimální notaci)
	concatenation symbol 03 04=0304 (symbol zřetězení).

1.2. Odkazy

V tomto dodatku jsou odkazy na následující normy:

EN 726-3	Systémy s identifikačními kartami – Telekomunikační karty s integrovanými obvody a koncová zařízení – Část 3: Aplikačně nezávislé požadavky na karty. Prosinec 1994
ISO/IEC 7816-2	Informační technika – Identifikační karty – Karty s integrovanými obvody a s kontakty – Část 2: Rozměry a umístění kontaktů. První vydání: 1999.
ISO/IEC 7816-3	Informační technika – Identifikační karty – Karty s integrovanými obvody a s kontakty – Část 3: Elektronické signály a protokoly přenosu. Druhé vydání: 1997.

- ISO/IEC 7816-4 Informační technika – Identifikační karty – Karty s integrovanými obvody a s kontakty – Část 4: Mezioborové příkazy pro výměnu. První vydání: 1995 + Změna 1: 1997.
- ISO/IEC 7816-6 Informační technika – Identifikační karty – Karty s integrovanými obvody a s kontakty – Část 6: Mezioborové prvky dat. První vydání: 1996 + Korigendum 1: 1998.
- ISO/IEC 7816-8 Informační technika – Identifikační karty – Karty s integrovanými obvody a s kontakty – Část 8: Bezpečnost mezioborových příkazů. První vydání: 1999.
- ISO/IEC 9797 Informační technika – Bezpečnostní postupy – Mechanismus úplnosti dat používající kódované kontrolní funkce zaměstnávající blokový šifrový algoritmus. Druhé vydání: 1997.

2. ELEKTRICKÉ A FYZIKÁLNÍ VLASTNOSTI

TCS_200 Všechny elektronické signály musí být v souladu s normou ISO/IEC 7816-3, pokud nejsou specifikovány jinak.

TCS_201 Umístění a rozměry kontaktů karty musí splňovat normu ISO/IEC 7816-2.

2.1. Napájecí napětí a spotřeba proudu

TCS_202 Karta pracuje podle specifikace uvnitř hranic spotřeby dle ISO/IEC 7816-3.

TCS_203 Karta pracuje při $U_{cc} = 3 \text{ V}$ (+/- 0,3 V) nebo při $U_{cc} = 5 \text{ V}$ (+/- 0,5 V).

Volba napětí se provede v souladu s ISO/IEC 7816-3.

2.2. Programovací napětí U_{pp}

TCS_204 Karta nevyžaduje na kontaktu C6 programovací napětí. Předpokládá se, že kontakt C6 není spojen s rozhraním (IFD). Kontakt C6 může být spojen s napětím U_{cc} , nesmí být ale ukostřen. Toto napětí nesmí být v žádném případě interpretováno.

2.3. Generátor hodinových impulsů a frekvence

TCS_205 Karta pracuje s frekvenčním rozsahem 1 až 5 MHz. Během jedné operace karty se může hodinová frekvence měnit $\pm 2 \%$. Hodinová frekvence je generována celkem ve vozidle, ne kartou. Pracovní cyklus se může měnit mezi 40 a 60 %.

TCS_206 Za podmínek obsažených v souboru EF_{ICC} karty mohou být externí hodiny zastaveny. První byte těla souboru EF_{ICC} kóduje podmínky módu Clockstop (další podrobnosti viz norma EN 726-3):

L-úroveň	H-úroveň	
----------	----------	--

Bit 3	Bit 2	Bit 1	
0	0	1	Zastavení hodin dovoleno, žádná preferovaná úroveň
0	1	1	Zastavení hodin dovoleno, preferována H-úroveň
1	0	1	Zastavení hodin dovoleno, preferována L-úroveň
0	0	0	Zastavení hodin není dovoleno
0	1	0	Zastavení hodin dovoleno pouze při H-úrovni
1	0	0	Zastavení hodin dovoleno pouze při L-úrovni

Bity 4 až 8 nejsou použity.

2.4. Kontakt vstup/výstup (I/O)

TCS_207 I/O kontakt C7 je použit pro příjem dat z rozhraní a pro vysílání dat na zařízení rozhraní (IFD). Během provozu se nachází ve vysílacím módu buď karta nebo zařízení rozhraní. Budou-li obě jednotky ve vysílacím módu, nesmí tím být karta poškozena. Pokud karta nevysílá, musí nastoupit přijímací mód.

2.5. Stavy karty

TCS_208 Při napájecím napětí pracuje karta ve dvou módech:

- provozní stav během vykonávání příkazů nebo během propojení s digitální jednotkou,
- klidový stav v ostatním čase: v tomto stavu musejí být všechna data na kartě zachována.

3. HARDWARE A PŘENOS DAT

3.1. Úvod

Tento odstavec popisuje nutnou funkčnost požadovanou kartami tachografu a celkem ve vozidle k zajištění správného provozu a součinnosti.

Karty tachografu splňují pokud možno co nejvíce normy ISO/IEC (především normu ISO/IEC 7816). Příkazy a protokoly jsou plně popsány, aby specifikovaly omezené použití nebo některé rozdíly, pokud existují. Určené příkazy plně odpovídají uvedeným normám, pokud není uvedeno jinak.

3.2. Protokol přenosu

TCS_300 Protokol přenosu odpovídá normě ISO/IEC 7816-3. Především celek ve vozidle musí rozeznat prodloužení čekací doby odeslané kartou.

3.2.1. Protokoly

TCS_301 Karta podporuje jak protokol T=0 tak protokol T=1.

TCS_302 T=0 je standardní protokol, pro změnu na protokol T=1 je nutný příkaz PTS.

TCS_303 Zařízení podporují v obou protokolech 'direct convention', která je proto pro kartu povinná.

TCS_304 Byte pro velikost informačního pole karty bude uveden v ATR ve znaku TA3. Tato hodnota činí nejméně 'F0h' (= 240 bytů).

Pro protokoly platí následující omezení:

TCS_305 T=0

- Zařízení rozhraní podporuje odpověď při I/O na náběžnou hranu signálu RST od 400 cc.
- Zařízení rozhraní musí být schopno číst znaky oddělené 12 etu.
- Zařízení rozhraní čte chybný znak a jeho opakování, jestliže je oddělen 13 etu. Jestliže je chybný znak detekován, objeví se na I/O chybový signál mezi 1 etu a 2 etu. Zařízení podporuje zpoždění od 1 etu.
- Zařízení rozhraní akceptuje ATR 33 bytů (TS+32)
- Jestliže se TC1 nachází v ATR, je Extra Guard Time k dispozici pro znaky poslané zařízením rozhraní, ačkoliv znaky poslané kartou mohou být odděleny 12 etu. To také platí pro ACK znak poslaný kartou po vyslání znaku P3 zařízením rozhraní.
- Zařízení rozhraní bere v úvahu znak NUL vyslaný kartou.
- Zařízení rozhraní akceptuje komplementární mód pro ACK.
- Příkaz GET RESPONSE nemůže být použit v módu řetězení k získání dat, jejichž délka by mohla přesáhnout 255 bytů.

TCS_306 T=1

- NAD byte: nepoužívaný (NAD je nastaven na '00').
- S-block ABORT: nepoužívaný.
- S-block VPP- stav chyby: nepoužívaný.
- Celková délka zřetězení pro pole dat nepřesáhne 255 bytů (zajištěno IFD).

- Velikost informačního pole terminálu (IFSD) je indikována IFD ihned po ATR: zařízení rozhraní přenáší S-Block IFS požadavek po ATR a karta posílá S-Block IFS zpět. Doporučená hodnota pro IFSD je 254 bytů.
- Karta nevyžaduje na IFS nové seřízení.

3.2.2. ATR

TCS_307 Zařízení kontroluje ATR byty podle normy ISO/IEC 7816-3. Nenasleduje kontrola historických ATR znaků.

Příklad základního dvojitého protokolu ATR podle normy ISO/IEC 7816-3

Znak	hodnota	poznámky
TS	'3Bh'	Indikátor pro 'direct convention'
T0	'85h'	TD1 k dispozici: 5 historických bytů k dispozici
TD1	'80h'	TD2 k dispozici: T=0 použito
TD2	'11h'	TD3 k dispozici: T=1 použito
TA3	'XXh'(min.'F0h')	Velikost informačního pole karty (IFSC)
TH1 až TH5	'XXh'	Historické znaky
TCK	'XXh'	Kontrolní znak (kromě OR)

TCS_308 Po odpovědi na reset (ATR) je hlavní soubor (MF) implicitně vybrán a stává se aktuálním adresářem.

3.2.3. PTS

TCS_309 Standardní protokol je T=0. Pro nastavení protokolu T=1 musí být zařízením posláno PTS (také známé jako PPS) na kartu.

TCS_310 Poněvadž protokoly T=0 i T=1 jsou pro kartu povinné, základní PTS pro přepínání protokolů je pro kartu povinný.

Jak je uvedeno v normě ISO/IEC 7816-3, může PTS být použit pro přepínání na vyšší přenosový rozsah než standardní, při kterém je při přenosu z karty do ATR použita navržená rychlost přenosu (TA(1) byte).

Vyšší přenosový rozsah je pro kartu volitelný.

TCS_311 Jestliže žádný jiný přenosový rozsah než standardní rychlost přenosu nejsou podporovány (nebo zvolený přenosový rozsah není podporován), odpovídá karta na PTS přesně podle normy ISO/IEC 7816-3 vynecháním PPS1 byte.

Příklady základního PTS pro výběr protokolu:

znak	hodnota	poznámky
------	---------	----------

PPSS	'FFh'	Znak zahájení
PPS0	'00h' nebo '01h'	PPS1 až PPS3 nejsou k dispozici: '00h' k výběru T0, '01h' k výběru T1
PK	'XXh'	Kontrolní znak: 'XXh' = 'FFh' jestliže PPS0 = '00h' 'XXh' = 'FEh' jestliže PPS0 = '01h'

3.3. Podmínky přístupu (AC)

Podmínky přístupu pro příkazy UPDATE_BINARY a READ_BINARY jsou definovány pro každý elementární soubor.

TCS_312 Před přístupem k aktuálním datům musí být splněny podmínky AC.

Definice podmínek přístupu jsou tyto:

- ALW: Akce je vždy možná a může být provedena bez omezení.
- NEV: Akce není nikdy možná.
- AUT: Právo přístupu odpovídající úspěšnému externímu prokázání totožnosti musí být otevřené (provede se příkazem EXTERNAL_AUTHENTICATE).
- PRO SM: Příkaz musí být přenesen s kryptografickým kontrolním součtem při použití Secure Messaging (viz příloha 11).
- AUT a PRO SM (kombinovaný)

S příkazy pro zpracování (UPDATE_BINARY a READ_BINARY) mohou být stanoveny na kartě následující podmínky přenosu:

	UPDATE BINARY	READ BINARY
ALW	ano	ano
NEV	ano	ano
AUT	ano	ano
PRO SM	ano	ne
AUT a PRO SM	ano	ne

Podmínky přístupu PRO SM nejsou k dispozici pro příkaz READ_BINARY. To znamená, že přítomnost kryptografického kontrolního součtu pro příkaz READ není povinná. Při použití hodnoty '0C' pro třídu je možné použít příkaz READ BINARY s Secure Messaging, jak je uvedeno v odstavci 3.6.2.

3.4. Kódování dat

Jestliže utajení dat musí být ochráněno proti jejich přečtení ze souboru dat, soubor je označen jako 'zakódovaný'. Kódování se provádí použitím 'Secure Messaging (viz dodatek 11).

3.5. Příkazy a kódy chyb - přehled

Příkazy a organizace souborů dat jsou odvozeny od normy ISO/IEC 7816-4 a tuto normu splňují.

TCS_313 Tento odstavec popisuje následující APDU páry příkaz-odezva:

příkaz	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 ENVIROMENT: SETTING A KEY	22
PERFORM HASH OF FILE	2A

TCS_314 V každé zprávě odezvy jsou poslány zpět stavové byty SW1 a SW2, které stav zpracování příkazů označí.

SW1	SW2	Význam
90	00	Normální zpracování
61	XX	Normální zpracování. XX = počet platných bytů odezvy
62	81	Zpracování výstrahy. Část vrácených dat může být poškozena
63	CX	Chybný CHV (PIN). Čítač zbývajících pokusů 'X'
64	00	Chyba provedení – stav stálé paměti nezměněn. Chyba integrity
65	00	Chyba provedení – stav stálé paměti změněn
65	81	Chyba provedení – stav stálé paměti změněn – porucha paměti
66	88	Chyba bezpečnosti: chybný kryptografický kontrolní součet (během Secure Messaging) nebo chybný certifikát (během ověření certifikátu) nebo chybný kryptogram (během externího ověřování pravosti) nebo chybný podpis (během ověřování podpisu)
67	00	Chybná délka (chybná Lc nebo Le)
69	00	Zakázaný příkaz (žádná dostupná odezva v T = 0)
69	82	Status bezpečnosti nesplněn
69	83	Metoda ověřování pravosti zablokována
69	85	Podmínky použití nesplněny
69	86	Nedovolený příkaz (žádné aktuální EF)
69	87	Očekávané Secure Messaging datové objekty chybí
69	88	Nesprávné Secure Messaging datové objekty
6A	82	Datové soubory nenalezeny
6A	86	Chybné parametry P1 – P2
6A	88	Referenční data nenalezena
6B	00	Chybné parametry (offset mimo EF)
6C	XX	Chybná délka, SW2 udává přesnou délku. Žádné datové pole není vráceno
6D	00	Kód příkazu není podporován nebo je neplatný
6E	00	Třída není podporována
6F	00	Jiné kontrolní chyby

3.6. Popis příkazů

Povinné příkazy pro karty tachografu jsou popsány v této kapitole.

Další účelné podrobnosti vztahující se ke kryptografickým operacím jsou v příloze 11, společný bezpečnostní mechanismus.

Všechny příkazy jsou popsány nezávisle na použití protokolu (T=0 nebo T=1). APDU byty CLA, INS, P1, P2, Lc a Le jsou vždy indikovány. Jestliže Lc a Le nejsou potřebné pro popisovaný příkaz, odpovídající délka, hodnota a popis zůstanou prázdné.

TCS_315 Jestliže délka obou bytů (Lc a Le) odpovídá požadované, popisovaný příkaz se rozdělí na dvě části, jestliže zařízení rozhraní (IFD) použije protokol T=0: pokud IFD pošle příkaz jak je popsáno s P3=Lc + data a pošle potom příkaz GET_RESPONSE (viz odst. 3.6.6.) s P3=Le.

TCS_316 Jestliže délka obou bytů odpovídá požadované, a Le=0 (Secure Messaging), potom platí:

- Při použití protokolu T=1 odpovídá karta na Le=0 vysláním všech dostupných dat.
- Při použití protokolu T=0 vyšle IFD první příkaz s P3=Lc + data a karta odpoví (na implicitní Le=0) stavovým bytem 61La', kde La je počet dostupných bytů odezvy. IFD potom generuje příkaz GET RESPONSE s P3=La pro čtení dat.

3.6.1. Select File

Tento příkaz odpovídá ustanovením ISO/IEC 7816-4, jeho použití je ale ve srovnání s příkazem definovaným normou omezeno.

Příkaz SELECT FILE je použit:

- k výběru aplikace DF (musí být použit výběr podle názvu)
- k výběru elementárního souboru dat odpovídajícího předloženému souboru ID.

3.6.1.1. Výběr podle názvu (AID)

Tento příkaz dovoluje výběr aplikace DF na kartě.

TCS_317 Tento příkaz může být vykonán z libovolného místa v datové struktuře (po ATR nebo kdykoliv).

TCS_318 Výběr aplikace obnovuje současné bezpečnostní prostředí. Po provedení výběru aplikace není již vybrán žádný současný veřejný klíč a dřívější klíč relace není již dále vhodný pro Secure Messaging. Podmínka přístupu AUT je rovněž ztracena.

TCS_319 Příkazová zpráva

byte	délka	hodnota	popis
CLA	1	'00h'	
INS	1	'A4h'	
P1	1	'04h'	výběr podle názvu (AID)
P2	1	0Ch'	neočekává se žádná odezva
Lc	1	'NNh'	počet bytů odeslaných na kartu (délka AID): '06h' pro aplikaci tachografu
#6-#(5+NN)	NN	'XX...XXh'	AID: 'FF 54 41 43 48 4F' pro aplikaci tachografu

Nevyžaduje se žádná odezva na příkaz SELECT FILE (Le chybí v T=1 nebo se nepožaduje odezva v T=0).

TCS_320 Zpráva o odezvě (nepožaduje se žádná odezva)

Byte	délka	hodnota	popis
SW	2	'XXXXh'	stavová slova (SW1, SW2)

- Pokud je příkaz úspěšný, vrací karta zpět '9000',
- pokud aplikace odpovídající AID není nalezena, zpět poslaný status zpracování je '6A82',
- při T=1 a pokud je Le byte přítomen, zpět posílaný status je '6700',
- při T=0 a pokud je vyžadována odezva po příkazu SELECT FILE, zpět posílaný status je '6900',
- jestliže vybraná aplikace je považována za poškozenou (je detekována chyba integrity uvnitř souboru atributů), zpět poslaný status je '6400' nebo '6581'.

3.6.1.2. Výběr elementárního souboru na základě jeho identifikátoru souboru

TCS_321 Příkazová zpráva

byte	délka	hodnota	popis
CLA	1	'00h'	
INS	1	'A4h'	
P1	1	'02h'	výběr EF při aktuálním DF
P2	1	'0Ch'	neočekává se žádná odezva
Lc	1	'02h'	počet bytů odeslaných na kartu
#6-#7	2	'XXXXh'	identifikátor souboru

Nevyžaduje se žádná odezva na příkaz SELECT FILE (Le chybí v T=1 nebo se nepožaduje odezva v T=0).

TCS_322 Zpráva o odezvě (nepožaduje se žádná odezva)

byte	délka	hodnota	popis
SW	2	'XXXXh'	stavová slova (SW1, SW2)

- Pokud je příkaz úspěšný, vrací karta zpět '9000',
- pokud soubor odpovídající identifikátoru souborů není nalezen, zpět poslaný status zpracování je '6A82',
- při T=1 a pokud je Le byte přítomen, zpět posílaný status je '6700',
- při T=0 a pokud je vyžadována odezva po příkazu SELECT FILE, zpět posílaný status je '6900',
- jestliže vybraný soubor je považován za poškozený (je detekována chyba integrity uvnitř souboru atributů), zpět poslaný status zpracování je '6400' nebo '6581'.

3.6.2. Read Binary

Tento příkaz odpovídá ustanovením ISO/IEC 7816-4, jeho použití je ale ve srovnání s příkazem definovaným normou omezeno.

Příkaz Read Binary se používá ke čtení dat z transparentního souboru.

Odezva karty sestává z přečtených a zpět poslaných dat, volitelně uzavřených ve struktuře Secure Messaging.

TCS_323 Příkaz může být vykonán pouze tehdy, jestliže status bezpečnosti splňuje bezpečnostní atributy definované pro EF pro funkci READ.

3.6.2.1. Příkaz bez Secure Messaging

Tento příkaz dává možnost IFD číst data z EF aktuálně vybraná bez Secure Messaging.

TCS_324 Čtení dat ze souboru označeného „zakódovaný“ není možné tímto příkazem.

TCS_325 Příkazová zpráva

Byte	délka	hodnota	Popis
CLA	1	'00h'	nepožaduje se Secure Messaging
INS	1	'B0h'	
P1	1	'XXh'	offset v bytech od začátku souboru: nejvýznamnější byte
P2	1	'XXh'	offset v bytech od začátku souboru: nejméně významný byte
Le	1	'XXh'	očekávaná délka dat, počet bytů ke čtení

Poznámka: bit 8 z P1 musí být nastaven na 0.

TCS_326 Zpráva o odezvě

byte	délka	hodnota	popis
#1-#X	X	'XX...XXh'	čtená data
SW	2	'XXXXh'	stavová slova (SW1, SW2)

- Pokud je příkaz úspěšný, vrací karta zpět '9000',
- pokud EF není vybrán, zpět poslaný status zpracování je '6986',
- jestliže řízení přístupu vybraného souboru dat není uspokojivé, příkaz je přerušen s '6982'
- jestliže offset není kompatibilní s velikostí EF (offset > velikost EF), zpět posílaný status zpracování je '6B00',
- jestliže velikost dat ke čtení není kompatibilní s velikostí EF (offset + Le > velikost EF) zpět posílaný status zpracování je '6700' nebo '6Cxx', kde 'xx' udává přesnou délku,
- jestliže je detekována chyba integrity uvnitř souboru atributů, karta považuje soubor za poškozený a obnovitelný, zpět poslaný status zpracování je '6400' nebo '6581',
- pokud chyba integrity je detekována uvnitř uložených dat, karta vrátí požadovaná data a zpět poslaný status zpracování je '6281'.

3.6.2.2. Příkaz s Secure Messaging

Tento příkaz dává možnost IFD číst data z EF aktuálně vybraná s Secure Messaging za účelem ověření integrity přijatých dat a ochrany utajení dat v případě, že EF je označeno jako "zakódovaný".

TCS_327 Příkazová zpráva

byte	délka	hodnota	Popis
CLA	1	'0Ch'	požaduje se Secure Messaging
INS	1	'B0h'	INS
P1	1	'XXh'	P1 (offset v bytech od začátku souboru): nejvýznamnější byte
P2	1	'XXh'	P2 (offset v bytech od začátku souboru): nejméně významný byte
Lc	1	'09h'	délka vstupních dat pro Secure Messaging
#6	1	'97h'	T _{LE} : jmenovka pro specifikaci očekávané délky
#7	1	'01h'	L _{LE} : očekávaná délka
byte	délka	hodnota	Popis

#8	1	'NNh'	specifikace očekávané délky (originál Le): počet bytů ke čtení
#9	1	'8Eh'	T _{CC} : jmenovka pro kryptografický kontrolní součet
#10	1	'04h'	L _{CC} : délka následujícího kryptografického kontrolního součtu
#11- #14	4	'XX...XXh'	kryptografický kontrolní součet (4 nejvýznamnější byty)
Le	1	'00h'	podle specifikace v ISO/IEC 7816-4

TCS_328 Zpráva o odezvě, pokud EF není označeno jako „zakódovaný“ a jestliže vstupní formát Secure Messaging je správný:

byte	délka	hodnota	popis
#1	1	'81h'	T _{PV} : jmenovka pro zřetelnou hodnotu dat
#2	L	'NNh' nebo '81 NNh'	L _{PV} : délka vrácených dat (=originál Le) L je 2 byty, jestliže L _{PV} > 127 bytů
#(2+L)- #(1+L+NN)	NN	'XX...XXh'	zřetelná datová hodnota
#(2+L+NN)	1	'8Eh'	T _{CC} : jmenovka pro kryptografický kontrolní součet
#(3+L+NN)	1	'04h'	L _{CC} : délka následujícího kryptografického kontrolního součtu
#(4+L+NN)- #(7+L+NN)	4	'XX...XXh'	kryptografický kontrolní součet (4 nejvýznamnější byty)
SW	2	'XXXXh'	stavová slova (SW1, SW2)

TCS_329 Zpráva o odezvě, pokud EF není označeno jako „zakódovaný“ a jestliže vstupní formát Secure Messaging je správný:

byte	délka	hodnota	popis
#1	1	'87h'	T _{PI CG} : jmenovka pro kódovaná data (kryptogram)
#2	L	'MMh' nebo '81 MMh'	L _{PI CG} : délka vrácených kódovaných dat (v důsledku doplnění odlišných od originálu Le příkazu) L je 2 byty, jestliže L _{PI CG} >127 bytů
#(2+L)- #(1+L+MM)	MM	'01XX...XXh'	Kódovaná data: indikátor doplnění a kryptogram
#(2+L+MM)	1	'8Eh'	T _{CC} : jmenovka pro kryptografický kontrolní součet
#(3+L+MM)	1	'04h'	L _{CC} : délka následujícího kryptografického kontrolního součtu
#(4+L+MM)- #(7+L+MM)	4	'XXh...XXh'	kryptografický kontrolní součet (4 nejvýznamnější byty)
SW	2	'XXXXh'	stavová slova (SW1, SW2)

Vrácená kódovaná data obsahují první byte indikující použitý mód doplnění. Pro aplikaci tachografu přijímá indikátor doplnění vždy hodnotu '01h', indikující, že použitý mód doplnění odpovídá módu dle ISO/IEC 7816-4 (jeden byte s hodnotou '80h' následovaný několika nulovými byty: ISO/IEC 9797, metoda 2).

“Regulérní” stavy zpracování popsané pro příkaz READ BINARY bez Secure Messaging (viz odstavec 3.6.2.1.), mohou být vráceny za použití struktur zprávy o odezvě popsané dále, pod jmenovkou '99h' (jak je uvedeno v TCS 335).

Dodatečně se mohou vyskytnout nějaké chyby, které se týkají Secure Messaging. V takovém případě je status zpracování jednoduše vrácen bez struktury Secure Messaging:

TCS_330 Zpráva o odezvě, jestliže vstupní formát Secure Messaging je nekorektní

Byte	délka	hodnota	popis
SW	2	'XXXXh'	stavová slova (SW1, SW2)

- Jestliže neexistuje žádný aktuální klíč relace, stav zpracování '6A88' se posílá zpět. To se stane tehdy, jestliže klíč relace již není generován, nebo platnost klíče relace je prošlá (v tomto případě musí IFD zopakovat vzájemný proces prokázání totožnosti nastavením nového klíče relace).

- Jestliže některé datové objekty (jak je uvedeno výše) ve formátu Secure Messaging chybí, zpět poslaný stav zpracování je ‘6987’. Tato chyba se objeví, jestliže očekávaná jmenovka chybí nebo jestliže tělo příkazu neodpovídá požadavkům.
- Jestliže jsou některé datové objekty nekorektní, zpět poslaný stav zpracování je ‘6988’. Tato chyba se objeví, jestliže všechny požadované jmenovky existují, ale některé délky se liší od očekávaných.
- Jestliže přezkoušení kryptografického kontrolního součtu je chybné, zpět poslaný stav zpracování je ‘6688’.

3.6.3. Update Binary

Příkaz odpovídá ustanovením ISO/IEC 7816-4, jeho použití je však ve srovnání s příkazem definovaným v normě omezené.

Příkazová zpráva UPDATE BINARY spouští aktualizaci (erase + write) bitů již přítomných v binárním čísle EF s bity existujícími v příkazu APDU.

TCS_331 Příkaz může být vykonán pouze tehdy, jestliže status bezpečnosti splňuje bezpečnostní atributy definované pro EF pro funkci UPDATE (jestliže řízení přístupu funkce UPDATE obsahuje PRO SM, do příkazu musí být přidáno Secure Messaging).

3.6.3.1. Příkaz bez Secure Messaging

Tento příkaz umožňuje IFD psát data do aktuálně vybraného EF bez toho, aby karta přezkoušela integritu přijatých dat. Tento zřetelný mód je jen tehdy dovolený, když odpovídající soubor dat není označen “zakódovaný”.

TCS_332 Příkazová zpráva

Byte	délka	hodnota	popis
CLA	1	‘00h’	nepožaduje se Secure Messaging
INS	1	‘D6h’	
P1	1	‘XXh’	offset v bytech od začátku souboru: nejvýznamnější byte
P2	1	‘XXh’	offset v bytech od začátku souboru: nejméně významný byte
Lc	1	‘NNh’	Lc délka dat k aktualizaci, počet bytů k napsání
#6- #(5+NN)	NN	‘XX...XXh’	zapsaná data

Poznámka: bit 8 z P1 musí být nastaven na 0.

TCS_333 Zpráva o odezvě

Byte	délka	hodnota	popis
SW	2	'XXXXh'	stavová slova (SW1, SW2)

- Pokud je příkaz úspěšný, vrací karta zpět '9000',
- pokud EF není vybrán, zpět poslaný status zpracování je '6986',
- jestliže řízení přístupu vybraného souboru dat není uspokojivé, příkaz je přerušen s '6982'
- jestliže offset není kompatibilní s velikostí EF (offset > velikost EF), zpět posílaný status zpracování je '6B00',
- jestliže velikost dat k zapsání není kompatibilní s velikostí EF (offset + Le > velikost EF) zpět posílaný status zpracování je '6700',
- jestliže je detekována chyba integrity uvnitř souboru atributů, karta považuje soubor za poškozený a neopravitelný, zpět poslaný status zpracování je '6400' nebo '6500',
- jestliže je zápis neúspěšný, zpět poslaný status zpracování je '6581'.

3.6.3.2. Příkaz s Secure Messaging

Tento příkaz umožňuje IFD psát data do aktuálně vybraného EF s kartou přezkušující integritu přijatých dat. Protože není požadováno utajení, data nejsou zakódovaná.

TCS_334 Příkazová zpráva

byte	délka	hodnota	popis
CLA	1	'0Ch'	požaduje se Secure Messaging
INS	1	'D6h'	INS
P1	1	'XXh'	offset v bytech od začátku souboru: nejvýznamnější byte
P2	1	'XXh'	offset v bytech od začátku souboru: nejméně významný byte
Lc	1	'XXh'	délka zabezpečeného datového pole
#6	1	'81h'	T _{PV} : jmenovka pro zřetelnou hodnotu dat
#7	L	'NNh' nebo '81 NNh'	L _{PV} : délka přenesených dat L je 2 byty, jestliže L _{PV} > 127 bytů
#{7+L}- #{6+L+NN}	NN	'XX...XXh'	zřetelná datová hodnota
#{7+L+NN}	1	'8Eh'	T _{CC} : jmenovka pro kryptografický kontrolní součet

byte	délka	hodnota	Popis
#(8+L+NN)	1	'04h'	L _{CC} : délka následujícího kryptografického kontrolního součtu
#(9+L+NN)- #(12+L+NN)	4	'XX...XXh'	kryptografický kontrolní součet (4 nejvýznamnější byty)
Le	1	'00h'	podle specifikace v ISO/IEC 7816-4

TCS_335 Zpráva o odezvě jestliže vstupní formát Secure Messaging je správný:

byte	délka	hodnota	Popis
#1	1	'99h'	T _{SW} : jmenovka pro stavová slova (chráněno CC)
#2	1	'02h'	L _{SW} : délka vrácených stavových slov
#3- #4	2	'XXXXh'	stavová slova (SW1, SW2)
#5	1	'8Eh'	T _{CC} : jmenovka pro kryptografický kontrolní součet
#6	1	'04h'	L _{CC} : délka následujícího kryptografického kontrolního součtu
#7- #10	4	'XX...XXh'	kryptografický kontrolní součet (4 nejvýznamnější byty)
SW	2	'XXXXh'	stavová slova (SW1, SW2)

“Regulérní” stavy zpracování popsané pro příkaz UPDATE BINARY bez Secure Messaging (viz odstavec 3.6.3.1.), mohou být vráceny za použití struktury zprávy o odezvě popsané dále.

Dodatečně se mohou vyskytnout nějaké chyby, které se týkají Secure Messaging. V takovém případě je status zpracování jednoduše vrácen bez struktury Secure Messaging:

TCS_336 Zpráva o odezvě, jestliže je chyba v Secure Messaging

byte	délka	hodnota	Popis
SW	2	'XXXXh'	stavová slova (SW1, SW2)

- Jestliže neexistuje žádný aktuální klíč relace, stav zpracování '6A88' se posílá zpět,
- jestliže některé datové objekty (jak je uvedeno výše) ve formátu Secure Messaging chybí, zpět poslaný stav zpracování je '6987'. Tato chyba se objeví, jestliže očekávaná jmenovka chybí nebo jestliže tělo příkazu neodpovídá požadavkům,

- pokud jsou některé datové objekty nekorektní, zpět poslaný stav zpracování je '6988'. Tato chyba se objeví, jestliže všechny požadované jmenovky existují, ale některé délky se liší od očekávaných,
- jestliže přezkoušení kryptografického kontrolního součtu je chybné, zpět poslaný stav zpracování je '6688'.

3.6.4. Get Challenge

Tento příkaz je v souladu s ustanoveními ISO/IEC 7816-4; má ale omezené použití ve srovnání s příkazem definovaným v normě.

Příkaz GET CHALLENGE požaduje, aby karta k vydání výzvy o použití v proceduře vztahující se k bezpečnosti v které kryptogram nebo nějaká kódovaná data jsou poslána na kartu.

TCS_337 Kartou vydaná výzva je platná pouze pro příští příkaz, který používá výzvu poslanou na kartu.

TCS_338 Příkazová zpráva

byte	délka	hodnota	popis
CLA	1	'00h'	CLA
INS	1	'84h'	INS
P1	1	'00h'	P1
P2	1	'00h'	P2
Le	1	'08h'	Le (očekávaná délka výzvy)

TCS_339 Zpráva o odezvě

byte	délka	hodnota	popis
#1-#8	8	'XX...XXh'	Výzva
SW	2	'XXXXh'	stavová slova (SW1, SW2)

- Pokud je příkaz úspěšný, vrací karta zpět '9000',
- jestliže Le je odlišné od '08h', stav zpracování je '6700',
- jestliže jsou parametry P1 – P2 nekorektní, stav zpracování je '6A86'.

3.6.5. Verify

Tento příkaz je v souladu s ustanoveními ISO/IEC 7816-4; má ale omezené použití ve srovnání s příkazem definovaným v normě.

Příkaz Verify spouští na kartě srovnání příkazem poslaných CHV (PIN) dat s odkazem CHV uloženým na kartě.

Poznámka: PIN vložený uživatelem musí být vpravo doplněn přes IFD byty 'FFh' do délky 8 bytů.

TCS_340 Jestliže je příkaz úspěšný, jsou práva odpovídající CHV prezentaci uvolněna a čítač zbývajících pokusů opět spuštěn

TCS_341 Neúspěšné srovnání se zaznamená na kartě, aby se omezil počet dalších pokusů použití odkazu CHV.

TCS_342 Příkazová zpráva

byte	délka	hodnota	popis
CLA	1	'00h'	CLA
INS	1	'20h'	INS
P1	1	'00h'	P1
P2	1	'00h'	P2 (ověřená CHV je implicitně známá)
Lc	1	'08h'	délka přenášených CHV kódů
#6- #13	8	'XX...XXh'	CHV

TCS_343 Zpráva o odezvě

byte	délka	hodnota	popis
SW	2	'XXXXh'	stavová slova (SW1, SW2)

- Pokud je příkaz úspěšný, vrací karta zpět '9000',
- pokud odkaz CHV není nalezen, zpět poslaný status zpracování je '6A88',
- jestliže je CHV zablokován (čítač zbývajících pokusů je na nule), zpět poslaný status zpracování je '6983'. Když je tohoto stavu dosaženo, CHV nemůže už nikdy být úspěšně prezentován,
- jestliže je srovnání neúspěšné, čítač zbývajících pokusů se sníží a status '63CX' je vrácen ($X > 0$ a X se rovná čítači zbývajících CHV pokusů. Jestliže $X = 'F'$, čítač CHV pokusů je větší než 'F'),
- jestliže odkaz CHV je považován za poškozený, zpět poslaný status zpracování je '6400' nebo '6581'.

3.6.6. Get Response

Tento příkaz odpovídá ustanovením ISO/IEC 7816-4.

Tento příkaz (pouze pro protokol T=0 nutný a dostupný) je použit pro přenos připravených dat z karty do zařízení rozhraní (případ, kdy příkaz obsahoval jak Lc, tak Le).

Příkaz GET RESPONSE musí být vydán ihned po příkazu k přípravě dat, jinak jsou data ztracena. Po vykonání příkazu GET RESPONSE (kromě toho, kdy se vyskytne chyba '61xx' nebo '6Cxx', viz dále) dříve připravená data nejsou dále k dispozici.

TCS_344 Příkazová zpráva

byte	délka	hodnota	popis
CLA	1	'00h'	
INS	1	'C0h'	
P1	1	'00h'	
P2	1	'00h'	
Le	1	'XXh'	počet očekávaných bytů

TCS_345 Zpráva o odezvě

byte	délka	hodnota	popis
#1-#X	X	'XX...XXh'	data
SW	2	'XXXXh'	stavová slova (SW1, SW2)

- Pokud je příkaz úspěšný, vrací karta zpět '9000'.
- Pokud nejsou kartou připravena žádná data, zpět poslaný status zpracování je '6900' nebo '6F00'.
- Jestliže Le překročí počet dostupných bytů nebo jestliže Le je nula, zpět poslaný status zpracování je '6Cxx', kde 'xx' udává přesný počet dostupných bytů. V takovém případě připravená data jsou ještě pro následující příkaz GET RESPONSE k dispozici.
- Jestliže Le není nula a je menší než počet dostupných bytů, požadovaná data jsou normálně poslána kartou. Zpět poslaný status zpracování je '61xx', kde 'xx' udává počet dodatečných bytů, které jsou pro následující příkaz GET RESPONSE k dispozici.
- Jestliže příkaz není podporován (protokol T=1), karta vrací '6D00'.

3.6.7. PSO: Verify Certificate

Tento příkaz je v souladu s ustanoveními ISO/IEC 7816-8; má ale omezené použití ve srovnání s příkazem definovaným v normě.

Příkaz VERIFY CERTIFICATE je používán kartou k získání veřejného klíče zvenku a ke kontrole jeho platnosti.

TCS_346 Pokud je příkaz VERIFY CERTIFICATE úspěšný, veřejný klíč je uložen k budoucímu použití v bezpečném prostředí. Tento klíč bude explicitně nastaven pro použití v příkazech vztahujících se k bezpečnosti

(INTERNAL AUTHENTICATE, EXTERNAL AUTHENTICATE nebo VERIFY CERTIFICATE) pomocí příkazu MSE (viz bod 3.6.10.) při použití jeho identifikátoru klíče.

TCS_347 V každém případě používá příkaz VERIFY CERTIFICATE veřejný klíč, dříve vybraný příkazem MSE k otevření certifikátu. Přitom se musí jednat o veřejný klíč členského státu nebo Evropy.

TCS_348 Příkazová zpráva

Byte	délka	hodnota	popis
CLA	1	'00h'	CLA
INS	1	'2Ah'	Perform Security Operation
P1	1	'00h'	P1
P2	1	'AEh'	P2: ne BER-TLV kódovaná data (zřetězení datových elementů)
Lc	1	'CEh'	Lc: délka certifikátu, 194 bytů
#6- #199	194	'XX...XXh'	Certifikát: zřetězení datových elementů (jak je popsáno v doplňku 11)

TCS_349 Zpráva o odezvě

Byte	délka	hodnota	popis
SW	2	'XXXXh'	stavová slova (SW1, SW2)

- Pokud je příkaz úspěšný, vrací karta zpět '9000',
- jestliže ověření certifikátu je chybné, zpět poslaný status zpracování je '6688'. Proces ověření a rozvinutí certifikátoru je popsán v dodatku 11,
- jestliže v bezpečném prostředí neexistuje žádný veřejný klíč, vrací se '6A88',
- jestliže vybraný veřejný klíč (použitý k rozvinutí certifikátu) se považuje za poškozený, zpět poslaný status zpracování je '6400' nebo '6581',
- jestliže vybraný veřejný klíč (použitý k rozvinutí certifikátu) má CHA.LSB (CertificateHolderAuthorisation.equipmentType) rozdílný od '00' (např. není jedním z členských států nebo Evropy), zpět poslaný status zpracování je '6985'.

3.6.8. Internal Authenticate

Tento příkaz je v souladu s ustanoveními ISO/IEC 7816-4.

Použitím příkazu INTERNAL AUTHENTICATE může IFD ověřit pravost karty.

Proces ověření pravosti je popsán v dodatku 11. Obsahuje následující výroky:

TCS_350 Příkaz INTERNAL AUTHENTICATE používá soukromý klíč karty (implicitně vybraný) k označování ověřených dat včetně K1 (první element pro dohodu klíče relace) a RND1, a používá aktuálně vybraný veřejný klíč (pomocí posledního MSE příkazu) k zakódování značky a tvaru známky prokázání totožnosti (další podrobnosti v dodatku 11).

TCS_351 Příkazová zpráva

Byte	délka	hodnota	popis
CLA	1	'00h'	CLA
INS	1	'88h'	INS
P1	1	'00h'	P1
P2	1	'00h'	P2
Lc	1	'10h'	délka dat poslaných na kartu
#6- #13	8	'XX...XXh'	výzva k prokázání totožnosti karty
#14- #21	8	'XX...XXh'	VU.CHR (viz dodatek 11)
Le	1	'80h'	délka dat očekávaných z karty

TCS_352 Zpráva o odezvě

Byte	délka	hodnota	popis
#1- #128	128	'XX...XXh'	Známka prokázání totožnosti karty (viz dodatek 11)
SW	2	'XXXXh'	stavová slova (SW1, SW2)

- Pokud je příkaz úspěšný, vrací karta zpět '9000',
- jestliže neexistuje žádný veřejný klíč v bezpečném prostředí, zpět poslaný status zpracování je '6A88',
- jestliže neexistuje žádný soukromý klíč v bezpečném prostředí, zpět poslaný status zpracování je '6A88',
- jestliže VU.CHR se neshoduje s aktuálním identifikátorem veřejného klíče, zpět poslaný status zpracování je '6A88',
- jestliže vybraný soukromý klíč je považován za poškozený, zpět poslaný status zpracování je '6400' nebo '6581'.

TCS_353 Jestliže příkaz INTERNAL AUTHENTICATE je úspěšný, aktuální klíč relace, pokud existuje, je vymazán a již není k dispozici. Aby byl nový klíč relace k dispozici, musí být úspěšně proveden příkaz EXTERNAL AUTHENTICATE.

3.6.9. External Authenticate

Tento příkaz je v souladu s ustanoveními ISO/IEC 7816-4.

Použitím příkazu EXTERNAL AUTHENTICATE může karta prokázat totožnost IFD.

Proces ověření pravosti je popsán v dodatku 11. Obsahuje následující výroky:

TCS_354 Příkaz GET CHALLENGE musí bezprostředně předcházet příkaz EXTERNAL AUTHENTICATE. Karta vydává ven výzvu (RND3).

TCS_355 Ověření zakódování používá RND3 (výzva vydaná kartou), soukromý klíč karty (implicitně vybraný) a veřejný klíč dříve vybraný příkazem MSE.

TCS_356 Karta ověřuje zakódování a jestliže je toto správné, podmínka přístupu AUT se otevře.

TCS_357 Vstupní zakódování nese druhý element pro dohodu klíče relace K2.

TCS_358 Příkazová zpráva

Byte	délka	hodnota	popis
CLA	1	'00h'	CLA
INS	1	'2Ah'	INS
P1	1	'00h'	P1
P2	1	'AEh'	P2 (použitý veřejný klíč je implicitně známý a byl již dříve nastaven příkazem MSE)
Lc	1	'CEh'	Lc (délka dat poslaných na kartu)
#6- #133	128	'XX...XXh'	zakódování (viz dodatek 11)

TCS_359 Zpráva o odezvě

Byte	délka	hodnota	popis
SW	2	'XXXXh'	stavová slova (SW1, SW2)

- Pokud je příkaz úspěšný, vrací karta zpět '9000',
- jestliže žádný veřejný klíč není v bezpečném prostředí, vrací se zpět '6A88',
- jestliže CHA aktuálně nastaveného veřejného klíče není zřetězení AID aplikace tachografu a typu zařízení celku ve vozidle, zpět poslaný status zpracování je '6F00 (viz dodatek 11),'
- jestliže žádný soukromý klíč není v bezpečném prostředí, zpět poslaný status zpracování je '6A88',

- jestliže ověření certifikátu je chybné, zpět poslaný status zpracování je ‘6688’,
- jestliže příkaz bezprostředně nepředchází příkaz GET CHALLENGE, zpět poslaný status zpracování je ‘6985’,
- jestliže vybraný soukromý klíč se považuje za poškozený, zpět poslaný status zpracování je ‘6400’ nebo ‘6581’.

TCS_360 Jestliže příkaz EXTERNAL AUTHENTICATE je úspěšný a jestliže první část klíče relace je k dispozici krátce před úspěšným provedením příkazu INTERNAL AUTHENTICATE, klíč relace je nastaven pro příští příkazy při použití Secure Messaging.

TCS_361 Jestliže první část klíče relace není k dispozici z dřívějšího příkazu INTERNAL AUTHENTICATE, druhá část klíče relace poslaná IFD není uložena na kartu. Tento mechanismus zajistí, že vzájemný proces prokázání totožnosti je proveden v pořadí specifikovaném v dodatku 11.

3.6.10. Manage Security Environment

Tento příkaz je použit pro nastavení veřejného klíče k účelu prokázání totožnosti.

Tento příkaz je v souladu s ustanoveními ISO/IEC 7816-8. Použití tohoto příkazu je však omezeno s ohledem na odpovídající normu.

TCS_362 Klíč, na který je v MSE datovém poli odkazováno, je platný pro každý soubor dat DF tachografu.

TCS_363 Klíč, na který je v MSE datovém poli odkazováno, zůstává aktuálním veřejným klíčem do příštího správného MSE příkazu.

TCS_364 Jestliže klíč, na který je odkazováno, již není na kartě k dispozici, bezpečné prostředí zůstává nezměněno.

TCS_365 Příkazová zpráva

Byte	délka	hodnota	popis
CLA	1	‘00h’	CLA
INS	1	‘22h’	INS
P1	1	‘C1h’	P1: klíč, na který je odkazováno, platí pro všechny kódované operace
P2	1	‘B6h’	P2 (data, na která je odkazováno, týkající se digitálního podpisu)
Lc	1	‘0Ah’	Lc: délka následujícího datového pole
#6	1	‘83h’	jmenovka pro odkaz na veřejný klíč v asymetrických případech
#7	1	‘08h’	délka odkazu na klíč (identifikátor klíče)
#8- #15	08h	‘XX...XXh’	Identifikátor klíče dle specifikace v dodatku 11

TCS_366 Zpráva o odezvě

Byte	délka	hodnota	popis
SW	2	'XXXXh'	stavová slova (SW1, SW2)

- Pokud je příkaz úspěšný, vrací karta zpět '9000',
- pokud klíč, na který je odkazováno, není na kartě, zpět poslaný status zpracování je '6A88',
- pokud chybějí některé očekávané datové objekty v Secure Messaging Format, zpět poslaný status zpracování je '6987'. To může nastat, když chybí jmenovka '83h',
- jestliže některé datové objekty jsou nekorektní, zpět poslaný status zpracování je '6988'. To může nastat, když délka identifikátoru klíče není '08h',
- jestliže vybraný klíč je považován za poškozený, zpět poslaný status zpracování je '6400' nebo '6581'.

3.6.11. PSO: Hash

Tento příkaz slouží k přenosu výsledku hash zpracování určitých dat na kartu. Tento příkaz slouží pro ověření digitálních podpisů. Hash hodnota je uložena v EPROM paměti pro následující příkaz ověření digitálního podpisu.

Tento příkaz je v souladu s ustanoveními ISO/IEC 7816-8. Použití tohoto příkazu je však omezeno s ohledem na odpovídající normu.

TCS_367 Příkazová zpráva

Byte	délka	hodnota	popis
CLA	1	'00h'	CLA
INS	1	'2Ah'	Perform Security Operation
P1	1	'90h'	zpět poslaný Hash-Code
P2	1	'A0h'	jmenovka: datové pole obsahuje příslušný DO pro použití Hash-Code
Lc	1	'16h'	délka Lc následujícího datového pole
#6	1	'90h'	jmenovka pro Hash-Code
#7	1	'14h'	délka Hash-Code
#8- #27	20	'XX...XXh'	Hash-Code

TCS_368 Zpráva o odezvě

Byte	délka	hodnota	popis
SW	2	'XXXXh'	stavová slova (SW1, SW2)

- Pokud je příkaz úspěšný, vrací karta zpět ‘9000’,
- pokud chybějí některé očekávané datové objekty (jak je uvedeno výše), zpět poslaný status zpracování je ‘6987’. To může nastat, když chybí jmenovka ‘90h’,
- jestliže některé datové objekty jsou nekorektní, zpět poslaný status zpracování je ‘6988’. Tato chyba nastane, když potřebná jmenovka sice existuje, ale s jinou délkou než ‘14h’.

3.6.12. Perform Hash of File

Tento příkaz není v souladu s ustanoveními ISO/IEC 7816-8. Potom CLA-byte tohoto příkazu udává, že následuje chráněné použití PERFORM SECURITY OPERATION/HASH.

TCS_369 Příkaz PERFORM HASH OF FILE je použit k Hash-zpracování rozsahu dat aktuálně vybraného transparentního souboru EF.

TCS_370 Výsledek Hash-operace se uloží na kartu. To může potom být použito k tomu, aby soubor byl opatřen digitálním podpisem pomocí příkazu PSO: COMPUTE DIGITAL SIGNATURE. Tento výsledek pak zůstává k dispozici pro příkaz COMPUTE DIGITAL SIGNATURE do příštího úspěšného příkazu PERFORM HASH OF FILE.

TCS_371 Příkazová zpráva

Byte	délka	hodnota	popis
CLA	1	‘80h’	CLA
INS	1	‘2Ah’	Perform Security Operation
P1	1	‘90h’	jmenovka: Hash
P2	1	‘00h’	P2: Hash-zpracování dat aktuálně vybraného transparentního souboru

TCS_372 Zpráva o odezvě

Byte	délka	hodnota	popis
SW	2	‘XXXXh’	stavová slova (SW1, SW2)

- Pokud je příkaz úspěšný, vrací karta zpět ‘9000’,
- pokud není vybrána žádná aplikace, zpět poslaný status zpracování je ‘6985’,
- jestliže vybraný EF je považován za poškozený (chyby integrity atributů souboru nebo uložených dat), zpět poslaný status zpracování je ‘6400’ nebo ‘6581’,
- jestliže vybraný soubor není transparentní soubor, zpět poslaný status zpracování je ‘6986’.

3.6.13. PSO: Compute Digital Signature

Tento příkaz se používá pro výpočet digitálního podpisu dříve vypočteného Hash-Code (viz PERFORM HASH OF FILE, odstavec 3.6.12.).

Tento příkaz je v souladu s ustanoveními ISO/IEC 7816-8. Použití tohoto příkazu je však omezeno s ohledem na odpovídající normu.

TCS_373 Soukromý klíč karty je použit k výpočtu digitálního podpisu a kartě je implicitně znám.

TCS_374 Karta provede digitální podpis použitím metody doplnění podle PKCS1 (podrobnosti viz doplněk 11).

TCS_375 Příkazová zpráva

Byte	délka	hodnota	popis
CLA	1	'00h'	CLA
INS	1	'2Ah'	Perform Security Operation
P1	1	'9Eh'	zpět poslaný digitální podpis
P2	1	'9Ah'	jmenovka: datové pole obsahuje data k označení. Jestliže žádné datové pole není zahrnuto, předpokládá se, že data jsou již na kartě (hash of file)
Le	1	'80h'	délka očekávaného podpisu

TCS_376 Zpráva o odezvě

Byte	délka	hodnota	popis
#1- #128	128	'XX...XXh'	podpis dříve vypočítané Hash
SW	2	'XXXXh'	stavová slova (SW1, SW2)

- Pokud je příkaz úspěšný, vrací karta zpět '9000',
- jestliže implicitně vybraný soukromý klíč se považuje za poškozený, zpět poslaný status zpracování je '6400' nebo '6581'.

3.6.14. PSO: Verify Digital Signature

Tento příkaz se používá k ověření digitálního podpisu, prováděného jako vstup podle PKCS1 zprávy, jejíž Hash je kartě znám. Algoritmus podpisu je kartě implicitně znám.

Tento příkaz je v souladu s ustanoveními ISO/IEC 7816-8. Použití tohoto příkazu je však omezeno s ohledem na odpovídající normu.

TCS_377 Příkaz VERIFY DIGITAL SIGNATURE používá vždy veřejný klíč vybraný předchozím příkazem MANAGE SECURITY ENVIRONMENT, jakož předchozí Hash-Code vložený PSO: Hash příkaz.

TCS_378 Příkazová zpráva

Byte	délka	hodnota	popis
CLA	1	'00h'	CLA
INS	1	'2Ah'	Perform Security Operation
P1	1	'00h'	jmenovka: datové pole obsahuje DO příslušný k ověření
P2	1	'A8h'	
Lc	1	'83h'	délka Lc následujícího datového pole
#28	1	'9Eh'	jmenovka pro digitální podpis
#29- #30	1	'8180h'	délka digitálního podpisu (128 bytů, kódovaných dle ISO/IEC 7816-6)
#31- #158	128	'XX...XXh'	obsah digitálního podpisu

TCS_379 Zpráva o odezvě

Byte	délka	hodnota	popis
SW	2	'XXXXh'	stavová slova (SW1, SW2)

- Pokud je příkaz úspěšný, vrací karta zpět '9000',
- jestliže se ověření podpisu se nezdaří, zpět poslaný status zpracování je '6688'. Průběh ověřování je popsán v doplňku 11,
- jestliže není vybrán žádný veřejný klíč, zpět poslaný status zpracování je '6A88',
- pokud chybějí některé očekávané datové objekty (jak je uvedeno výše), zpět poslaný status zpracování je '6987'. To může nastat, když chybí jedna z požadovaných jmenovek,
- jestliže není k dispozici žádný Hash-Code ke zpracování příkazu (jako výsledek předchozího PSO: Hash příkaz), zpět poslaný status zpracování je '6985',
- jestliže některé datové objekty jsou nekorektní, zpět poslaný status zpracování je '6988'. To může nastat, když jedna z požadovaných délek datových objektů je nekorektní,
- jestliže vybraný klíč je považován za poškozený, zpět poslaný status zpracování je '6400' nebo '6581'.

4. STRUKTURA KARET TACHOGRAFU

V tomto odstavci jsou specifikovány struktury dat, které slouží pro uložení přístupných dat na karty tachografu.

Nejsou specifikovány vnitřní struktury závislé na výrobci karty, jako například počáteční návěští souboru nebo paměť a zpracování datových prvků, které jsou nutné pouze pro interní potřebu, například

EuropeanPublicKey, CardPrivateKey, TDesSessionKey or WorkshopCardPin.

Užitečná kapacita paměti karet tachografu musí být nejméně 11 Kbyťů. Větší kapacity mohou být použity. V takovém případě struktura karty zůstává stejná, ale zvyšuje se počet záznamů některých prvků struktury. Tento odstavec specifikuje nejmenší a největší hodnoty počtu záznamů.

4.1. Struktura karty řidiče

TCS_400 Po její personalizaci vykazuje karta řidiče následující trvalou strukturu souborů a podmínek přístupu do souborů:

File	File ID	Access conditions		
		Read	Update	Encrypted
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

Access conditions - podmínky přístupu

TCS_401 Struktury všech EF jsou transparentní

TCS_402 Čtení s Secure Messaging musí být možné pro všechny soubory pod DF tachograf.

TCS_403 Karta řidiče má následující strukturu dat:

File/Data element	No of Records	Size (bytes)		Default Values
		Min	Max	
MF	11411	25	25	
EF ICC	25	25	25	
CardIccIdentification	25	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	11378	24926	24926	
EF Application_Identification	10	10	10	
DriverCardApplicationIdentification	10	10	10	
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}
EF Card_Certificate	194	194	194	
CardCertificate	194	194	194	{00..00}
EF CA_Certificate	194	194	194	
MemberStateCertificate	194	194	194	{00..00}
EF Identification	143	143	143	
CardIdentification	65	65	65	
cardIssuingMemberState	1	1	1	{00}
cardNumber	16	16	16	{20..20}
cardIssuingAuthorityName	36	36	36	{20..20}
cardIssueDate	4	4	4	{00..00}
cardValidityBegin	4	4	4	{00..00}
cardExpiryDate	4	4	4	{00..00}
DriverCardHolderIdentification	78	78	78	
cardHolderName	72	72	72	
holderSurname	36	36	36	{00, 20..20}
holderFirstNames	36	36	36	{00, 20..20}
cardHolderBirthDate	4	4	4	{00..00}
cardHolderPreferredLanguage	2	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}
occasionOpenVehicle				
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}

File/Data element - soubor/prvek dat
 No of Records - počet záznamů
 Size (bytes) - velikost (v bytech)
 Default Values - standardní hodnoty

TCS_404 Následující, v tabulce uvedené hodnoty k údajům o rozměrech, jsou nejmenší a největší počty záznamů, které musí datová struktura karty řidiče použít:

		Min	Max
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 bytes (28 days * 93 activity changes)	13 776 bytes (28 days * 240 activity changes)

28 days - 28 dnů
 93 activity changes - 93 změn činnosti

4.2. Struktura dílenské karty

TCS_405 Po její personalizaci vykazuje dílenská karta následující trvalou strukturu souborů a podmínek přístupu do souborů:

File	File ID	Access conditions		
		Read	Update	Encrypted
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	0509	ALW	ALW	No
EF Calibration	050A	ALW	PRO SM / AUT	No
EF Sensor_Installation_Data	050B	ALW	NEV	Yes
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 Struktury všech EF jsou transparentní.

TCS_407 Čtení s Secure Messaging musí být možné pro všechny soubory pod DF tachograf.

TCS_408 Dílenská karta má následující strukturu dat:

File/Data element	No of Records	Size (Bytes)		Default Values
		Min	Max	
MF	11088	25	29061	
EF ICC	25	25	25	
CardIccIdentification	25	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	11	
WorkshopCardApplicationIdentification	11	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
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	
entryTime	4	4	{00..00}
entryTypeDailyWorkPeriod	1	1	{00}
dailyWorkPeriodCountry	1	1	{00}
dailyWorkPeriodRegion	1	1	{00}
vehicleUdometerValue	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	
entryTime	4	4	{00..00}
SpecificConditionType	1	1	{00}

TCS_409 Následující, v tabulce uvedené hodnoty k údajům o rozměrech, jsou nejmenší a největší počty záznamů, které musí datová struktura dílenské karty použít:

		Min	Max
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 bytes (1 day * 93 activity changes)	492 bytes (1 day * 240 activity changes)

4.3. Struktura kontrolní karty

TCS_410 Po její personalizaci vykazuje kontrolní karta následující trvalou strukturu souborů a podmínek přístupu do souborů:

File	File ID	Access conditions		
		Read	Update	Encrypted
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 Struktury všech EF jsou transparentní.

TCS_412 Čtení s Secure Messaging musí být možné pro všechny soubory pod DF tachograf.

TCS_413 Kontrolní karta má následující strukturu dat:

Archivo/Elemento de datos	No of Records	Size (Bytes)		Default Values
		Min	Max	
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	n ₇	46	46	
controlType		1	1	{00}
controlTime		4	4	{00..00}
controlledCardNumber				
cardType		1	1	{00}
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
controlledVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
controlDownloadPeriodBegin		4	4	{00..00}
controlDownloadPeriodEnd		4	4	{00..00}

TCS_414 Následující, v tabulce uvedené hodnoty k údajům o rozměrech, jsou nejmenší a největší počty záznamů, které musí datová struktura kontrolní karty použít:

		Min	Max
n ₇	NoOfControlActivityRecords	230	520

4.4. Struktura karty společnosti

TCS_415 Po její personalizaci vykazuje karta společnosti následující trvalou strukturu souborů a podmínek přístupu do souborů:

File	File ID	Access conditions		
		Read	Update	Encrypted
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 Struktury všech EF jsou transparentní.

TCS_417 Čtení s Secure Messaging musí být možné pro všechny soubory pod DF tachograf.

TCS_418 Karta společnosti má následující strukturu dat:

File/Data element	No of Records	Size (bytes)		Default Values
		Min	Max	
MF	1	11147	24487	
EF ICC	25	25	25	
CardIccIdentification	25	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	1	1114	24454	
EF Application_Identification	5	5	5	
CompanyCardApplicationIdentification	5	5	5	
typeOfTachographCardId	1	1	1	{00}
cardStructureVersion	2	2	2	{00 00}
noOfCompanyActivityRecords	2	2	2	{00 00}
EF Card_Certificate	194	194	194	
CardCertificate	194	194	194	{00..00}
EF CA_Certificate	194	194	194	
MemberStateCertificate	194	194	194	{00..00}
EF Identification	139	139	139	
CardIdentification	65	65	65	
cardIssuingMemberState	1	1	1	{00}
cardNumber	16	16	16	{20..20}
cardIssuingAuthorityName	36	36	36	{00, 20..20}
cardIssueDate	4	4	4	{00..00}
cardValidityBegin	4	4	4	{00..00}
cardExpiryDate	4	4	4	{00..00}
CompanyCardHolderIdentification	74	74	74	
companyName	36	36	36	{00, 20..20}
companyAddress	36	36	36	{00, 20..20}
cardHolderPreferredLanguage	2	2	2	{20 20}
EF Company_Activity_Data	10582	23922	23922	
CompanyActivityData	10582	23922	23922	
companyPointerNewestRecord	2	2	2	{00 00}
companyActivityRecords	10580	23920	23920	
companyActivityRecord	n _g	46	46	
companyActivityType	1	1	1	{00}
companyActivityTime	4	4	4	{00..00}
cardNumberInformation				
cardType	1	1	1	{00}
cardIssuingMemberState	1	1	1	{00}
cardNumber	16	16	16	{20..20}
vehicleRegistrationInformation				
vehicleRegistrationNation	1	1	1	{00}
vehicleRegistrationNumber	14	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 Následující, v tabulce uvedené hodnoty k údajům o rozměrech, jsou nejmenší a největší počty záznamů, které musí datová struktura karty společnosti použít:























		Min	Max
n _g	NoOfCompanyActivityRecords	230	520

DODATEK 3

PIKTOGRAMY

PIC_01 Záznamové zřízení může používat následující piktogramy a jejich kombinace:

1. ZÁKLADNÍ PIKTOGRAMY

	Osoby	Akce	Mód provozu
	společnost		mód společnosti
	kontrolor	kontrola	kontrolní mód
	řidič	řízení	provozní mód
	dílna/ zkušební stanice	přezkoušení/kalibrace	kalibrační mód
	výrobce		
	Činnosti	Trvání	
	pohotovost	průběžná doba pohotovosti	
	řízení	nepřetržitá doba řízení	
	odpočinek	nepřetržitá doba odpočinku	
	práce	nepřetržitě trvání práce	
	přestávka	kumulovaná doba odpočinku	
	neznámá		
	Zařízení	Funkce	
	slot řidiče		
	slot druhého řidiče		
	karta		
	hodiny		
	displej	zobrazení	
	externí uložení	stažení dat	
	napájení (proudem)		
	tiskárna/výtisk	tisknout	
	snímač		
	rozměr pneumatiky		
	vozidlo/celek ve vozidle		






Zvláštní podmínky			
OUT	kontrolní zařízení není nutné		
⚠	trajekt/jízda vlakem		
Různé			
!	události	✕	závady
▶	začátek denní pracovní doby	⏸	konec denní pracovní doby
•	umístění	M	manuální vstup činností řidiče
🔒	bezpečnost	➤	rychlost
⌚	čas	Σ	celkový/souhrn

Kvalifikace	
24h	denně
	týdně
	dva týdny
➔	od nebo do




2. KOMBINACE PIKTOGRAMŮ

Různé			
🔒 •	kontrolní místo		
• ▶	místo začátku denní pracovní doby	▶ •	místo konce denní pracovní doby
⌚ ➔	začátek času	➔ ⌚	konec času
🚗 ➔	z vozidla		
OUT ➔	kontrolní zařízení není nutné - začátek	➔ OUT	kontrolní zařízení není nutné - konec







Karty

	karta řidiče
	karta společnosti
	kontrolní karta
	dílenská karta
 - - -	žádná karta









Řízení




	řízení posádkou
	doba řízení během jednoho týdne
	doba řízení během dvou týdnů

Tisky








24h 	denní výtisk činností řidiče z karty
24h 	denní výtisk činností řidiče z celku ve vozidle
! x 	výtisk událostí a závad z karty
! x 	výtisk událostí a závad z celku ve vozidle
T 	výtisk technických dat
>> 	výtisk překročení rychlosti

Události






! 	vložení neplatné karty
! 	konflikt karty
! 	překrytí času
! 	řízení bez vhodné karty
! 	vložení karty během řízení
! 	poslední operace, která nebyla korektně uzavřena
>>	překročení rychlosti
! 	přerušeni napájení proudem
! 	chyba dat dráhy a rychlosti

	narušení spolehlivosti
	nastavení času (dílnou)
	kontrola překročení rychlosti

Závady

	závada karty (slot řidiče)
	závada karty (slot druhého řidiče)
	závada displeje
	závada stahování dat
	závada tiskárny
	závada snímače
	závada celku ve vozidle

Manuální vstupní proces

	nadále stejná denní pracovní doba?
	konec předešlé pracovní doby?
	potvrzení nebo vložení místa a konce pracovní doby
	vložení začátku času
	vložení místa začátku pracovní doby

Poznámka: Další kombinace piktogramů jako blok nebo identifikátory záznamového zařízení jsou uvedeny v dodatku 4.

Dodatek 4

VÝTISKY

OBSAH

1.	VŠEOBECNĚ	193
2.	SPECIFIKACE DATOVÝCH BLOKŮ	193
3.	SPECIFIKACE VÝTISKU	201
3.1	Činnosti řidiče na výpisu denní karty	201
3.2	Činnosti řidiče na denním výpisu VU	202
3.3	Události a chyby z výtisku karty	203
3.4	Události a chyby z výpisu VU	203
3.5	Události a chyby z výpisu VU	204
3.6	Výtisk překročení povolené rychlosti	204

1. VŠEOBECNĚ

Každý výtisk sestává z řetězce bloků různých údajů, které je možné rozlišit blokovým identifikátorem

Údaje v bloku obsahují jeden nebo více záznamů, které je možné rozlišit identifikátorem záznamu

PRT_001 Pokud má identifikátor bloku okamžitou přednost před identifikátorem záznamu identifikátor záznamu se netiskne.

PRT_002 V případě, když není známa část údajů nebo nemohou být vytištěny z důvodů právního přístupu k těmto údajům jsou místo nich mezery.

PRT_003 Pokud je neznám obsah celé řádky nebo nemůže být vytištěn vynechá se celá řádka

PRT_004 Číselná data se vytisknou seřazeny vpravo s mezerami mezi tisíci a miliony a bez nul na začátku.

PRT_005 Alfnumerická data se vytisknou seřazeny vlevo doplněny mezerami délky datového článku nebo zkrácené o délku datového článku pokud je to zapotřebí (jména a adresy)

2. Specifikace datových bloků

V této kapitole byl použit následující formát smluvených znaků:

znaky vytištěné **tučně** znamenají jednoduchý text (zbytek je vytištěn normálně),

normální znaky označují proměnné (piktogramy nebo údaje), pro vytištění jsou nahrazeny svými hodnotami,

různá jména byla podtržena, aby se ukázala postačující délka údajového článku pro proměnnou,

datumy jsou uvedeny ve tvaru „dd/mm/yyyy“ (den/měsíc/rok). Tvar „dd.mm.yyyy“ je též smí použit

termín „identifikace karty“ označuje skladbu: typu karty pomocí kombinace piktogramů, kódu členského státu vydávajícího kartu, znakem lomítka a číslem karty s náhradním indexem a obnovovacím indexem oddělenými mezerami:

P	<input checked="" type="checkbox"/>	x	x	x	/	x	x	x	x	x	x	x	x	x	x	x	x	x	x		x		x
kombinace piktogramu karty	Státní kód vydávajícího státu				Prvních čtrnáct znaků čísla karty (pokud možno zahrnující i pořadový index)															Index náhrady		Index obnovení	

PRT_006 Výtisky musí použít následující bloky údajů a/nebo záznamy údajů
v souladu s následujícími významy a formáty

Blok nebo záznam čísla znamená

Data Format

- Datum a čas, kdy byl dokument
vytištěn**

▼ dd/mm/yyyy hh:mm (UTC)

- Typ výtisku**
Identifikátor bloku
Vytištěná kombinace piktogramů (viz
dopl. 3). Nastavení omezovače
rychlosti (Vytištění pouze překročení
rychlosti)

-----▼-----
Picto xxx km/h

- Označení držitele karty**
Identifikátor bloku, P = piktogram
lidí
Příjmení držitele karty
Křestní jméno (jména) držitele karty
(pokud je)
Identifikace karty
Datum ukončení platnosti karty
V případě, když karta není osobní a
neobsahuje příjmení držitele musí být
místo něj vytištěno jméno společnosti
nebo dílny nebo kontrolního útvaru.

-----P-----
P Last_Name _____
First_Name _____
Card_Identification _____
dd/mm/yyyy

- Identifikace vozidla**
Identifikátor bloku
(VIN)
Registrující členský stát a a
registrační číslo vozidla

-----A-----
A VIN _____
Nat/VRN _____

- Identifikace celku ve vozidle**
Identifikátor bloku
Název výrobce VU
číslo VU

-----B-----
B VU_Manufacturer _____
VU_Part_Number _____

6. **Poslední kalibrace záznamového zařízení**

Identifikátor bloku
Název dílny
Identifikace karty dílny
Datum kalibrace

```

-----↑-----
↑ Last_Name _____
Card_Identification _____
↑ dd/mm/yyyy
  
```

7. **Poslední kontrola (kontrolním úředníkem)**

Identifikátor bloku
Identifikace karty kontrolora
Datum, čas a typ kontroly
Typ kontroly; Do čtyř piktogramů.
Typ kontroly může být (nějakou kombinací): Vyprázdnění karty, vyprázdněním VJ, vytištěním, zobrazením na displeji

```

-----□-----
Card_Identification _____
□ dd/mm/yyyy hh:mm pppp
  
```

8. **Činnosti řidiče zaznamenané na kartě v pořadí událostí**

Identifikátor bloku
Datum šetření (kalendářní den výtisku) + denní karta počítadla

```

-----□-----
Card_Identification _____
□ dd/mm/yyyy hh:mm pppp
  
```

8.1 Doba po níž nebyla karta vložena

8.1a Identifikátor záznamu (začátek časového úseku)

8.1b Neznámá doba. Začátek a konec doby trvání

8.1c Manuálně vložené činnosti
Piktogram činnosti, začátek a konec doby trvání (včetně)
alespoň jednohodinové doby
odpočinku jsou označeny hvězdičkou

```

-----
? hh:mm hh:mm hh:mm
A hh:mm hh:mm hh:mm *
```

8.2 Vložení karty do otvoru pro kartu S
Identifikátor záznamu, Piktogram otvoru pro kartu
Členský stát, který vozidlo registruje a registrační číslo vozidla
Stav tachometru při vložení karty

```

-----S-----
A Nat/VRN _____
x xxx xxx km
```

8.3 Činnosti (po vložení karty)
Piktogram činnosti, začátek a konec doby trvání (včetně)
Stav posádky (piktogram posádky, pokud je, prázdko, pokud je jeden), alespoň jednohodinové doby
odpočinku jsou označeny hvězdičkou

```

A hh:mm hh:mm hh:mm 00 *
```

8.3a	Specifické podmínky. Čas vstupu, piktogram specifické podmínky (nebo kombinace piktogramů)	hh:mm - - - - pppp - - - -
8.4	<i>Vyjmutí karty</i> Stav tachometru vozidla a ujetá vzdálenost od posledního zasunutí po kterou je stav tachometru znám	x xxx xxx km; x xxx km
9.	Činnosti řidiče zaznamenané ve VU za otvor pro kartu v chronologickém pořádku Blokový identifikátor Datum šetření (kalendářní den výtisku) Stav tachometru v 00:00 a 24:00	----- dd/mm/yyyy x xxx xxx - x xxx xxx km
10.	Činnosti uvedené v otvoru pro kartu S Identifikátor bloku	----- S -----
10.1	<i>Doba po kterou nebyla karta vložena do otvoru pro kartu S</i> Identifikátor záznamu Žádná karta nevložena Stav tachometru na začátku doby	----- --- x xxx xxx km
10.2	<i>Vložení karty</i> Identifikátor záznamu vložení karty Jméno řidiče Křestní jméno řidiče Identifikační karta řidiče Datum ukončení platnosti karty řidiče Registrující členský stát a registrační číslo předtím používaného vozidla Datum a čas vyjmutí karty z předtím používaného vozidla Prázdná řádka Stav tachometru při zasunutí karty, manuální vstup políčka činnosti řidiče (M pokud je, prázdné pokud není)	----- ☐ Last_Name _____ First_Name _____ Card_Identification _____ dd/mm/yyyy A → Nat/VRN _____ dd/mm/yyyy hh:mm x xxx xxx km M
10.3	<i>Činnost</i> Piktogram činnosti, začátek a konec doby trvání (včetně) Stav posádky (piktogram posádky, pokud je, prázdné, pokud je jeden), alespoň jednohodinové doby odpočinku jsou označeny hvězdičkou	A hh:mm hh:mm hh:mm ☐☐ *

10.3a	<i>Specifické podmínky. Čas vstupu, piktogram specifické podmínky (nebo kombinace piktogramů)</i>	hh:mm - - - - pppp - - - -
10.4	<i>Vyjmutí karty nebo konec doby bez použití karty</i> Stav tachometru vozidla při vyjmutí karty nebo na konci doby bez použití karty a ujetá vzdálenost od posledního zasunutí nebo od začátku doby bez použití karty	x xxx xxx km; x xxx km
11.	Denní součet Identifikátor bloku	- - - - - Σ - - - - -
11.1	<i>Součet dob celku ve vozidle bez karty v otvoru pro kartu řidiče</i> Identifikátor bloku	10 - - -
11.2	<i>Součet dob celku ve vozidle bez karty v otvoru pro kartu spolujezdce</i> Identifikátor bloku	20 - - -
11.3	<i>Denní součet celku ve vozidle připadající na řidiče</i> Identifikátor záznamu Příjmení řidiče Křestní jméno (jména) řidiče Identifikační karta řidiče	- - - - - ⊙ Last_Name _____ First_Name _____ Card_Identification _____
11.4	<i>Vstupní místo, kde denní pracovní doba začíná a/nebo končí</i> pi = umístění piktogramu začátku/konce, čas, země, region. Měřič ujeté vzdálenosti	pihh:mm Cou Reg x xxx xxx km
11.5	<i>Celkové činnosti (z karty)</i> Celková doba řízení, ujetá vzdálenost Celková doba práce a dosažitelnosti Celková doba odpočinku a nevyužitelnosti Celková doba činnosti posádky	⊙ hhhmm x xxx km ✱ hhhmm ☐ hhhmm └ hhhmm ? hhhmm ⊙⊙ hhhmm
11.6	<i>Celkové činnosti (v době bez karty v otvoru pro kartu řidiče)</i> Celková doba řízení, ujetá vzdálenost Celková doba práce a dosažitelnosti	⊙ hhhmm x xxx km ✱ hhhmm ☐ hhhmm └ hhhmm

Celková doba odpočinku

- 11.7 *Celkové činnosti (v době bez karty
v otvoru pro kartu spolujezdce)*
Celková doba práce a dosažitelnosti
Celková doba odpočinku

⌘	hh:mm	⌘	hh:mm
⌘	hh:mm		

- 11.8 *Celkové činnosti (na řidiče včetně
obou otvorů pro kartu)*
Celková doba řízení, ujetá vzdálenost
Celková doba řízení, ujetá vzdálenost
Celková doba odpočinku
Celková doba činnosti posádky
Pokud je požadován pro běžný den
denní výtisk denně se vypočítají
součty s dostupnými údaji k času
výtisku

⌘	hh:mm	x	xxx km
⌘	hh:mm	⌘	hh:mm
⌘	hh:mm		
⌘	hh:mm		

12. **Události a/nebo chyby zaznamenané na kartě**

- 12.1 Identifikátor bloku posledních 5
„událostí a chyb“ na kartě
- 12.2 Blokový identifikátor všech
zaznamenaných „událostí“ na kartě
- 12.3 Blokový identifikátor „chyb“ na kartě

-----	! x ⌘	-----
-------	-------	-------

-----	! ⌘	-----
-------	-----	-------

-----	x ⌘	-----
-------	-----	-------

- 12.4 *Záznam událostí a/nebo chyb*
Identifikátor záznamu
Piktogram události/chyby, účel
záznamu, čas startu
Dodatečný kód události/chyby
(pokud je), trvání
Registrující členský stát & VRN
vozidla, v kterém k události nebo
chybě došlo

Pic	dd/mm/yyyy hh:mm
! xxx	hh:mm
⌘ Nat/VRN	_____

13. **Události a/nebo chyby zaznamenané nebo nabíhající ve vozidlové jednotce**

- 13.1 Identifikátor bloku posledních 5
„událostí a chyb“ z VU
- 13.2 Identifikátor bloku všechny
zaznamenané nebo nabíhající
„události“ ve vozidlové jednotce
- 13.3 Identifikátor bloku všechny
zaznamenané nebo nabíhající „chyby“

-----	! x ⌘	-----
-------	-------	-------

-----	! ⌘	-----
-------	-----	-------

-----	x ⌘	-----
-------	-----	-------

ve vozidlové jednotce

13.4 Záznam události a/nebo chyb

Identifikátor záznamu

Piktogram události/chyby, účel záznamu, čas startu

Dodatečný kód události/chyby (pokud je), žádná z podobných události tohoto dne, trvání

Identifikace karet vložených na počátku nebo konci události nebo chyby, až 4 řádky, bez opakování dvojice stejných čísel karty
Případ, kdy nebyla vložena žádná karta

Účel záznamu (p) je numerický kód vysvětlující, kdy byla událost nebo chyba zaznamenána, kódování je v souladu s datovými prvky

UdálostChybaZáznamÚčel

Pic	(p)	dd/mm/yyyy	hh:mm
xxx		(xxx)	hh:mm
Card_Identification _____			
Card_Identification _____			
Card_Identification _____			
Card_Identification _____			
■ ---			

14. Identifikace VU (celku ve vozidle)

Identifikátor bloku

Název výrobce VU

Adresa výrobce VU

Číslo VU

Homologační číslo VU

Výrobní číslo VU

Rok výroby VU

Verze softwaru a datum instalace VU

-----		■	-----	
■	Name	_____		
	Address	_____		
	PartNumber	_____		
	Apprv	_____		
	S/N	_____		
	yyyy	_____		
V	xx.xx.xx	dd/mm/yyyy		

15. Identifikace čidla

Identifikátor bloku

Výrobní číslo čidla

Homologační číslo čidla

Datum první instalace čidla

-----		■	-----	
■	S/N	_____		
	Apprv	_____		
	dd/mm/yyyy	_____		

16. Údaje o kalibraci

Identifikátor bloku

-----		■	-----	
-------	--	---	-------	--

- 16.1 *Kalibrační záznam*
 Identifikátor záznamu
 Organizace, která provedla kalibraci
 Adresa organizace
 Identifikační karta organizace
 Datum platnosti karty organizace
 Prázdný řádek
 Datum kalibrace + účel kalibrace
 VIN
 Registrující členský stát & VRN
 (registrační číslo vozidla)
 Charakteristický koeficient vozidla
 Konstanty záznamového zařízení
 Dynamický obvod pneumatik
 Rozměr použitých pneumatik
 Staré a nové hodnoty měřiče ujeté vzdálenosti
 Účel kalibrace (p) je numerický kód vysvětlující proč byly tyto kalibrační parametry zaznamenány a je zakódován podle datových prvků
 KalibraceÚčel

```

-----
T Workshop_name _____
  Workshop_address _____
Card-Identification _____
  dd/mm/yyyy

T dd/mm/yyyy (p)
A VIN _____
  Nat/VRN _____
w xx xxx Imp/km
k xx xxx Imp/km
l xx xxx mm
• TyreSize _____
> xxx km/h
x xxx xxx - x xxx xxx km

```

- 17 Časové nastavení
 Identifikátor bloku

```

----- @ -----

```

- 17.1 *Časové nastavení záznamu*
 Identifikátor záznamu
 Staré datum a čas
 Nové datum a čas
 Organizace, která provedla časové nastavení
 Adresa organizace
 Identifikační karta organizace
 Datum platnosti karty organizace

```

-----
! @ dd/mm/yyyy hh:mm
@ dd/mm/yyyy hh:mm
T Workshop_name _____
  Workshop_address _____
Card-Identification _____
  dd/mm/yyyy

```

18. **Nejposlednější událost a chyba zaznamenaná ve VU**
 Identifikátor bloku
 Časový údaj nejposlednější události
 Časový údaj nejposlednější chyby

```

----- ! x A -----
! jj/mm/aaaa hh:mm
x jj/mm/aaaa hh:mm

```

19. **Kontrolní informace překročení rychlosti**
 Identifikátor bloku
 Datum a čas poslední KONTROLY PŘEKROČENÍ RYCHLOSTI
 Datum/čas prvního překročení rychlosti a počet překročení rychlosti od té doby

```

----- >> -----
> @ dd/mm/yyyy hh:mm
>> dd/mm/yyyy hh:mm (nnn)

```


20. Záznam překročení rychlosti

20.1 Identifikátor bloku „První překročení rychlosti po poslední kalibraci“

----- >>↑ -----

20.2 Identifikátor bloku „5 nejvýznamnějších překročení v posledních 365 dnech“

----- >>(365) -----

20.3 Identifikátor bloku „Nejvýznamnější z událostí v posledních 10 dnech“

----- >>(10) -----

20.4 Identifikátor záznamu
Časový údaj a trvání
Maximální a průměrné rychlosti.
Žádné z podobných událostí tento den
Příjmení řidiče
Křestní jméno (jména) řidiče
Identifikační karta řidiče

```
-----
>> dd/mm/yyyy hh:mm hh:mm
    xxx km/h xxx km/h (xxx)
☐ Last_Name _____
  First_Name _____
Card_Identification _____
```

20.5 Pokud není v bloku žádný záznam o překročení rychlosti

>> ---

21. Informace psané rukou

Identifikátor bloku

21.1 Kontrolní místo

21.2 Podpis kontrolora

21.3 Počáteční čas

21.4 Konečný čas

21.5 Podpis řidiče

```
-----
☐ * .....
☐ .....
☐ + .....
+ ☐ .....
☐ .....
```

„Rukou psané informace“ Vložit dost prázdných řádků nad rukou psaný článek, aby bylo skutečně možné napsat požadované informace nebo se podepsat

3. SPECIFIKACE VÝTISKU

V této kapitole byly použity následující smluvené znaky:

N	Tisk bloku nebo záznamu čísla N
N	Tisk bloku nebo záznamu čísla N dle potřeby opakovaný
X/Y	Tisk bloků nebo záznamů X a/nebo Y dle potřeby a dle nutnosti opakovaný

3.1 Činnosti řidiče na výpisu denní karty

PRT 007 Činnosti řidiče na výpisu denní karty musí mít následující tvar

1	Datum a čas, kdy byl dokument vytištěn
2	Typ výtisku
3	Identifikace kontrolora (pokud je kontrolní karta vložena ve VU)
3	Identifikace řidiče (z výtisku karty)
4	Identifikace vozidla (vozidla, z něhož byl výtisk získán)
5	Identifikace VU (VU, z níž byl výtisk získán)
6	Poslední kalibrace této VU
7	Poslední kontrola sledovaného řidiče byla vystavena k
8	Vymezení činností řidiče
8.1a/8.1b/8.1c/8.2/8.3/8.3a/8.4	Činnosti řidiče podle sledu událostí
11	Vymezení denního počtu
11.4	Místa vstupů v časovém sledu
11.5	Celkové činnosti
12.1	Události a chyby podle vymezení karty
12.4	Záznamy událostí/chyb (Posledních 5 událostí/chyb zaznamenaných na kartě)
13.1	Události a chyby podle vymezení VU
13.4	Záznamy událostí/chyb (Posledních 5 událostí/chyb zaznamenaných nebo vzniklých ve VU)
21.1	Místo kontroly
21.2	Podpis kontrolora
21.5	Podpis řidiče

3.2 Činnosti řidiče na denním výpisu VU

PRT 008 Činnosti řidiče na denním výpisu musí mít následující tvar

1	Datum a čas, kdy byl dokument vytištěn
2	Typ výtisku
3	Identifikace držitele karty (všech karet vložených do VU)
4	Identifikace vozidla (vozidla, z něhož byl výtisk získán)
5	Identifikace VU (VU, z níž byl výtisk získán)
6	Poslední kalibrace této VU
7	Poslední kontrola tohoto záznamového zařízení
9	Vymezení činností řidiče
10	Vymezení otvoru pro kartu řidiče (slot I)
10.1/10.2/10.3/10.3a/10.4	Činnosti v časovém sledu (slot řidiče)
10	Vymezení otvoru pro kartu spolujezdce (slot2)
10.1/10.2/10.3/10.3a/10.4	Činnosti v časovém sledu (slot druhého řidiče)
11	Vymezení denního počtu
11.1	Počet období bez karty v otvoru pro kartu řidiče
11.4	Místa vstupů v časovém sledu

11.6	Celkové činnosti
11.2	Počet období bez karty v otvoru pro kartu spolujezdce
11.4	Místa vstupů v časovém sledu
11.7	Celkové činnosti
11.3	Počet činností pro oba otvory pro karty řidiče
11.4	Místa vstupů řidičem v časovém sledu
11.7	Celkové činnosti pro tohoto řidiče
13.1	Vymezení událostí/chyb
13.4	Záznamy událostí/chyb (Posledních 5 událostí/chyb zaznamenaných nebo vzniklých ve VU)
21.1	Místo kontroly
21.2	Podpis kontrolora
21.3	Počáteční čas
21.4	Konečný čas
21.5	Podpis řidiče

3.3 Události a chyby z výtisku karty

PRT 009 Události a chyby na výtisku karty musí mít následující tvar

1	Datum a čas, kdy byl dokument vytištěn
2	Typ výtisku
3	Identifikace kontrolora (pokud je kontrolní karta vložena ve VU)
3	Identifikace řidiče (z výtisku karty)
4	Identifikace vozidla (vozidla, z něhož byl výtisk získán)
12.2	Vymezení událostí
12.4	Záznamy událostí (všechny události zaznamenané na kartě)
12.3	Vymezení chyb
12.4	Záznamy chyb (všechny chyby zaznamenané na kartě)
21.1	Místo kontroly
21.2	Podpis kontrolora
21.5	Podpis řidiče

3.4 Události a chyby z výpisu VU

PRT 010 Události a chyby na výpisu VU musí mít následující tvar

1	Datum a čas, kdy byl dokument vytištěn
2	Typ výtisku
3	Identifikace držitele karty (všech karet vložených do VU)
4	Identifikace vozidla (vozidla, z něhož byl výtisk získán)
13.2	Vymezení událostí
13.4	Záznamy událostí (všechny události zaznamenané nebo vzniklé ve VU)
13.3	Vymezení chyb
13.4	Záznamy chyb (všechny chyby zaznamenané nebo vzniklé ve

	VU)
21.1	Místo kontroly
21.2	Podpis kontrolora
21.5	Podpis řidiče

3.5 Události a chyby z výpisu VU

PRT 011 Technická data výtisku musí mít následující tvar

1	Datum a čas, kdy byl dokument vytištěn
2	Typ výtisku
3	Identifikace držitele karty (všech karet vložených do VU)
4	Identifikace vozidla (vozidla, z něhož byl výtisk získán)
14	Identifikace VU
15	Identifikace čidla
16	Vymezení kalibračních údajů
16.1	Záznamy o kalibraci (všechny dosažitelné záznamy v časovém sledu)
17	Vymezení časového nastavení
17.1	Záznamy časového nastavení (všechny dosažitelné záznamy z časového nastavení a z kalibračních záznamů)
18	Nejposlednější událost nebo chyba zaznamenaná ve VU

3.6 Výtisk překročení povolené rychlosti

PRT 012 Výtisk překročení povolené rychlosti musí mít následující tvar

1	Datum a čas, kdy byl dokument vytištěn
2	Typ výtisku
3	Identifikace držitele karty (všech karet vložených do VU)
4	Identifikace vozidla (vozidla, z něhož byl výtisk získán)
19	Informace o kontrole překročení povolené rychlosti
20.1	Identifikátor údajů o překročení povolené rychlosti
20.4/20.5	První překročení povolené rychlosti po poslední kalibraci
20.2	Identifikátor údajů o překročení povolené rychlosti
20.4/20.5	5 nejzávažnějších překročení povolené rychlosti v posledních 365 dnech
20.3	Identifikátor údajů o překročení povolené rychlosti
20.4/20.5	Nejzávažnější překročení povolené rychlosti, které se vyskytlo v každém z posledních 10 dnů
21.1	Místo kontroly
21.2	Podpis kontrolora
21.5	Podpis řidiče

PŘÍLOHA 5

DISPLEJ

V této příloze se musí užít následující formát

- znaky vytištěné **tučně** znamenají jednoduchý text uvedený na displeji (to co zůstává na displeji je normálními znaky),
- normální znaky označují proměnné (piktogramy nebo údaje), pro zobrazení na displeji jsou nahrazeny svými hodnotami,

dd mm yyyy: den, měsíc, rok

hh: hodiny




mm: minuty

D: piktogram trvání

EF: kombinace piktogramů událostí a chyb

O: piktogram druhu činnosti

DIS 001 Záznamové zařízení musí zobrazovat na displeji data v následujícím tvaru

Data	Format
Chybové zobrazení	
Místní čas	hh : mm
Druh činnosti	o
Informace o řidiči	1 Dhmm hhmm
Informace o druhém řidiči	2 Dhhmm
Mimo rozsah podmínek	OUT
Varovná zobrazení	
Překročení průběžné doby řízení	1  hhmm hhmm
Událost nebo chyba	EF
Další zobrazení	
UTC data	UTC  dd/mm/yyyy nebo
čas	UTC  dd.mm.yyyy hh:mm

Doba nepřetržitého řízení řidiče a nasbíraný čas přestávky	1 ☉ hh <h>mm ■■ hh<h>mm</h></h>
Doba nepřetržitého řízení druhého řidiče a nasbíraný čas přestávky	2 ☉ hh <h>mm ■■ hh<h>mm</h></h>
Doba nepřetržitého řízení řidiče v předchozím a probíhajícím týdnu	1 ☉ ■■ hh <h>mm</h>
Doba nepřetržitého řízení druhého řidiče v předchozím a probíhajícím týdnu	2 ☉ ■■ hh <h>mm</h>

PŘÍLOHA 6

VNĚJŠÍ INTERFACE

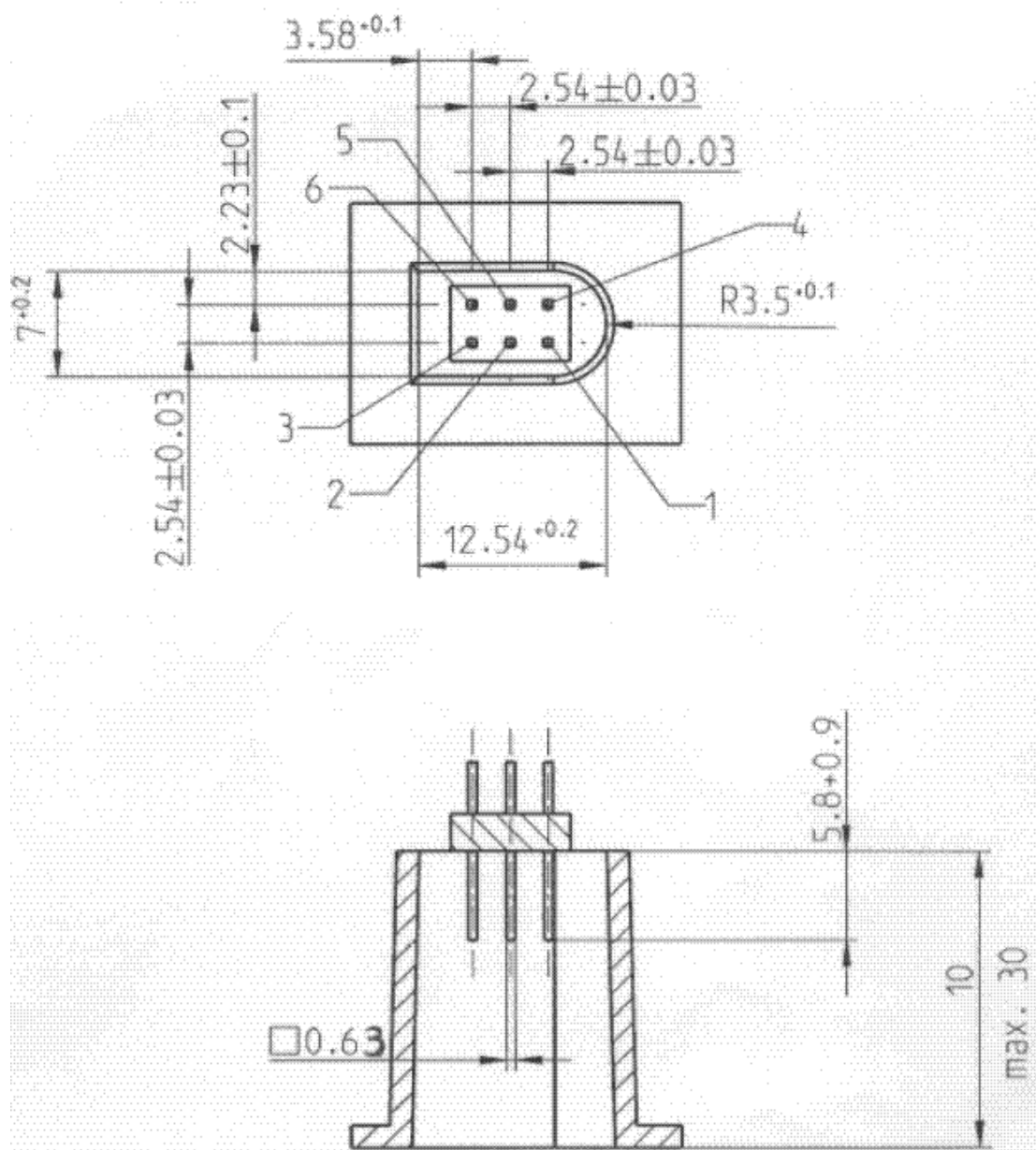
OBSAH

1. HARDWARE	208
1.1 Konektor.....	208
1.2 Propojení kontaktů	210
1.3 Blokové schéma	210
2. INTERFACE STAŽENÍ DAT	211
3. INTERFACE KALIBRACE.....	211

1. HARDWARE

1.1 Konektor

INT 001 Konektor pro stažení dat / kalibraci musí být šesti kolíkový, přístupný na předním panelu bez nutnosti odpojení jakékoli části záznamového zařízení a odpovídat následujícímu výkresu (všechny rozměry jsou uvedeny v milimetrech):



Následující obrázek znázorňuje typickou šestikolíkovou zástrčku.

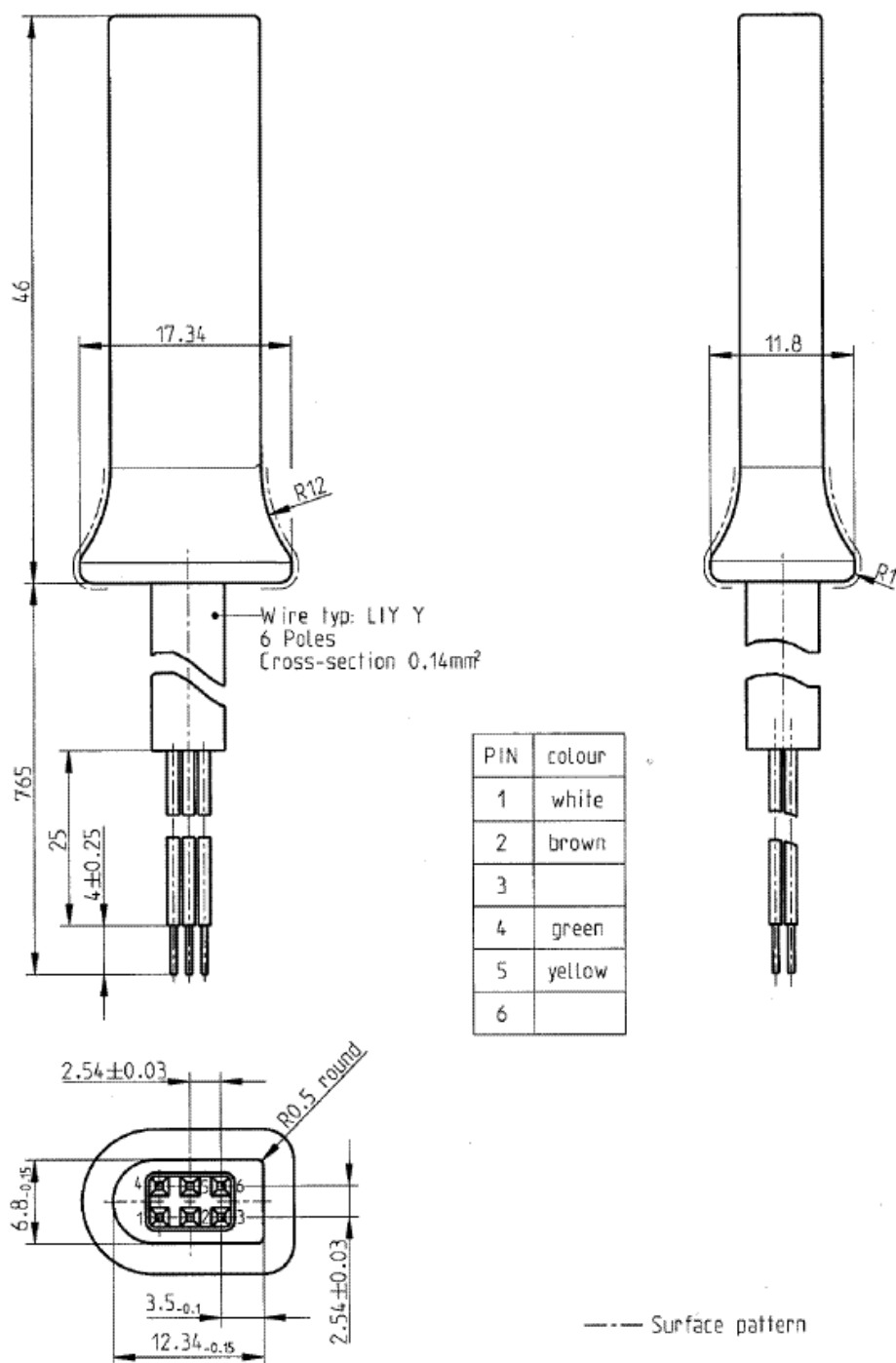
Wire typ – Typ vodiče

6 Poles – 6 pólů

Cross-section – průřez

Kolík	Barva
1	bílá
2	hnědá
3	
4	zelená
5	žlutá
6	

Surface pattern – Čelní pohled



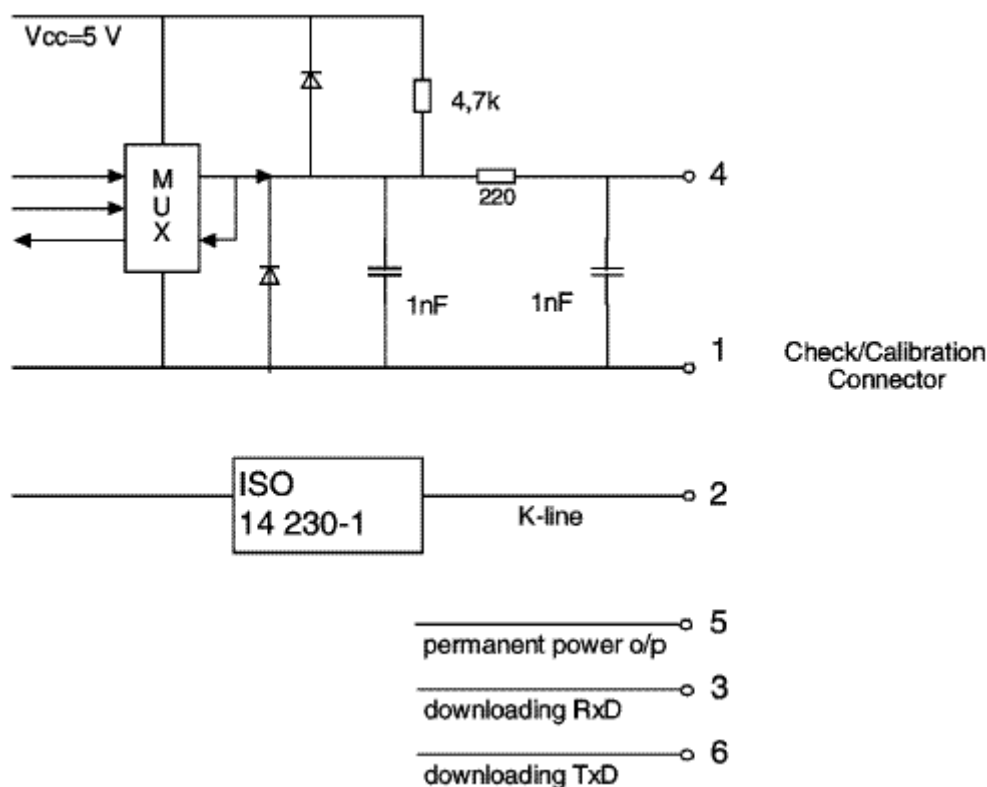
1.2 Propojení kontaktů

INT 002 Kontakty musí být připojeny podle následující tabulky:

Kolík	Popis	Poznámka
1	Záporný pól baterie	Připojení na záporný pól baterie vozidla
2	Propojení dat	K – připojení (ISO 14 230-1)
3	RxD – Stahování dat	Vstup dat do záznamového zařízení
4	Vstupní/výstupní signál	Kalibrace
5	Stálý výkonový výstup	Rozsah napětí je určen tak, aby byl napětím vozidla minus 3V poklesu napětí na ochranném obvodu Výstup 40mA
6	TxD – Stahování dat	Výstup dat ze záznamového zařízení

1.3 Blokové schéma

INT 003 Blokové schéma se musí shodovat s následujícím:



Check/Calibration connector – Kontrolní/Kalibrační konektor

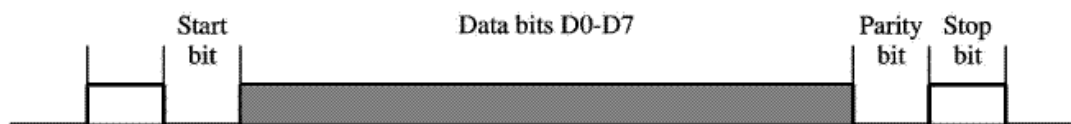
permanent power – stálé připojení

downloading – stahování dat

2. INTERFACE STAŽENÍ DAT

INT 004 Interface stažení dat musí splňovat specifikaci RS232

INT 005 Interface stažení dat musí použít jeden spouštěcí bit, 8 datových bitů LSB, jeden rovný stejný a 1 koncový bit.



Uspořádání datových bitů

Spouštěcí bit: jeden bit s logickou hladinou 0

Datové bity: přenášeny s LSB

Stejný bit: rovný stejný

Koncový bit: jeden bit s logickou hladinou 1

Když jsou přenášena numerická data vytvořená více než jedním bytem, většina důležitých bytů je přenesena nejdříve a následně jsou přenášeny nejméně důležité byty.

INT 006 Přenosová rychlost musí být nastavitelná od 9600 bps do 115200 bps. Přenos musí být uskutečnitelný při nejvyšší možných přenosových rychlostech, počáteční rychlost po začátku komunikace se nastaví na 9600 bps.

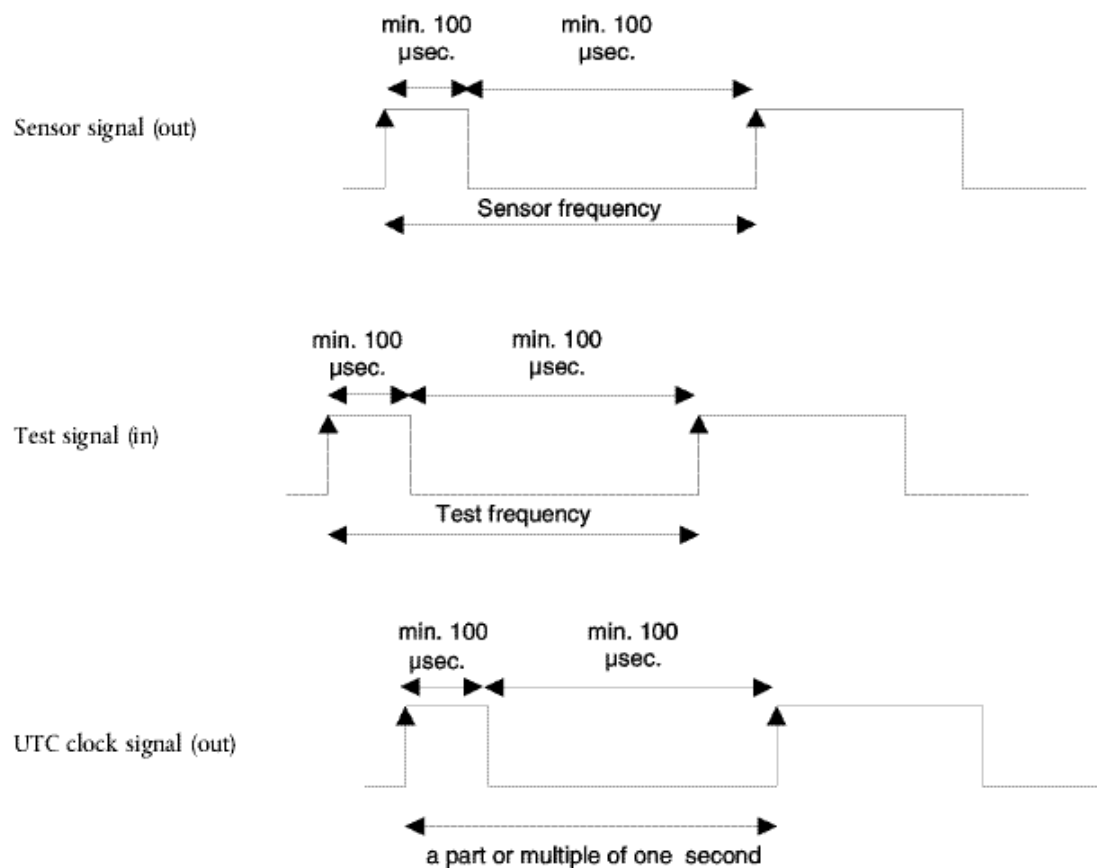
3. INTERFACE KALIBRACE

INT 007 Datová komunikace musí splňovat ISO 14230-1 Silniční vozidla – Diagnostické systémy – protokol klíčového slova 2000 – Část 1: Physical layer, První vydání 1999

INT 008 Vstupní/výstupní signál musí splňovat následující specifikace:

Parametr	Minimální	Typický	Maximální	Poznámka
U_N (vstupní)			1,0 V	$I = 750 \mu A$
U_V (vstupní)	4 V			$I = 200 \mu A$
Kmitočet			4 kHz	
U_N (vstupní)			1,0 V	$I = 1 \text{ mA}$
U_V (výstupní)	4 V			$I = 1 \text{ mA}$

INT 009 Vstupní/výstupní signál musí splňovat následující časový diagram:



Signál z čidla (výstupní)

Sensor frequency – Kmitočet čidla

Zkušební signál (vstupní)

Test frequency – Zkušební kmitočet

UTC časový signál (výstupní)

a part or multiple of one second – část nebo násobek jedné vteřiny

PŘÍLOHA 7

PROTOKOLY STAŽENÍ DAT

OBSAH

1.	ÚVOD	215
1.1	Rozsah platnosti	215
1.2	Zkratky a označování	215
2.	STAŽENÍ DAT CELKU VE VOZIDLE (VU)	216
2.1	Postup stahování	216
2.2	Protokol stažení dat	216
2.2.1	Struktura zprávy	216
2.2.2	Typy zpráv	218
2.2.2.1	Požadavek na začátek spojení (SID 81)	219
2.2.2.2	Kladná odezva na začátek spojení (SID C1)	220
2.2.2.3	Požadavek na spuštění diagnostiky (SID 10)	220
2.2.2.4	Kladná odezva na spuštění diagnostiky (SID 50)	220
2.2.2.5	Funkce řízení spojení (SID 87)	220
2.2.2.6	Kladná odezva na řízení spojení (SID C7)	220
2.2.2.7	Požadavek na odeslání dat (SID 35)	220
2.2.2.8	Kladná odezva na požadavek odeslání dat (SID 75)	220
2.2.2.9	Požadavek na přenos dat SID 36)	221
2.2.2.10	Kladná odezva na přenos dat (SID 76)	221
2.2.2.11	Požadavek na ukončení přenosu (SID 77)	222
2.2.2.12	Kladná odezva na požadavek na ukončení přenosu (SID 77)	222
2.2.2.13	Požadavek na ukončení spojení (SID 82)	222
2.2.2.14	Kladná odezva na ukončení spojení (SID C2)	222
2.2.2.15	Potvrzení příjmu dílčí zprávy	222
2.2.2.16	Záporná odezva (SID 7F)	222
2.2.3	Tok zprávy	224
2.2.4	Časování	224
2.2.5	Chybná obsluha	226
2.2.5.1	Fáze začátku spojení	226
2.2.5.2	Fáze spojení	226
2.2.6	Obsah zprávy s odezvou	228

2.2.6.1	Přehled přenášených dat kladné odezvy	229
2.2.6.2	Kladná odezva na činnost přenosu dat.....	230
2.2.6.3	Kladná odezva přenosu dat událostí a závad	232
2.2.6.4	Kladná odezva přenosu dat detailních rychlostí	233
2.2.6.5	Kladná odezva přenosu dat detailních rychlostí	234
2.3	ESM paměť souboru	234
3.	PROTOKOL O STAŽENÍ DAT KARET TACHOGRAFU.....	235
3.1	Přehled.....	235
3.2.	Definice	235
3.3.1	Souslednost při inicializace	236
3.3.2	Souslednost při neoznačených souborech dat.....	236
3.3.3	Souslednost při označených souborech dat	236
3.3.4	Souslednost při resetování kalibračního počítadla.....	238
3.4	Formát uložených dat	238
3.4.1	Úvod	238
3.4.2	Formát souboru	238
4.	STAHOVÁNÍ DAT KARTY TACHOGRAFU PŘES CELEK VE VOZIDLE	239

1. ÚVOD

Tato příloha určuje postup pro uložení různých typů stažených dat na vnější paměťové médium dohromady s protokoly. Toto uložení musí být proveditelné, aby se zajistil správný přenos dat a plná slučitelnost formátu stažených dat, aby umožnilo kontrolorovi prozkoumání těchto dat a umožnilo kontrolu jejich autenticity a úplnosti před analyzováním.

1.1 Rozsah platnosti

Data se smí stáhnout na ESM

- z jednotky vozidla inteligentním zařízením (IDE) připojeným k VU
- z karty tachografu přes IDE vybaveným kartovým interfacem (IFD)
- z karty tachografu přes jednotku vozidla a IDE připojeným k VU

Pro možnost ověřit autenticitu a úplnost stažených dat uložených na ESM data jsou stažena s přiloženým podpisem v souladu s Přílohou 11 Běžné bezpečnostní postupy. Identifikaci zdrojového zařízení (VU nebo karta) a jeho bezpečnostní potvrzení (Členský stát a zařízení) se též stáhnou. Ověřovatel dat musí mít nezávisle v držení důvěrný veřejný evropský klíč.

DDP 001 Stažená data během jednoho stahování být zapamatována v ESM v jednom filu.

1.2 Zkratky a označování

V příloze jsou použity následující zkratky

AID	Identifikátor aplikace
ATR	Odpověď pro opětné spuštění
CS	Byte kontroly obsahu
DF	Přiřazený file
DS	Diagnostika
EF	Základní file
ESM	Vnější nosič pro uložení
FID	Identifikátor filu (File ID)
FMT	Formát bytu (první byte hlavičky zprávy)
ICC	Karta integrovaného obvodu
IDE	Inteligentní zařízení: Zařízení používané k stažení dat do ESM (na. př. osobní počítač)
IFD	Interface
KWP	Protokol klíčového slova 2000
LEN	Délkový bytu (poslední byte hlavičky zprávy)
PPS	Výběr parametrů prokolu
PSO	Provedení bezpečné činnosti
SID	Identifikátor servisu
SRC	Zdrojový byte

TGT	Cílový byte (byte označující konec)
TLV	Hodnota délky štítku
TREP	Parametr odezvy přenosu
TRTP	Parametr aplikace přenosu
VU	Jednotka vozidla

2. STAŽENÍ DAT CELKU VE VOZIDLE (VU)

2.1 Postup stahování

Aby se provedlo stažení dat VU, musí operátor provést následující činnosti:

- vsunout svou kartu tachografu do kartového slotu VU¹⁷
- připojit IDE ke konektoru VU určenému pro stahování
- zařídit spojení mezi IDE a VU
- vybrat na IDE data ke stažení a poslat požadavek do VU
- uzavřít stahování

2.2 Protokol stažení dat

Struktura protokolu je způsobem pán-otrok, kdy IDE hraje roli pána VU roli otroka

Struktura zprávy, typy a tok jsou v principu založeny na Protokolu klíčového slova 2000(KWP) (ISO 14230-2 Silniční vozidla – Diagnostické systémy - Protokol klíčového slova 2000 – Část 2: Vrstva spojení dat)

Vrstva aplikace je v principu založena na projednávaném návrhu ISO 14229-1 (Silniční vozidla – Diagnostické systémy – Část 1: Diagnostické servisy, verze 6 z 22. února 2001).

2.2.1 Struktura zprávy

DDP 002 Všechny vyměněné zprávy mezi IDE a VU jsou formátovány ve struktuře sestávající ze tří částí:

- hlavička sestává z bytového formátu (FMT), cílového bytu (TGT), zdrojového bytu, délkového bytu (LEN)
- datové pole sestává z bytu servisního identifikátoru (SID) a různého počtu datových bytů, které mohou obsahovat dle přání byte diagnostiky nebo nezávazný byte přenosového parametru TRTP nebo TREP).
- Kontrolní součet sestává z bytu kontroly součtu (CS)

¹⁷ Vložená karta spustí příslušná přístupová práva k funkci stažení dat a k datům.

Hlavička				Datové pole					Kontrola počtu
FMT	TGT	SRC	LEN	SID	Data	CS
4 Byty				Max 225 bytů					1 byte

TGT a SRC byte zastupuje fyzickou adresu příjemce a původce zprávy. Hodnoty jsou F0 Hex pro IDE a EE Hex pro VU.

Byte LEN je délka části datového pole.

Byte kontroly počtu je série 256 osmibitových modulů ze všech bytů zprávy vyjma samotného CS.

FMT, SID, DS, TRTP a TREP byty jsou definovány dále v tomto dokumentu.

DDP 003 V případě, že dat kterých má být přeneseno zprávou je víc než získatelný prostor v části datového pole, zpráva je aktuálně poslána v několika částech. Každá část nese hlavičku, stejný SID, TREP a 2 byty počítadla zpráv ukazujícího číslo dílčí zprávy v celkové zprávě. Aby bylo umožněno ověření chyb a ztrát, IDE potvrdí každou dílčí zprávu. IDE může přijmout dílčí zprávu, požádat o to aby byla znovu přenesena, žádat VU o opětovný start nebo o ztracený přenos.

DDP 004 Jestliže poslední část zprávy obsahuje přesně 255 bytů z datového pole, musí se koncová část s prázdným (vyjma SID TREP a počítadla částí) datovým polem připojit, aby se označil konec zprávy.

Příklad:

Hlavička	SID	TREP	Zpráva	CS
4 byty	Delší než 255 Bytů			

Přeneso se jako:

Hlavička	SID	TREP	00	01	Část 1	CS
4 byty	255 Bytů					

Hlavička	SID	TREP	00	01	Část 2	CS
4 byty	255 Bytů					

Hlavička	SID	TREP	xx	yy	Část n	CS
4 byty	Méně než 255 Bytů					

nebo jako

Hlavička	SID	TREP	00	01	Část 1	CS
4 byty	255 Bytů					

Hlavička	SID	TREP	00	01	Část 2	CS
4 byty	255 Bytů					

Hlavička	SID	TREP	xx	yy	Část n	CS
4 byty	255 Bytů					

Hlavička	SID	TREP	xx	yy + 1	CS
4 byty	4 byty				

2.2.2 Typy zpráv

Zápis z přenosu při stahování dat mezi VU a IDE požaduje změnu osmi různých typů zpráv.

Následující tabulka uvádí přehled těchto zpráv

Struktura zprávy IDE-> -VU	Minimálně 4 byty Hlavička				Max. 255 bytů Data			1 byte kontrola počtu
	FMT	TGT	SRC	LEN	SID	DS TRTP	DATA	CS
Požadavek začátku spojení	81	EE	F0		81			E0
Kladná odezva na začátek spojení	80	F0	EE	03	C1		SF,EA	9B
Požadavek na spuštění diagnostiky	80	EE	F0	02	10	81		F1
Kladná odezva na spuštění diagnostiky	80	F0	EE	02	50	81		31
Funkce řízení spojení Ověření rychlosti přenosu v baudech (stav 1)								
9 600 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
Kladná odezva ověření rychlosti přenosu	80	FO	EE	02	C7		01	28
Změna rychlosti přenosu (stav 2)	80	EE	FO	03	87		02,03	ED
Požadavek odeslání dat	80	EE	FO	OA	35		00,00,00, 00,00,FF, FF,FF,FF	99
Kladná odezva na požadavek odeslání dat	80	FO	EE	03	75		00,FF	D5
Požadavek na převod dat								
Přehled	80	EE	FO	02	36	01		97
Činnosti	80	EE	FO	06	36	02	Datum	CS
Události a chyby	80	EE	FO	02	36	03		99
Rychlosti podrobně	80	EE	FO	02	36	04		9A
Technická data	80	EE	FO	02	36	05		9B
Karta stažení dat	80	EE	FO	02	36	06		9C
Kladná odezva na přenos dat	80	FO	EE	Len	76	TREP	Data	CS
Požadavek na ukončení přenosu	80	EE	FO	01	37			96
Kladná odezva na požadavek ukončení	80	FO	EE	01	77			D6
Požadavek na ukončení spojení	80	EE	FO	01	82			E1
Kladná odezva na požadavek ukončení	80	FO	EE	01	C2			21
Potvrzení přijetí dílčí zprávy	80	EE	FO	Len	83		Data	CS
Záporné odezvy								
Úplné odmítnutí	80	FO	EE	03	7F	Sid Req	10	CS
Služba nepodpořena	80	FO	EE	03	7F	Sid Req	11	CS
Dílčí funkce nepodpořena	80	FO	EE	03	7F	Sid Req	12	CS
Nesprávná délka zprávy	80	FO	EE	03	7F	Sid Req	13	CS
Nesprávné podmínky nebo chybný požadavek úseku	80	FO	EE	03	7F	Sid Req	22	CS
Požadavek mimo rozsah	80	FO	EE	03	7F	Sid Req	31	CS
Odeslání neakceptováno	80	FO	EE	03	7F	Sid Req	50	CS
Nevyřízená odezva	80	FO	EE	03	7F	Sid Req	78	CS
Nedosažitelná data	80	FO	EE	03	7F	Sid Req	FA	CS

Poznámky:

Sid Req = Sid souhlasného požadavku

TREP = TRTP souhlasného požadavku

Tmavá buňka znamená, že se nic nepřenáší

Termín odeslání dat (jak je vidět z IDE) se používá z důvodu shodnosti s ISO 14229. To znamená totéž jako stažení dat (jak je vidět z VU).

Možná okénka 2-bytové dílčí zprávy nejsou v tabulce uvedena

2.2.2.1 Požadavek na začátek spojení (SID 81)

DDP 005 Tuto zprávu vydá IDE, aby zajistila spojení s VU. Počáteční spojení vždy probíhají na 9600 baudech (až do doby případné změny rychlosti přenosu vhodnou funkcí řízení spojení)

2.2.2.2 Kladná odezva na začátek spojení (SID C1)

DDP 006 Tato zpráva je vydána celkem ve vozidle, aby kladně odpověděl na požadavek začátku spojení. Obsahuje 2 klíčové byty „8F“ „EA“ potvrzující, že VU podporuje protokol s hlavičkou včetně cílového zdroje a délky informace

2.2.2.3 Požadavek na spuštění diagnostiky (SID 10)

DDP 007 Zprávu o požadavku na spuštění diagnostiky vydává IDE, aby požádala o novou diagnostiku VU. Dílčí funkce „chyba“ (81 Hex) indikuje otevření standardní diagnostiky.

2.2.2.4 Kladná odezva na spuštění diagnostiky (SID 50)

DDP 008 Zprávu o kladné odezvě na spuštění diagnostiky posílá VU, aby kladně odpověděl na požadavek o diagnostiku.

2.2.2.5 Funkce řízení spojení (SID 87)

DDP 052 Funkci řízení spojení použije IDE, aby vyvolala změnu rychlosti přenosu v baudech. To probíhá ve dvou krocích. V kroku jedna IDE navrhne změnu rychlosti přenosu v baudech, jejichž počet ukazuje novou rychlost. Na základě kladné zprávy od VU, IDE odešle potvrzení o změně rychlosti přenosu v baudech do VU (krok dvě). IDE pak provede změnu. Po obdržení potvrzení VU přejde na novou rychlost přenosu.

2.2.2.6 Kladná odezva na řízení spojení (SID C7)

DDP 053 Kladnou odezvu na řízení spojení vydává VU, aby kladně odpověděl na požadavek funkce řízení spojení (krok jedna). Poznamenejme, že žádná odezva se nedává, aby potvrdila požadavek (krok dvě).

2.2.2.7 Požadavek na odeslání dat (SID 35)

DDP 009 Zprávu o požadavku na odeslání dat vydává IDE, aby uvedla VU, že je požadována činnost stahování dat. Pro splnění požadavků ISO14229 data jsou včetně adresy, velikosti a podrobností formátu pro požadovaná data. Tyto nejsou před svým stažením do IDE známy, adresa paměti je nastavena na 0, formát je nešifrovaný a nekomprimovaný a velikost paměti je nastavena na maximum.

2.2.2.8 Kladná odezva na požadavek odeslání dat (SID 75)

DDP 10 Zprávu o kladné odezvě na požadavek odeslání dat posílá VU, aby ukázal IDE, že VU je připravena stáhnout data. Pro splnění požadavků ISO 14229 data obsažená v této zprávě o kladné odezvě ukazují IDE, že příští zprávy o kladné odezvě na přenos dat budou obsahovat maximálně 00FF hex bytů.

2.2.2.9. Požadavek na přenos dat SID 36)

DDP 011 Zprávu o požadavku na přenos dat posílá IDE, aby uvedla VU typ dat, která budou stahována. Jedno bytový přenosový požadavkový parametr (TRTP) ukazuje typ přenosu.

Existuje šest typů přenosu dat:

- přehled (TRTP 01)
- činnosti určitých dat (TRTP 02)
- události a chyby (TRTP 03)
- podrobné rychlosti (TRTP 04)
- technická data (TRTP 05)
- karta stažení dat (TRTP 06)

DDP 054 Pro IDE je povinné žádat přehled přenosu dat (TRTP 01) během stahování dat, aby se zajistilo, že certifikáty VU jsou zaznamenány během stahování datových souborů (a umožnilo ověření digitálního podpisu).

V druhém případě (TRTP 02) zpráva o požadavku stažení dat obsahuje, aby byla stažena data označení kalendářního dne `TimeReal` formát

2.2.2.10 Kladná odezva na přenos dat (SID 76)

DDP 012 Kladnou odezvu na přenos dat posílá VU v odezvě na požadavek přenosu dat. Zpráva obsahuje požadovaná data s parametrem odezvy přenosu (TREP), který se shoduje s TRTP požadavku.

DDP 055 V prvním případě (TREP 01), VU pošle data pomáhající operátoru IDE vybrat data, která chce dále stáhnout. Informace obsažené v této zprávě jsou:

- certifikace bezpečnosti
- identifikace vozidla
- běžná data VU a čas
- minimální a maximální datum stažitelnosti dat (dat VU)
- indikace přítomnosti karet ve VU
- předešlé stažení dat do společnosti
- zámky společnosti
- předešlé kontroly

2.2.2.11 Požadavek na ukončení přenosu (SID 77)

DDP 013 Zprávu o požadavku na ukončení přenosu zasílá IDE, aby sdělila VU, že stažení dat je ukončeno.

2.2.2.12 Kladná odezva na požadavek na ukončení přenosu (SID 77)

DDP 014 Zprávu o kladné odezvě na požadavek na ukončení přenosu posílá VU, aby potvrdil příjem požadavku na ukončení přenosu

2.2.2.13 Požadavek na ukončení spojení (SID 82)

DDP 015 Zprávu o požadavku na ukončení spojení zasílá IDE, aby přerušila spojení s VU

2.2.2.14 Kladná odezva na ukončení spojení (SID C2)

DDP 016 Zprávu o kladné odezvě na ukončení spojení zasílá VU, aby potvrdila příjem požadavku na ukončení spojení.

2.2.2.15 Potvrzení příjmu dílčí zprávy

DDP 017 Potvrzení příjmu dílčí zprávy zasílá IDE, aby potvrdila stvrzenku každé části zprávy, která byla přenesena jako několik dílčích zpráv. Datové pole obsahuje SID obdržené od VU následující dvou bytové kódy:

- MagC + 1 Potvrzení příjmu správné stvrzenky o počtu dílčích zpráv MagC

Požadavek od IDE na VU, aby poslal další dílčí zprávu

- MagC značí problém se stvrzenkou počtu dílčích zpráv MagC

Požadavek od IDE na VU, aby poslal dílčí zprávu znovu.

- FFFFpožadují ukončení zprávy

Toto může použít IDE, aby z nějakých důvodů ukončila přenos zpráv VU.

Příjem poslední dílčí zprávy ze zprávy (LEN byte < 255) může být potvrzen některým z těchto kódů nebo nepotvrzen.

Odezvy VU, které se budou skládat z několika dílčích zpráv jsou:

- kladná odezva na přenos dat (SID 76)

2.2.2.16 Záporná odezva (SID 7F)

DDP 018 Zprávu o záporné odezvě zasílá VU v odezvě na výše požadované zprávy, kdy VU nemůže uspokojit požadavek. Datové pole zprávy obsahuje SID odezvy (7F), SID požadavku a kód, který určuje důvody negativní odezvy..K dispozici jsou následující kódy:

- 10 úplné odmítnutí
Akce nemůže být provedena z důvodů níže neuvedených
- 11 služba nepodpořena
Nebylo porozuměno SID požadavku
- 12 dílčí funkce nepodpořena
Nebylo porozuměno DS nebo TRTP požadavku nebo žádné další dílčí zprávy nebudou přenášeny
- 13 nesprávná délka zpravy
Délka obdržené zprávy je špatná
- 22 nesprávné podmínky nebo chyba požadavkového úseku
Požadovaná služba není v činnosti nebo je nesprávný úsek požadovaných zpráv
- 31 požadavek je mimo rozsah
Záznam parametru požadavku (datové pole) je neplatný
- 50 odeslání dat nebylo přijato
Požadavek nemůže být proveden (VU je v nevhodném modu činnosti nebo má VU vnitřní chybu)
- 78 nevyřízená odezva
Požadovaná akce nemůže být dokončena v čas a VU není připraven přijmout další požadavek
- FA data nejsou k dispozici
Datový objekt požadavku přenosu dat není k dispozici ve VU (na př. není vložena žádná karta, ...)

2.2.3 Tok zprávy

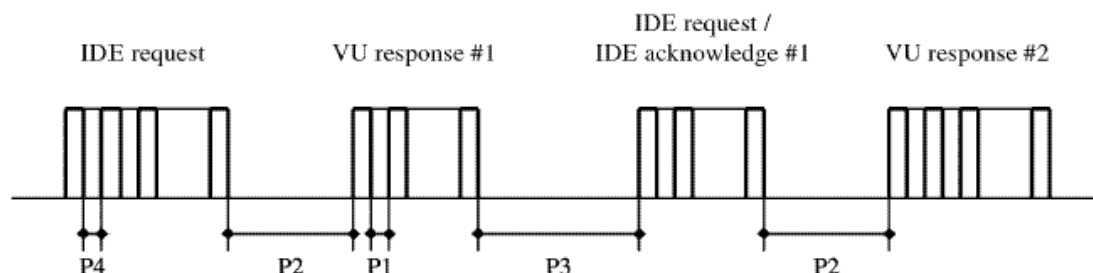
Typický tok zprávy během normálního postupu stahování dat je následující:

IDE		IE
Požadavek na začátek spojení	⇒ ⇐	Kladná odezva
Požadavek na začátek diagnostiky	⇒ ⇐	Kladná odezva
Požadavek na odeslání dat	⇒ ⇐	Kladná odezva
Požadavek na přehled přenášených dat	⇒ ⇐	Kladná odezva na přenos
Požadavek dat #2	⇒ ⇐	Kladná odezva #1
Potvrzení přijetí dílčí zprávy #1	⇒ ⇐	Kladná odezva #2
Potvrzení přijetí dílčí zprávy #2	⇒ ⇐	Kladná odezva #m
Potvrzení přijetí dílčí zprávy #m	⇒ ⇐	Kladná odezva
Potvrzení přijetí dílčí zprávy (na přání)	⇒	(Datové pole < 255 bytů)
...		
Požadavek na přenos dat #n	⇒ ⇐	Kladná odezva
Požadavek na ukončení přenosu	⇒ ⇐	Kladná odezva
Požadavek na ukončení spojení	⇒ ⇐	Kladná odezva

2.2.4 Časování

DDP 019 Parametry časování uvedené na obr. 1 jsou při normální činnosti důležité:

Obrázek 1

Tok zprávy, časování

IDE request – požadavek IDE

VU response #1 – Odezva celku ve vozidle (VU) #1

IDE request / acknowledge #1 – Požadavek IDE / Potvrzení příjmu #1

VU response #2 – Odezva VU #2

Kde:

P1 = Vnitřní čas bytu pro odezvu VU

P2 = čas mezi koncem požadavku IDE a začátkem odezvy VU nebo mezi koncem potvrzení příjmu IDE a začátkem následující odezvy VU

P3 = Čas mezi koncem odezvy VU a začátkem nového požadavku IDE nebo mezi koncem odezvy VU a začátkem potvrzení příjmu IDE a nebo mezi koncem požadavku IDE a začátkem nového požadavku IDE pokud VU nestačí odpovédět

P4 = Vnitřní čas bytu pro požadavek IDE

P5 = Rozšířená platnost P3 na stažení dat karty

Přípustné hodnoty parametrů časování jsou uvedeny v následující tabulce (KWP rozšířený soubor parametrů časování používaný v případě fyzického adresování kvůli rychlejšímu spojení)

Parametr časování	Nižší limitní hodnota (ms)	Vyšší limitní hodnota (ms)
P1	0	20
P2	20	1000 (*)
P3	10	5000
P4	5	20
P5	10	20 minut

(*) Pokud aplikace VU se zápornou odezvou obsahuje kód znamenající „požadavek správně přijat, odezva se očekává“ je tato hodnota prodloužena na stejnou vyšší hodnotu P3

2.2.5 Chybná obsluha

Pokud se objeví chyba při změně zprávy, schéma toku zprávy je změněno v závislosti na zařízení, kterým byla chyba zjištěna a na zprávě jež chybu vyvolala.

Na obrázku 1 a obrázku 2 jsou uvedeny zvlášť uvedeny pro VU a IDE chybné postupy obsluhy

2.2.5.1 Fáze začátku spojení

DDP 020 Pokud IDE zjistí chybu v průběhu začátku spojení buď časováním nebo tokem bitů pak bude čekat po dobu P3 min. před opětovným vydáním požadavku.

DDP 021 Pokud VU zjistí chybu v úseku přicházejícím z IDE, neodešle žádnou odezvu počká na následující zprávu s aplikací o začátek spojení během doby P3 max.

2.2.5.2 Fáze spojení

Je možné definovat dvě různé oblasti chybné obsluhy

1. VU zjistí chybu v přenosu IDE

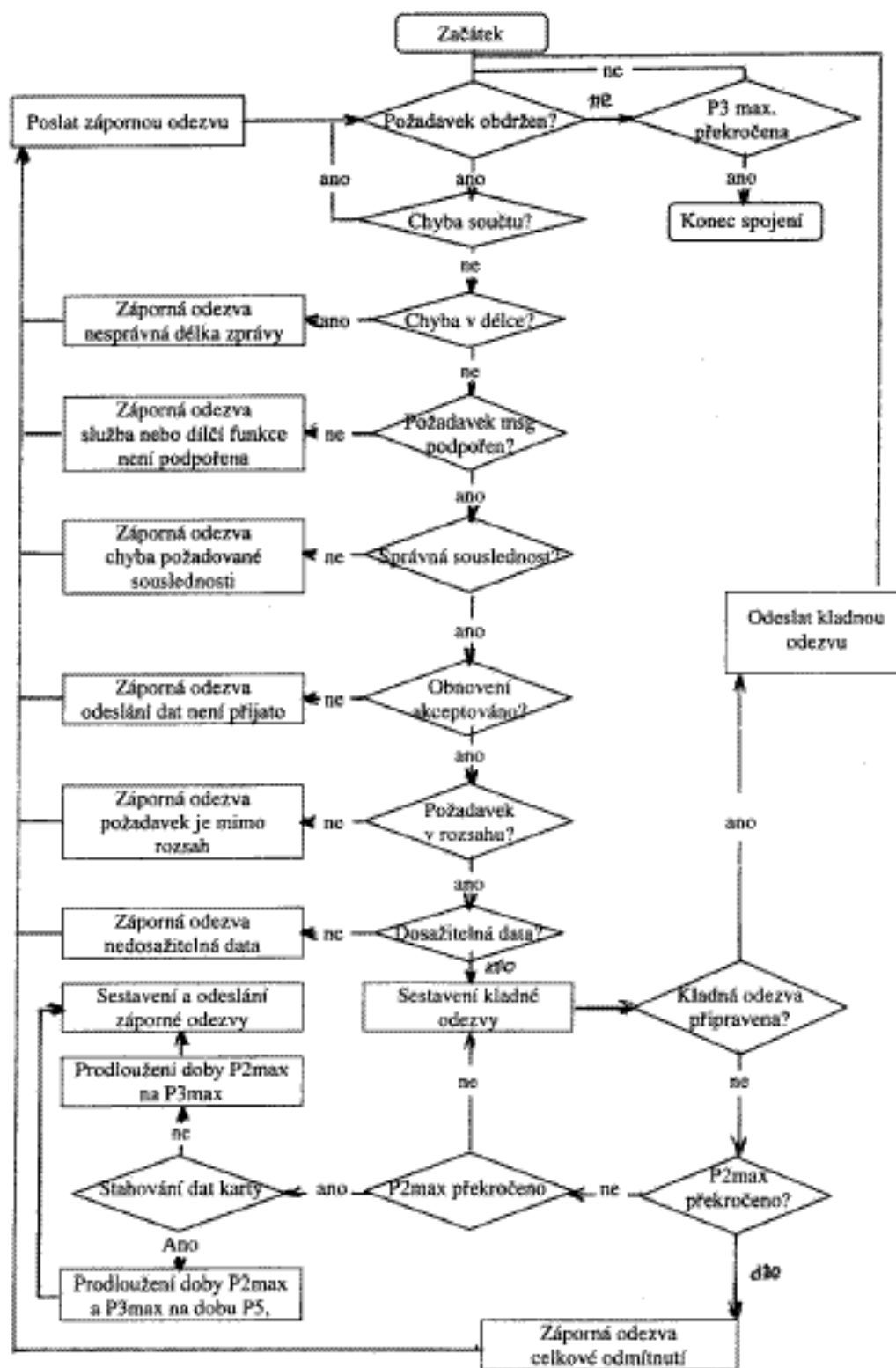
DDP 022 VU musí zjistit chyby v časování pro každou obdrženou zprávu, chyby ve formátu bytů (např. porušení počátečního a koncového bitu) a rámcové chyby (špatný počet obdržených bytů, špatný byte kontroly počtu)

DDP 023 Pokud VU zjistí jednu z výše uvedených chyb, pak neposílá žádnou odezvu a nebere na vědomí obdržené zprávy

DDP 024 VU může zjistit další chyby ve formátu nebo obsahu obdržené zprávy (např. nepodporovaná zpráva) i pokud zpráva splňuje délku a požadavky kontroly počtu, v takovém případě musí VU odpovědět IDE zprávou se zápornou odezvou určující podstatu chyby

Obrázek 2

Chybná obsluha VU



2. IDE zjistí chybu v přenosu VU

DDP 025 IDE musí zjistit chyby časování pro každou obdrženou zprávu, chyby ve formátu bytů (např. porušení počátečního a koncového bitu) a rámcové chyby (špatný počet obdržených bytů, špatný byte kontroly počtu)

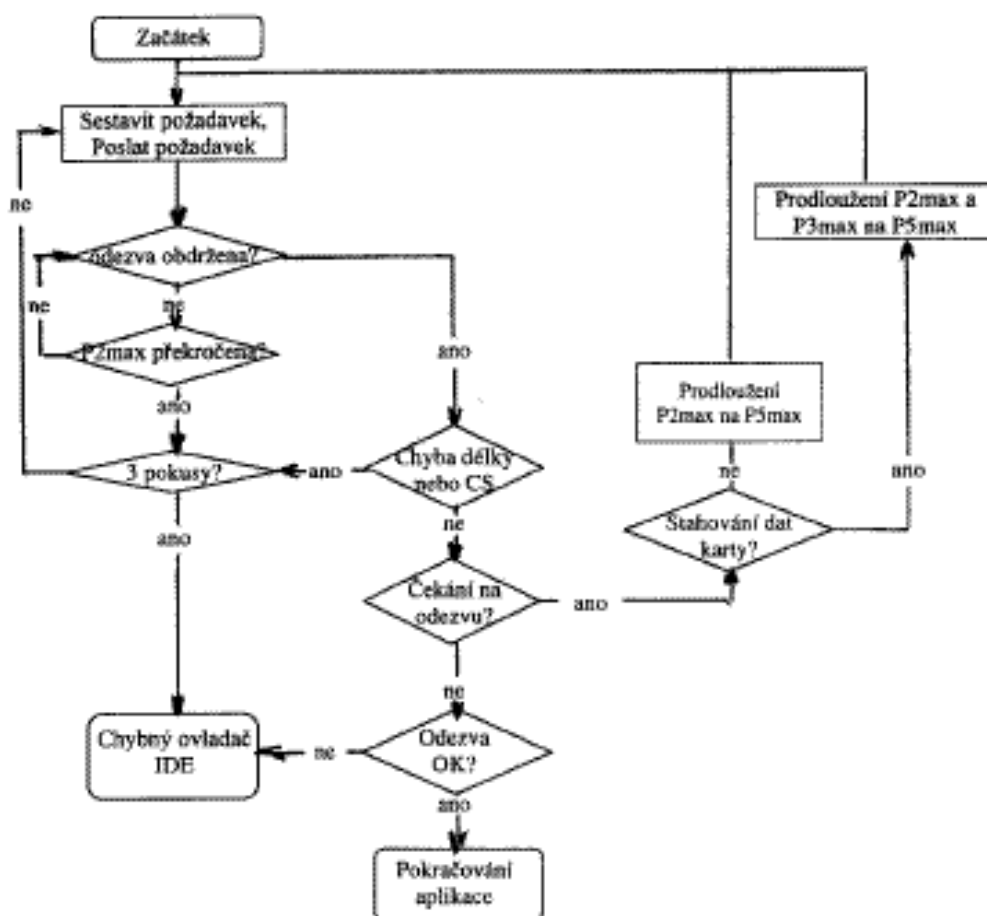
DDP 026 IDE musí zjistit chyby pořadí, např. nesprávná okénka dílčí zprávy v následujících obdržených zprávách

DDP 027 Pokud IDE zjistí chybu nebo neobdrží odezvu od VU za čas $P2_{max}$, pošle znova zprávu s požadavkem celkem maximálně třech přenosech. Pro účely této detekční chyby se bude považovat potvrzení příjmu dílčí zprávy za požadavek na VU.

DDP 028 IDE počká alespoň po dobu $P3_{min}$ před začátkem každého přenosu, doba čekání se musí měřit od posledně počítaného koncového bitu po zjištění chyby.

Obrázek 3

Chybná obsluha IDE



2.2.6 Obsah zprávy s odezvou

Tento odstavec určuje obsah datových polí různých zpráv s kladnou odezvou.

Prvky dat jsou definovány ve slovníku dat přílohy 1

2.2.6.1 Přehled přenášených dat kladné odezvy

DDP 029 Datové pole zprávy „přehledu přenášených dat kladné odezvy“ musí zajistit následující data v následujícím pořádku s SID 76 Hex, TREP 01 Hex a dílčí zprávou s vhodným dělením a řazením:

Datový prvek	Délka (Byty)	Komentář
MemberStateCertificate	194	Certifikát zabezpečení VU
VUCertificate	194	
VehicleIdentificationNumber	17	Identifikace vozidla
VehicleRegistrationIdentification	1	
vehicleRegistrationNation	14	
vehicleRegistrationNumber	14	
CurrentDateTime	4	Současné datum a čas
VuDownloadablePeriod	4	Perioda stažení dat VU
minDownloadableTime	4	
maxDownloadableTime	4	
CardSlotsStatus	1	Typ karet vložených do VU
VuDownloadActivityData	4	Předešlé stažení dat VU
downloadingTime	4	
fullCardNumber	18	
companyOrWorkshopName	36	
VuCompanyLocksData	1	Zajištění společnosti jsou uložena. Pokud je tato sekce prázdná je jen odesláno nezajištěna = 0
noOfLocks	(98)	
Vucompany	4	
Locks	4	
Record	4	
lockInTime	36	
lockOutTime	36	
companyName	36	
companyAddress	36	
companyCardNumber	18	
VuControlActivityData	1	Všechny záznamy o kontrole jsou uloženy ve VU.. Pokud je tato sekce prázdná je jen odesláno nekontrolována = 0
noOfControls	(31)	
Vucontrol	1	
Activity	4	
Record	18	
controlType	4	
controlTime	4	
controlCardNumber	4	
downloadPeriodBeginTime	4	
downloadPeriodEndTime	4	
Signature	128	RSA označení všech dat (vyjma certifikátů) začínají od stažení identifikačního čísla vozidla po poslední byte posledního záznamu kontroly činnosti VU

2.2.6.2 Kladná odezva na činnost přenosu dat

DDP 030 Datové pole zprávy „kladné odezvy na činnost přenosu dat“ musí zajistit následující data v následujícím pořádku s SID 76 Hex, TREP 02 Hex a dílčí zprávou s vhodným dělením a řazením

Datový prvek		Délka (Byty)	Komentář
TimeReal		4	Datum dne stažení dat
OdometerValueMidnight		3	Stav měřiče vzdálenosti na konci dne stažení dat
VuCardIWData noOfVuCardIWRecords		2	Data cyklů vložení a vyjmutí karet. – Pokud sekce neobsahuje dosažitelná data odešle se jen bez záznamů karty VU = 0. – Pokud IW záznam karty VU přechází přes 00:00 (karta vsunuta předchozí den) nebo přes 24:00 (karta vyjmuta následující den) musí se objevit vše za celé dva dny
		(129)	
VuCard IWRecord	cardHolderName		
	holderSurname	36	
	holderFirstName	36	
	fullCardNumber	18	
	cardExpiryDate	4	
	cardInsertionTime	4	
	vehicleOdometerValueAtInsertion	3	
	cardSlotNumber	1	
	cardWithdrawalTime	4	
	vehicleOdometerValueAtWithdrawal	3	
	previousVehicleInfo		
VuActivityDailyData noOfActivityChanges		2	Stav otvorů pro kartu v 00:00 a změny činnosti zaznamenané při denním stahování dat
ActivityChangeInfo		2	
VuPlaceDailyWorkPeriodData noOfPlaceRecords		1	Místa vztahující se k datům zaznamenaným při denním stažení dat. Pokud je sekce prázdná posílá se jen bez záznamů = 0
		(28)	
VuPlaceDaily Work Period Record	fullCardNumber	18	
	placeRecord		
	entryTime	4	
	entryTypeDaily		
	WorkPeriod		
	dailyWorkPeriod	1	
	Country	1	
	dailyWorkPeriod		
	Region	1	
	vehicleOdometer Value	3	
VuSpecificConditionData noOfSpecificConditionRecords		2	Data určitých podmínek zaznamenaných při denním stahování dat. Pokud je sekce prázdná posílá se jen bez záznamu určitých podmínek = 0
		(5)	
SpecificConditionRecord	EntryTime	4	
	specificCinditionType	1	
Signature		128	RSA označení všech dat začínají od stažení skutečného času po poslední byte posledního záznamu určitých podmínek

2.2.6.3 Kladná odezva přenosu dat událostí a závad

DDP 031 Datové pole zprávy „Kladná odezva přenosu dat událostí a závad“ musí zajistit následující data v následujícím pořádku s SID 76 Hex, TREP 03 Hex a dílčí zprávou s vhodným dělením a řazením

Datový prvek		Délka (Byty)	Komentář
VuFaultData NoOfFaults		1	Všechny závady zaznamenané nebo došlé do VU. Pokud je sekce prázdná posílá se jen žádné závady = 0
		(82)	
VuFaultRecord	FaultType	1	
	FaultRecordPurpose	1	
	EventBeginTime	4	
	EventEndTime	4	
	CardNumberDriverSlotBegin	18	
	CardNumberCocdriverSlotBegin	18	
	CardNumberDriverSlotEnd	18	
	CardNumberCocdriverSlotEnd	18	
VuEventData NoOfVuEvents		1	Všechny události (vyjma překročení rychlosti) zaznamenané nebo došlé do VU. Pokud je sekce prázdná posílá se jen žádné události = 0
		(83)	
VuEventRecord	EventType	1	
	EventRecordPurpose	1	
	EventBeginTime	4	
	EventEndTime	4	
	CardNumberDriverSlotBegin	18	
	CardNumberCocdriverSlotBegin	18	
	CardNumberDriverSlotEnd	18	
	CardNumberCocdriverSlotEnd	18	
VuOverSpeedingControlData LastOverspeedControlTime FirstOverspeedSince NumberOfOverspeedSince		4 4 1	Data vztažená k poslední kontrole překročení rychlosti. (Pokud chybí data jsou hodnoty opomenuty)
VuOverSpeedingEventData NoOfVuOverSpeedingEvents		1	
		(31)	Všechny události uložené do VU. Pokud je sekce prázdná posílá se jen žádné překročení rychlosti = 0
VuOverSpeedingEventRecord	EventType	1	
	EventRecordPurpose	1	
	EventBeginTime	4	
	EventEndTime	4	
	MaxSpeedValue	1	
	AverageSpeedValue	1	
	CardNumberDriverSlotBegin	18	
		1	
VuTimeAdjustmentData NoOfVuTimeAdjRecords		1	Všechna nastavení času uložené do VU (mimo rámec úplné kalibrace). Pokud je sekce prázdná posílá se jen žádné nastavení času = 0
		(98)	
VuTimeAdjustmentRecord	OldTimeValue	4	
	NewTimeValue	4	
	WorkshopName	36	
	WorkshopAddress	36	
	WorkshopCardNumber	18	
Signature		128	RSA označení všech dat začínají od stažení žádných závad po poslední byte posledního záznamu nastavení času

2.2.6.4. Kladná odezva přenosu dat detailních rychlostí

DDP 032 Datové pole zprávy „Kladná odezva přenosu dat detailních rychlostí“ musí zajistit následující data v následujícím pořádku s SID 76 Hex, TREP 04 Hex a dílčí zprávou s vhodným dělením a řazením

Datový prvek		Délka (Byty)	Komentář
VuDetailSpeedData			Všechna nastavení času uložené do VU (mimo rámec úplné kalibrace). Pokud je sekce prázdná posílá se jen žádné záznamy o nastavení času = 0
NoOfSpeedBlocks		2	
Vu Detailed Speed Block	SpeedBlockBeginDate	4	
	speedsPerSecond	60	
Signature		128	RSA označení všech dat začínají od stažení žádných závad po poslední byte posledního záznamu nastavení času

2.2.6.5 Kladná odezva přenosu dat detailních rychlostí

DDP 033 Datové pole zprávy „Kladná odezva přenosu dat detailních rychlostí“ musí zajistit následující data v následujícím pořádku s SID 76 Hex, TREP 05 Hex a dílčí zprávou s vhodným dělením a řazením

Datový prvek		Délka (Byty)	Komentář
VuIdentification			
vuManufacturerName		36	
vuManufacturerAddress		36	
vuPartNumber		16	
vuSerialNumber		8	
vuSoftwareIdentification		4	
vuSoftwareVersion		4	
vuSoftInstllationDate		4	
vuManufacturingDate		4	
vuApprovalNumber		8	
SensorPaired			
sensorSerialNumber		8	
sensorApprovalNumber		8	
sensorPairingDateFirst		4	
VuCalibrationData			Všechny kalibrační záznamy jsou uložena ve VU
noOFVuCalibrationRecords		1	
		(164)	
Vu Calibration Record	calibrationPurpose	1	
	workshopName	36	
	workshopAddress	36	
	workshopCardNumber	18	
	workshopCardExpiryDate	4	
	VehicleIdentification Number	17	
	vehicleRegistration Identification		
	vehicleRegistration Nation	1	
	vehicleRegistration Number	14	
	wVehicleCharacteristic Constant	2	
	kConstantOfRecording Equipment	2	
	lTyreCircuference	15	
	tyreSize	1	
	authorisedSpeed	3	
	oldOdometerValue	3	
	newOdometerValue	4	
	oldTimeValue	4	
	newTimeValue	4	
	nextCalibrationDate	4	
Sinature		128	RSA označení všech dat začínají od stažení názvu výrobce po poslední byte posledního kalibračního záznamu VU

2.3 ESM paměť souboru

DDP 034 Když stažená data obsahují přenos dat VU musí si IDE z jednoho fyzického souboru pamatovat všechna data obdržena z VU během stažení dat

ze zpráv s kladnou odezvou na přenos dat. Uložená data vylučují hlavičky zpráv, počty dílčích zpráv, prázdné dílčí zprávy a kontrolní součet, ale zahrnují SID a TREP (jen první dílčí zprávy pokud je dílčích zpráv několik).

3. PROTOKOL O STAŽENÍ DAT KARET TACHOGRAFU

3.1 Přehled

Paragraf popisuje přímé stahování dat karty z karty tachografu do IDE. IDE není část bezpečného prostředí, tudíž není splněna žádná autentičnost mezi kartou a IDE.

3.2. Definice

Stažení dat: Stažení dat z ICC je zajištěno v každou dobu. Doba překrývá úplný postup od resetování IDE pomocí IFD do deaktivace ICC (vyjmutí karty nebo dalšího resetování).

Značení datových souborů: Soubor od ICC. Soubor je převeden do IFD v jednoduchém textu. V ICC je soubor rozsekán a označen a označení je převedeno do IFD

3.3 Stažení dat karty

DDP 035 Stažení dat karty tachografu včetně následných kroků:

- Stažení dat běžných informací karty v EFs ICC a IC. Tyto informace jsou na přání a nejsou zabezpečeny digitálním podpisem.
- Stažení dat EFs certifikátu karty a certifikátu CA. Tato informace je zabezpečena digitálním podpisem.
- Je povinné stáhnout data těchto souborů při každém stahování dat
- stažení dat další EFs datové aplikace (z DF tachografu) vyjma stažení dat EF karty. Tato informace je zabezpečena digitálním podpisem.
- je povinné stáhnout data alespoň identifikace EFs aplikace a ID při každém stahování dat.
- při stahování dat karty řidiče je také povinné stáhnout data následující EFs:
 - Events_Data
 - Faults_Data
 - Driver_Activity_Data
 - Vehicles_Used

- Places
- Kontrol_Activity_Data
- Specific_Conditions
- Při stahování dat karty řidiče, obnovte datum posledního sta•ení dat karty v datumu EF Sard_Downloading.
- Při stahování dat karty dílny resetujte kalibrační počítadlo v EF Card_Downloading

3.3.1 Sousednost při inicializace

DDP 036 IDE musí zahájit souslednost následovně:

Karta	Směr	IDE/IFD	Význam/Poznámky
	←	Resetování hardwaru	
ATR	⇒		

Je možné zvolit použít PPS k přepnutí na vyšší přenosovou rychlost co nejdéle, pokud to podporuje ICC

3.3.2 Sousednost při neoznačených souborech dat

Karta	Směr	IDE/IFD	Význam/Poznámky
	←	Výběr souboru	Výběr souboru se provádí identifikátorem souboru
OK	⇒		
	←	Čtení v binárním kódu	Pokud soubor obsahuje více dat než velikost zásobníku čtečky nebo karty musí se příkaz opakovat dokud není celý soubor přečten
Data souboru OK	⇒	Uložení dat do ESM	

Poznámka: Před vybíráním EF Card_Certificate musí být vybrána aplikace tachografu (vybírá AID)

3.3.3 Sousednost při označených souborech dat

Karta	Směr	IDE/IFD	Význam/Poznámky
	←	Výběr souboru	
OK	⇒		
	←	Transformace souboru	Určit hodnotu transformace podle obsahu dat vybraného souboru použitím předepsaného algoritmu rozsekání podle přílohy 11. Tento

			příkaz není ISO příkaz
Určit transformaci souboru a transformovanou hodnotu dočasně uložit			
OK	⇒		

	⇐	Čtení v binárním kódu	Pokud soubor obsahuje více dat než velikost zásobníku čtečky nebo karty musí se příkaz opakovat dokud není celý soubor přečten
Data souboru OK	⇒	Uložení obdržených dat do ESM	V souladu s 3.4. (Formát uložených dat)
	⇐	PSO: Vypočítat digitální označení	Určit hodnotu transformace podle obsahu dat vybraného souboru použitím předepsaného algoritmu rozsekání podle přílohy 11. Tento příkaz není ISO příkaz
Zabezpečit operaci „vypočítat digitální označení“ dočasným uložením hodnoty rozsekání			
Označení OK	⇒	Přidat data k předešle uloženým do ESM	V souladu s 3.4. (Formát uložených dat)

3.3.4 Sousednost při resetování kalibračního počítadla

DDP 039 Sousednost při resetování počítadla
NoOfCalibrationsSinceDownload v dílně je následující:

Karta	Směr	IDE/IFD	Význam/Poznámky
	←	Výběr souboru EF Card_Download	Výběr identifikátorem souboru
OK	⇒		
	←	Binární obnovení NoOfCalibrations- SinceDownload = '00 00'	
Určit transformaci souboru a transformovanou hodnotu dočasně uložit			
OK	⇒		

3.4 Formát uložených dat

3.4.1 Úvod

DDP 040 Stažená data musí být uložena za následujících podmínek:

- data musí být uložena transparentně. To znamená, že pořadí bytů a právě tak bitů uvnitř bytu převedených z karty musí být při uložení zachováno
- všechny soubory stažených dat karty jsou při stahování uloženy v jednom souboru v ESM.

3.4.2 Formát souboru

DDP 041 Formát souboru je spojen z několika TLV bloků

DDP 042 Jmenovka pro EF musí být FID plus přípona „00“

DDP 043 Jmenovka EFs označení musí být FID souboru plus přípona „01“

DDP 044 Délka je dvou bytová hodnota. Hodnota určuje počet bytů v poli hodnot. Hodnota „FF FF“ je v délce pole rezervována pro budoucí použití.

DDP 045 Když se soubor nestahuje, neukládá se pro daný soubor nic (žádná jmenovka a žádná nulová délka)

DDP 046 Označení se musí uložit co nejbližší bloku TLV hned za Blok TLV, který obsahuje data souboru

Definice	Význam	Délka
FID (2 byty) "00"	Jmenovka pro EF (FID)	3 byty
FID (2 byty) "01"	Jmenovka označení EF(FID)	3 byty
xx xx	Délka pole hodnot	2 byty

Příklad dat v souboru stažených dat do ESM:

Jmenovka	Délka	Hodnota
00 02 00	00 11	Data ICC EF
C1 00 00	00 C2	Data Card_Certificate EF
	
05 05 00	0A02E	Data Vehicle_Used EF
05 05 01	00 80	Označení Vehicle_Used EF

4. STAHOVÁNÍ DAT KARTY TACHOGRAFU PŘES CELEK VE VOZIDLE

DDP 047 VU musí umožnit stažení obsahu dat karty řidiče, která je vložena do IDE

DDP 048 IDE musí poslat zprávu „požadavek na přenos stažených dat karty“ do VU, aby tuto činnost vyvolala (viz 2.2.2.9.)

DDP 049 VU pak musí stáhnout data z celé karty, soubor po souboru v souladu s protokolem o stažení dat z karty určeným v odstavci 3 a směřovat všechna data z karty do IDE ve vhodném formátu souboru TLV (viz 3.4.2.) a uzavřená ve zprávě „kladná odezva na přenos dat“.

DDP 050 IDE musí opět získat data karty ze zprávy „kladná odezva na přenos dat“ (odstraněním všech hlaviček, SID, TREP, počítadel dílčích zpráva kontroly celkového počtu) a uložit je v jednom fyzickém souboru jak předepisuje odstavec 2.3.

DDP 051 VU pak musí co nejvhodněji do současnosti obnovit Kontrol_Activity_Data nebo soubor Card_Download karty řidiče.

*Dodatek 8***KALIBRAČNÍ PROTOKOL****OBSAH**

1.	Úvod	242
2.	Pojmy, definice a odkazy	242
3.	Přehled služeb	243
3.1	Dostupné služby	243
3.2	Kódy odezvy	244
4.	Komunikační služby	244
4.1	Služba StartCommunication	244
4.2	Služba StopCommunication	247
4.2.1	Popis zprávy	247
4.2.2	Formát zprávy	248
4.2.3	Definice parametrů	248
4.3	Služba TesterPresent (zkušební přístroj připojen)	249
4.3.1	Popis zprávy	249
4.3.2	Formát zprávy	249
5.	Řídící služby	250
5.1	Služba StartDiagnosticSession	250
5.1.1	Popis zprávy	250
5.1.2	Formát zprávy	251
5.1.3	Definice parametru	252
5.2	Služba SecurityAccess	252
5.2.1	Popis zprávy	253
5.2.2	Formát zprávy – SecurityAccess – requestSeed	254
5.2.3	Formát zprávy – SecurityAccess - sendKey	255
6.	Služby přenosu dat	256
6.1	Služba ReadDataByIdentifier	256
6.1.1	Popis zprávy	256
6.1.2	Formát zprávy	256
6.1.3	Definice parametrů	257
6.2	Služba WriteDataByIdentifier	258
6.2.1	Popis zprávy	258

6.2.2	Formát zprávy	259
6.2.3	Definice parametru	259
7.	řízení zkušebních impulsů – řídicí funkční celek vstup/výstup	260
7.1	Popis zprávy	260
7.1.1	Popis zprávy	260
7.1.2	Formát zprávy	261
7.1.3	Definice parametrů	262
8.	formáty datarecords	262
8.1	Rozsahy přenášených parametrů	263
8.2	Formáty dataRecords	264

1. Úvod

Tento dodatek popisuje, jak se vyměňují data mezi celkem ve vozidle a zkušebním zařízením po lince K, která tvoří část kalibračního rozhraní popisovaného v dodatku 6. Popisuje také řízení signálního spojení vstup/výstup na kalibračním konektoru.

Vytváření komunikace na lince K je popsáno v části 4 „Komunikační služby“.

Tento dodatek užívá pojem diagnostické „jednání“ k tomu, aby stanovil rozsah platnosti řízení vedení K za různých podmínek. Opomenuté jednání je „StandardDiagnosticSession“ (standardní diagnostické jednání), kdy mohou být veškerá data čtena z celku ve vozidle, ale kdy nemohou být žádná data zapisována do celku ve vozidle.

Volba diagnostických jednání je popsána v části 5 „Řídící služby“.

CPR_001 „ECUProgrammingSession“ (programovací jednání ECU) umožňuje vstup dat do celku ve vozidle. V případě vstupu kalibračních dat (požadavek 097 a 098) musí celek ve vozidle navíc v pracovním módu CALIBRATION (kalibrace).

Přenos dat po lince K je popsán v části 6 „Služby přenosu dat“. Formáty přenášených dat jsou detailně uvedeny v části 8 „dataRecords formats“ (formáty záznamu dat).

CPR_002 „ECUAdjustmentSession“ (seřizovací jednání ECU) umožňuje volbu I/O módu (vstup/výstup) na kalibrační signální lince I/O přes rozhraní vedení K. Řízení kalibračního signálního spojení I/O je popsáno v části 7 „Řízení zkušebních impulsů – Řízení funkčního celku vstup/výstup“.

CPR_003 V tomto dokumentu je adresa zkušebního zařízení označována jako 'tt'. Může být také dáována přednost adresám zkušebních zařízení, celek ve vozidle musí správně spolupracovat s kterýmkoliv zkušebním zařízením. Fyzická adresa celku ve vozidle (VU) je 0xEE.

2. Pojmy, definice a odkazy

Protokoly, zprávy a chybové kódy jsou v podstatě založeny na současném návrhu ISO 14229-1 (Silniční vozidla – Diagnostické systémy – Část 1: Diagnostické služby, verze 6 ze dne 22. února 2001).

Pro služební identifikátory, požadavky a odezvy na služby a pro standardní parametry se užívá bytové kódování a hexadecimální hodnoty.

Pojem „zkušební zařízení“ se vztahuje na zařízení, užívané pro vstup programovacích/kalibračních dat do VU.

Pojmy „klient“ a „server“ se vztahují na zkušební zařízení a na VU.

Pojem ECU znamená „Electronic Control Unit“ (elektronický řídicí celek) a vztahuje se na VU (celek ve vozidle).

Odkazy:

ISO 14230-2: Silniční vozidla – Diagnostické systémy – Protokol klíčových slov 2000- Část 2: Vrstva datového spojení. Prvé vydání: 1999. Vozidla – Diagnostický systém.

3. Přehled služeb**3.1 Dostupné služby**

Dále uvedená tabulka podává přehled služeb, které budou dostupné v záznamovém zařízení a které jsou v tomto dokumentu definovány.

CPR_004 Tabulka uvádí služby, dostupné při určitém diagnostickém jednání.

- Prvý sloupec shrnuje dostupné služby,
- druhý sloupec zahrnuje číslo části v tomto dodatku, ve kterém jsou služby dále definovány,
- třetí sloupec přiděluje hodnoty identifikátorů služeb u požadavkových zpráv,
- čtvrtý sloupec stanovuje služby „StandardDiagnosticSession“ (standardní diagnostické jednání) – SD), které musí být zavedeny v každém celku ve vozidle (VU),
- pátý sloupec stanovuje služby „ECUAdjustmentSession“ (ECUAS), které musí být zavedeny pro umožnění řízení I/O signálního spojení z kalibračního konektoru na čelním panelu celku ve vozidle (VU),
- šestý sloupec stanovuje služby „ECUProgrammingSession“ (ECUPS), které musí být zavedeny pro umožnění programování parametrů v celku ve vozidle (VU).

Tabulka 1
Tabulka soupisu hodnot identifikátoru služeb

Název diagnostické služby	Část č.	SID hodnota požadavku	Diagnostické jednání		
			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		■	
■ Tento symbol značí, že služba je v tomto diagnostickém jednání povinná Žádný symbol značí, že služba není v tomto diagnostickém jednání povolena					

3.2 Kódy odezvy

Kódy odezvy jsou definovány pro každou službu.

4. Komunikační služby

Některé služby jsou potřebné k tomu, aby založily a udržovaly komunikaci. Neobjevují se na aplikační vrstvě. Dostupné služby jsou rozepsány v následující tabulce:

Tabulka 2
Komunikační služby

Název služby	popis
StartCommunication	Klient požaduje zahájení komunikačního jednání s serverem (serverem)
StopCommunication	Klient požaduje zakončení probíhajícího komunikačního jednání
TesterPresent	Klient oznamuje serveru, že je stále připojen

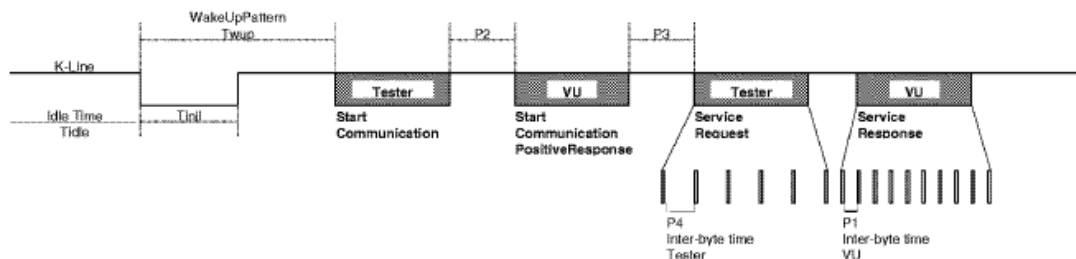
CPR_005 Služba StartCommunication je užita pro zahájení komunikace. Pro výkon jakékoliv služby musí být komunikace inicializována a komunikační parametry musí odpovídat požadovanému módu.

4.1 Služba StartCommunication

CPR_006 Po obdržení údaje StartCommunication primitiv musí celek ve vozidle ověřit, zda může být požadované komunikační spojení za současných podmínek inicializováno. Platné podmínky pro inicializaci komunikačního spojení jsou popsány v dokumentu ISO 14230-2.

CPR_007 Pak musí celek ve vozidle provést veškeré akce potřebné pro inicializaci komunikačního spojení a musí odeslat StartCommunication odezvu-primitiv společně se zvolenými parametry pozitivní odezvy.

- CPR_008 Pokud celek ve vozidle, který byl již inicializován (a který vstoupil do jakéhokoliv diagnostického jednání), obdrží nový požadavek StarCommunication (např. v důsledku výskytu závady ve zkušebním zařízení), musí být požadavek přijat a celek ve vozidle musí být znovu inicializován.
- CPR_009 Pokud nemůže být z jakéhokoliv důvodu komunikační spojení inicializováno, musí celek ve vozidle pokračovat v činnosti, kterou provozoval bezprostředně před obdržetím pokusu o inicializaci komunikačního spojení.
- CPR_010 Požadavek zprávy StratCommunication musí být fyzikálně adresován.
- CPR_011 Inicializace celku ve vozidle proběhne postupem „rychlé inicializace“,
- jakékoliv aktivitě předchází takt klidu sběrnice,
 - zkušební zařízení pak vyšle inicializační sekvenci,
 - veškeré informace, které jsou potřebné pro zajištění komunikace jsou obsaženy v odezvě celku ve vozidle.
- CPR_012 Po dokončení inicializace:
- se veškeré komunikační parametry nastaví podle klíčových bytů na hodnoty, definované v tabulce 4,
 - celek ve vozidle vyčkává na první požadavek od zkušebního zařízení,
 - celek ve vozidle je v diagnostickém módu prodlení, tj. StandardDiagnosticSession,
 - kalibrace signálního spojení I/O je ve stavu prodlení, tj. ve vyřazeném stavu.
- CPR_014 Rychlost přenosu dat na vedení K musí být 10400 Baud.
- CPR_016 Rychlá inicializace je zahájena zkušebním zařízením přenosem budící sekvence (Wup) po vedení K. Sekvence začíná po časové prodlevě na vedení K L-taktem Tinil. Zkušební zařízení vyšle první bit ze StartCommunicationService následně po Twup taktu, který začíná po první sestupné hraně impulsu.



K-line = vedení K

WakeUpPattern = budící sekvence

Idle Time Tidle = klidový stav

Tinil = Tinil

Tester = zkušební zařízení

VU = celek ve vozidle

StartCommunication = zahájení komunikace

StartCommunication positive Response = kladná odezva na zahájení komunikace

Serrvice Request = požadavek služby

Service Response = odezva služby

Inter-byte time Tester = zkušební zařízení na odstup bytového taktu

Inter-byte time = doba mezi byty.

CPR_017 Hodnoty časování pro rychlou inicializaci a komunikaci jsou obecně rozepsány v níže uvedených tabulkách. Existují různé možnosti pro dobu klidu (idle):

- první přenos po zapojení napájení, $T_{idle} = 300 \text{ ms}$,
- po dokončení služby StopCommunication, $T_{idle} = P3 \text{ min.}$,
- po zakončení komunikace v důsledku překročení doby $P3_{max}$, $T_{idle} = 0$.

Tabulka 3
Hodnoty časování pro rychlou inicializaci

Parametr		minimální hodnota	maximální hodnota
Tinil	$25 \pm 1 \text{ ms}$	24 ms	26 ms
Twup	$50 \pm 1 \text{ ms}$	49 ms	51 ms

Tabulka 4
Hodnoty časování komunikace

Parametr časování	Popis parametru	Dolní mezní hodnota (ms)	Horní mezní hodnota (ms)
		minimum	Maximum
P1	Doba mezi byty pro odezvu VU	0	20
P2	Doba mezi požadavkem zkušebního zařízení a odezvou VU nebo mezi dvěma odezvami VU	25	250
P3	Doba mezi konce odezvy VU a startem nového požadavku zkušebního zařízení	55	5000
P4	Doba mezi byty pro požadavek zkušebního zařízení	5	20

CPR_018 Formát zprávy pro rychlou inicializaci jsou rozepsány v níže uvedených tabulkách:

Tabulka 5
Zpráva o požadavku StartCommunication

Byt #	Název parametru	Hexagonální hodnota	Symbol
#1	Formátový byt – fyzikální adresa	81	FMT
#2	Byt cílové adresy	EE	TGT
#3	Byt adresy zdroje	tt	SRC
#4	Služba požadavku StartCommunication	81	SCR
#5	Kontrolní součet	00-FF	CS

Tabulka 6
Zpráva o kladné odezvě StartCommunication

Byt #	Název parametru	Hexagonální hodnota	Symbol
#1	Formátový byt – fyzikální adresa	80	FMT
#2	Byt cílové adresy	tt	TGT
#3	Byt adresy zdroje	EE	SRC
#4	Byt dodatečné délky	03	LEN
#5	Kladná odezva Id služby StartCommunication	C1	SCRPR
#6	Klíčový byt 1	EA	KB1
#7	Klíčový byt 2	8F	KB2
#8	Kontrolní součet	00-FF	CS

CPR_019 Na zprávu StartCommunication není záporná odezva a pokud není inicializována zpráva o kladné odezvě pro přenos do VU, nic se nepřenáší a vše zůstává v normálním provozu..

4.2 Služba StopCommunication

4.2.1 Popis zprávy

Tato služba buzení komunikační vrstvy slouží k ukončení komunikačního jednání.

CPR_020 Po obdržení StopCommunication-primitive musí VU ověřit, zda existující podmínky umožní tuto komunikaci ukončit. V tomto případě VU musí zajistit veškeré akce potřebné k ukončení komunikace.

CPR_021 Pokud je možno komunikaci ukončit, musí VU dříve než komunikace skončí vydat odezvu StopCommunication-primitive se zvolenými parametry Positive Response.

CPR_022 Pokud nemůže být komunikace z jakéhokoliv důvodu ukončena, Vydá VU odezvu StopCommunication-primitive se zvoleným parametrem Negative Response (záporná odezva).

CPR_023 Pokud VU zjistí překročení času P3max, komunikace se ukončí bez vydání jakékoliv odpovědi.

4.2.2 Formát zprávy

CPR_024 Formáty zpráv pro StopCommunication-primitive jsou rozepsány v níže uvedených tabulkách:

Tabulka 7
Zpráva požadavku StopCommunication

Byt #	Název parametru	Hexagonální hodnota	Symbol
#1	Formátový byt – fyzikální adresa	80	FMT
#2	Byt cílové adresy	EE	TGT
#3	Byt adresy zdroje	tt	SRC
#4	Byt dodatečné délky	01	LEN
#5	Služba Id požadavku StopCommunication	82	SPR
#6	Kontrolní součet	00-FF	CS

Tabulka 8
Zpráva o kladné odezvě StopCommunication

Byt #	Název parametru	Hexagonální hodnota	Symbol
#1	Formátový byt – fyzikální adresa	80	FMT
#2	Byt cílové adresy	tt	TGT
#3	Byt adresy zdroje	EE	SRC
#4	Byt dodatečné délky	01	LEN
#5	Služba kladné odezvy StopCommunication	C2	SPRPR
#6	Kontrolní součet	00-FF	CS

Tabulka 9
Zpráva o záporné odezvě StopCommunication

Byt #	Název parametru	Hexagonální hodnota	Symbol
#1	Formátový byt – fyzikální adresa	80	FMT
#2	Byt cílové adresy	tt	TGT
#3	Byt adresy zdroje	EE	SRC
#4	Byt dodatečné délky	03	LEN
#5	Služba záporné odezvy Id	7F	NR
#6	Záporná identifikace služby StopCommunication	82	SPR
#7	ResponseCode = generalReject	10	RC_GR
#8	Kontrolní součet	00-FF	CS

4.2.3 Definice parametrů

Tato služba nevyžaduje žádné definice parametrů

4.3 Služba TesterPresent (zkušební přístroj připojen)

4.3.1 Popis zprávy

Službu TesterPresent užívá zkušební zařízení k indikaci serveru, že je stále připojeno, aby tak bylo serveru zabráněno v automatickém návratu do normální činnosti a popřípadě v přerušení komunikace. Tato služba, která se vysílá periodicky, udržuje diagnostické jednání/komunikaci aktivní tím, že vždy po obdržení požadavku této služby resetuje časovač P3.

4.3.2 Formát zprávy

CPR_079 Formáty zpráv pro TesterPresent-primitive jsou rozepsány v níže uvedených tabulkách:

Tabulka 10
Zpráva o požadavku TesterPresent

Byt #	Název parametru	Hexagonální hodnota	Symbol
#1	Formátový byt – fyzikální adresa	80	FMT
#2	Byt cílové adresy	EE	TGT
#3	Byt adresy zdroje	tt	SRC
#4	Byt dodatečné délky	02	LEN
#5	Služba Id požadavku TesterPresent	3E	TP
#6	Dílčí funkce = responseRequired = [ano ne]	01 02	RESPREQ_Y RESPREQ_NO
#7	Kontrolní součet	00-FF	CS

Tabulka 11
Zpráva o kladné odezvě TesterPresent

Byt #	Název parametru	Hexagonální hodnota	Symbol
#1	Formátový byt – fyzikální adresa	80	FMT
#2	Byt cílové adresy	tt	TGT
#3	Byt adresy zdroje	EE	SRC
#4	Byt dodatečné délky	01	LEN
#5	Služba Id kladné odezvy TesterPresent	7E	TPPR
#6	Kontrolní součet	00-FF	CS

CPR_081 Služba podporuje následující kódy negativních odezev

Tabulka 12
Zpráva o záporné odezvě TesterPresent

Byt #	Název parametru	Hexagonální hodnota	Symbol
#1	Formátový byt – fyzikální adresa	80	FMT
#2	Byt cílové adresy	tt	TGT
#3	Byt adresy zdroje	EE	SRC
#4	Byt dodatečné délky	03	LEN
#5	Služba záporné odezvy Id	7F	NR
#6	Záporná identifikace služby TesterPresent	3E	TP
#7	ResponseCode = [SubFunctionNotSupported-InvalidFormat incorrectMessageLength]	12 13	RC_SFNS_IF RC IML
#8	Kontrolní součet	00-FF	CS

5. ŘÍDÍCÍ SLUŽBY

Dostupné služby jsou rozepsány v následující tabulce:

Název služby	popis
StartDiagnosticSession	Klient požaduje zahájení diagnostického jednání s VU
SecurityAccess	Klient požaduje přístup k funkcím, vyhrazeným autorizovaným uživatelům

5.1 Služba StartDiagnosticSession

5.1.1 Popis zprávy

CPR_025 Služba StartDiagnosticSession se užívá pro umožnění různých diagnostických jednání na serveru. Diagnostické jednání umožňuje zvláštní sadu služeb podle tabulky 17. Určité jednání umožňuje výrobcí zvláštní služby, které nejsou součástí tohoto dokumentu. Pravidla implementace musí odpovídat následujícím požadavkům:

- v celku ve vozidle musí být vždy aktivní jediné diagnostické jednání,
- vždy když je připojen na napájení, musí celek ve vozidle zahájit StandardDiagnosticSession. Pokud není zahájeno jiné diagnostické jednání, pak StandardDiagnosticSession probíhá tak dlouho, pokud je celek ve vozidle napájen,
- pokud je zkušebním zařízením požadováno diagnostické jednání, které již probíhá, odešle celek ve vozidle zprávu o kladné odezvě,
- kdykoliv zkušební zařízení požaduje nové diagnostické jednání, odešle celek ve vozidle nejprve zprávu o kladné odezvě StartDiagnosticSession, dříve než se nové jednání stane v celku ve vozidle aktivním. Pokud není celek ve vozidle schopen zahájit požadované nové diagnostické jednání, pak musí VU odpovědět

zprávou o záporné odezvě StartDiagnosticSession a probíhající jednání musí pokračovat.

CPR_026 Diagnostické jednání se zahájí pouze tehdy, pokud byla mezi klientem a celkem ve vozidle uskutečněna komunikace.

CPR_027 Pokud bylo jiné diagnostické jednání dříve aktivní, stanou se parametry časování podle definice v tabulce 4 aktivními po úspěšném StartDiagnosticSession s parametry diagnosticSession nastavenými ve zprávě o požadavku na „StandardDiagnosticSession“.

5.1.2 Formát zprávy

CPR_028 Formáty zpráv pro StartDiagnosticSession-primitive jsou rozepsány v níže uvedených tabulkách:

Tabulka 14
Zpráva o požadavku StartDiagnosticSession

Byt #	Název parametru	Hexagonální hodnota	Symbol
#1	Formátový byt – fyzikální adresa	80	FMT
#2	Byt cílové adresy	EE	TGT
#3	Byt adresy zdroje	tt	SRC
#4	Byt dodatečné délky	02	LEN
#5	Služba Id požadavku StartDiagnosticSession	10	STDS
#6	DiagnosticSession = (jedna z hodnot v tabulce 17)	xx	DS ...
#7	Kontrolní součet	00-FF	CS

Tabulka 15
Zpráva o kladné odezvě StartDiagnosticSession

Byt #	Název parametru	Hexagonální hodnota	Symbol
#1	Formátový byt – fyzikální adresa	80	FMT
#2	Byt cílové adresy	tt	TGT
#3	Byt adresy zdroje	EE	SRC
#4	Byt dodatečné délky	02	LEN
#5	Služba Id kladné odezvy StartDiagnosticSession	50	STDSPR
#6	DiagnosticSession = (shodná hodnota s #6 v tabulce 14)	xx	DS ...
#7	Kontrolní součet	00-FF	CS

Tabulka 16
Zpráva o záporné odezvě StartDiagnosticSession

Byt #	Název parametru	Hexagonální hodnota	Symbol
#1	Formátový byt – fyzikální adresa	80	FMT
#2	Byt cílové adresy	tt	TGT
#3	Byt adresy zdroje	EE	SRC
#4	Byt dodatečné délky	03	LEN
#5	Služba záporné odezvy Id	7F	NR
#6	Záporná identifikace služby StartDiagnosticService	10	STDS
#7	ResponseCode = (SubFunctionNotSupported ^a incorrectMessageLength ^b conditionsNotCorrect ^c)	12 13 22	RC_SFNS RC_IML RC_CNC
#8	Kontrolní součet	00-FF	CS
^a	Hodnota vložená do bytu #6 zprávy o požadavku není podporována, tj. není v tabulce 17.		
^b	Délka zprávy není správná.		
^c	Nejsou splněna kritéria pro požadavek StartDiagnosticSession.		

5.1.3 Definice parametru

CPR_029 Parametr diagnosticSession (DS_) využívá služba StartDiagnosticSession k výběru zvláštního chování serveru (severů). Následující diagnostická jednání jsou stanovena v tomto dokumentu:

Tabulka 17
definice hodnot diagnosticSession

Hexagonál	Popis	Symbol
81	StandardDiagnosticSession Toto diagnostické jednání umožňuje všechny stanovené služby podle tabulky 1, sloupec 4 „SD“. Tyto služby umožňují čtení dat ze serveru (VU). Toto diagnostické jednání je aktivní po úspěšném dokončení inicializace mezi klientem (zkušebním zařízením) a serverem (VU). Diagnostické jednání může být přepsáno jiným diagnostickým jednáním, stanoveným v této části.	SD
85	ECUProgramSession Toto diagnostické jednání umožňuje veškeré služby, stanovené v tabulce 1, sloupec 6 „ECUPS“. Tyto služby podporují programování paměti serveru (VU). Toto diagnostické jednání může být přepsáno jinými diagnostickými jednáními, stanovenými v této části.	ECUPS
87	ECUAdjustmentSession Toto diagnostické jednání umožňuje veškeré služby, stanovené v tabulce 1, sloupec 6 „ECUAS“. Tyto služby podporují řízení vstup/výstup serveru (VU). Toto diagnostické jednání může být přepsáno jinými diagnostickými jednáními, stanovenými v této části.	ECUAS

5.2 Služba SecurityAccess

Zapisování kalibračních dat nebo přístup ke spojení kalibrace vstup/výstup není možný, aniž by VU byl v módu KALIBRACE. Mimo vložení platné dílenské karty do

VU je nezbytné vložit do VU příslušný PIN dříve, než je udělen přístup k módu KALIBRACE.

Služba SecurityAccess zajišťuje prostředky pro vložení PIN a indikuje zkušebnímu zařízení, zda je nebo není VU v módu KALIBRACE.

Je přípustné, aby mohl být PIN vložen alternativními postupy.

5.2.1 Popis zprávy

Služba SecurityAccess je tvořena zprávou SecurityAccess „requestSeed“, popřípadě následovanou zprávou SecurityAccess „sendKey“. Služba SecurityAccess musí být provedena po službě StartDiagnosticSession.

CPR_033 Zkušební zařízení využívá zprávu SecurityAccess „requestSeed“, pro ověření, zda je celek ve vozidle připraven k přijetí PIN.

CPR_034 Pokud je celek ve vozidle již v módu KALIBRACE, musí odpovědět na požadavek vysláním „seed“ 0x0000 s užitím služby SecurityAccesspositiveResponse.

CPR_035 Pokud je celek ve vozidle připraven k přijetí PIN pro ověření dílenskou kartou, musí odpovědět na požadavek vysláním „seed“ většího než 0x0000 užitím kladné odezvy služby SecurityAccess.

CPR_036 Pokud není celek ve vozidle připraven k přijetí PIN od zkušebnímu zařízení, buď protože vložená dílenská karta není platná, nebo protože nebyla vložena žádná dílenská karta, nebo protože celek ve vozidle přijímá PIN jiným postupem, odpoví VU na požadavek zápornou odezvou s kódem odezvy nastaveným na conditionsNotCorrectOrRequestSequenceError.

CPR_037 Zkušební zařízení pak popřípadě užije zprávu SecurityAccess „sendKey“ k tomu, aby PIN doručilo do celku ve vozidle. K tomu, aby byl k dispozici čas, potřebný k postupu zjištění totožnosti karty, použije celek ve vozidle pro prodloužení času pro odezvu kód záporné odezvy requestCorrectlyReceived-RsponsePending. Maximální doba pro odezvu však nesmí překročit pět minut. Jakmile byla požadovaná služba dokončena, musí celek ve vozidle vyslat zprávu o kladné odezvě nebo zprávu o záporné odezvě s kódem odezvy, odlišným od kódu této služby. Kód záporné odezvy requestCorrectlyReceived-ResponsePending může být od celku ve vozidle opakován do dokončení požadované služby a do vyslání zprávy o konečné odezvě.

CPR_038 Celek ve vozidle musí na tento požadavek odpovědět užitím služby SecurityAccess PositiveResponse pouze v módu KALIBRACE.

CPR_039 Celek ve vozidle musí v následujících případech odpovědět na tento požadavek zápornou odezvou s kódem odezvy nastaveným na:

- subFunctionNot supported: neplatný formát pro parametr dílčí funkce (accessType),

- conditionNotCorrectOrRequestSequenceError: celek ve vozidle není připraven k přijetí vstupu PIN,
- invalidKey: PIN není platný a počet pokusů o ověření PIN není překročen,
- exceededNumberOfAttempts: PIN není platný a počet pokusů o ověření PIN je překročen,
- generalReject: PIN je správný, ale selhalo vzájemné prokazování totožnosti s dílenskou kartou.

5.2.2 Formát zprávy – SecurityAccess – requestSeed

CPR_040 Formáty zpráv SecurityAccess „requestSeed“ primitives jsou rozepsány v níže uvedených tabulkách:

Tabulka 18
Požadavek SecurityAccess – zpráva requestSeed

Byt #	Název parametru	Hexagonální hodnota	Symbol
#1	Formátový byt – fyzikální adresa	80	FMT
#2	Byt cílové adresy	EE	TGT
#3	Byt adresy zdroje	tt	SRC
#4	Byt dodatečné délky	02	LEN
#5	Služba Id požadavku SecurityAccess	27	SE
#6	accessType – requestSeed	7D	AT_RSD
#7	Kontrolní součet	00-FF	CS

Tabulka 19
Zpráva o kladné odezvě SecurityAccess –requestSeed

Byt #	Název parametru	Hexagonální hodnota	Symbol
#1	Formátový byt – fyzikální adresa	80	FMT
#2	Byt cílové adresy	tt	TGT
#3	Byt adresy zdroje	EE	SRC
#4	Byt dodatečné délky	04	LEN
#5	Služba Id kladné odezvy SecurityAccess	67	SAPR
#6	accessType – requestSeed	7D	AT_RSD
#7	Seed High (vysoké)	00-FF	SEEDH
#8	Seed Low (nízké)	00-FF	SEEDL
#9	Kontrolní součet	00-FF	CS

Tabulka 20
Zpráva o záporné odezvě SecurityAccess

Byt #	Název parametru	Hexagonální hodnota	Symbol
#1	Formátový byt – fyzikální adresa	80	FMT
#2	Byt cílové adresy	tt	TGT
#3	Byt adresy zdroje	EE	SRC
#4	Byt dodatečné délky	03	LEN
#5	Služba Id záporné odezvy	7F	NR
#6	Služba Id požadavku SecurityAccess	27	SA
#7	responseCode = (conditionsNotCorrectOrRequestSequenceError incorrectMessageLength)	22 13	RC_CNC RC_IML
#8	Kontrolní součet	00-FF	CS

5.2.3 Formát zprávy – SecurityAccess - sendKey

CPR_041 Formáty zprávy pro SecurityAccess „sendKey“ primitives jsou rozepsány v níže uvedených tabulkách:

Tabulka 21
Požadavek SecurityAccess – zpráva sendKey

Byt #	Název parametru	Hexagonální hodnota	Symbol
#1	Formátový byt – fyzikální adresa	80	FMT
#2	Byt cílové adresy	EE	TGT
#3	Byt adresy zdroje	tt	SRC
#4	Byt dodatečné délky	m+2	LEN
#5	Služba Id požadavku SecurityAccess	27	SA
#6	accessType – sendKey	7E	AT_SK
#7 až #m+6	Klíč #1 (vysoký) ... Klíč #m (nízký, m musí být nejméně 4 a nejvýše 8)	xx ... xx	KEY
#m+7	Kontrolní součet	00-FF	CS

Tabulka 22
Zpráva o kladné odezvě SecurityAccess – sendKey

Byt #	Název parametru	Hexagonální hodnota	Symbol
#1	Formátový byt – fyzikální adresa	80	FMT
#2	Byt cílové adresy	tt	TGT
#3	Byt adresy zdroje	EE	SRC
#4	Byt dodatečné délky	02	LEN
#5	Služba Id kladné odezvy SecurityAccess	67	SAPR
#6	accessType – sendKey	7E	AT_SK
#7	Kontrolní součet	00-FF	CS

Tabulka 23
Zpráva o záporné odezvě SecurityAccess

Byt #	Název parametru	Hexagonální hodnota	Symbol
#1	Formátový byt – fyzikální adresa	80	FMT
#2	Byt cílové adresy	tt	TGT
#3	Byt adresy zdroje	EE	SRC
#4	Byt dodatečné délky	03	LEN
#5	Služba Id záporné odezvy	7F	NR
#6	Služba Id požadavku SecurityAccess	27	SA
#7	responseCode = (generalReject	10	RC_GR
	subFunctionNotSupported	12	RC_SFNS
	incorrectMessageLength	13	RC_IML
	conditionsNotCorrectOrRequestSequenceError	22	RCCNC
	invalidKey	35	RC_IK
	exceededNumberOfAttempts	36	RC_ENA
	requestCorrectlyReceived-ResponsePending)	78	RC_RCR_RP
#8	Kontrolní součet	00-FF	CS

6. Služby přenosu dat

Dostupné služby jsou rozepsány v následující tabulce:

Tabulka 24
Služby přenosu dat

Název služby	popis
ReadDataByIdentifier	Klient požaduje přenos běžné hodnoty ze záznamu přístupem pomocí recordDataIdentifier
WriteDataByIdentifier	Klient žádá o zápis záznamu pomocí recordDataIdentifier

6.1 Služba ReadDataByIdentifier

6.1.1 Popis zprávy

CPR_050 Služba ReadDataByIdentifier je využívána klientem pro vyžádání záznamu dat ze serveru. Data jsou identifikována pomocí recordDataIdentifier. Je na odpovědnosti výrobce celku ve vozidle, aby byly při výkonu této služby splněny podmínky serveru.

6.1.2 Formát zprávy

CPR_031 Formáty zprávy pro ReadDataByIdentifier-primitives jsou rozepsány v níže uvedených tabulkách:

Tabulka 21
Zpráva o požadavku ReadDataByIdentifier

Byt #	Název parametru	Hexagonální hodnota	Symbol
#1	Formátový byt – fyzikální adresa	80	FMT
#2	Byt cílové adresy	EE	TGT
#3	Byt adresy zdroje	tt	SRC
#4	Byt dodatečné délky	03	LEN
#5	Služba Id požadavku ReadDataByIdentifier	22	RDBI
#6 a #7	recordDataIdentifier = (hodnota z tabulky 28)	xxxx	RDI...
#8	Kontrolní součet	00-FF	CS

Tabulka 26
Zpráva o kladné odezvě ReadDataByIdentifier

Byt #	Název parametru	Hexagonální hodnota	Symbol
#1	Formátový byt – fyzikální adresa	80	FMT
#2	Byt cílové adresy	tt	TGT
#3	Byt adresy zdroje	EE	SRC
#4	Byt dodatečné délky	m+3	LEN
#5	Služba Id kladné odezvy ReadDataByIdentifier	62	RDBIPR
#6 a #7	RecordDataIdentifier = (stejná hodnota, jako byty #6 a #7 v tabulce 25)	xxxx	RDI_...
#8 až #m+7	dataRecord() = (data#1 data#m)	xx ... xx	DREC_DATA1 ... DREC_DATAm
#m+8	Kontrolní součet	00-FF	CS

Tabulka 27
Zpráva o záporné odezvě ReadDataByIdentifier

Byt #	Název parametru	Hexagonální hodnota	Symbol
#1	Formátový byt – fyzikální adresa	80	FMT
#2	Byt cílové adresy	tt	TGT
#3	Byt adresy zdroje	EE	SRC
#4	Byt dodatečné délky	03	LEN
#5	Služba Id záporné odezvy	7F	NR
#6	Služba Id požadavku ReadDataByIdentifier	22	RDBI
#7	ResponseCode = (requestOutOfRande incorrectMessageLength conditionsNotCorrect')	31 13 22	RC_ROOR RC_IML RCCNC
#8	Kontrolní součet	00-FF	CS

6.1.3 Definice parametrů

CPR_052 Parametr recordDataIdentifier (RDI_) ve zprávě o požadavku ReadDataByIdentifier identifikuje záznam dat.

CPR_053 Hodnoty recordDataIdentifier, definované tímto dokumentem, jsou uvedeny v níže uvedené tabulce.

Tabulka recordDataIdentifier je tvořena čtyřmi sloupci a množstvím řádek

- první sloupec (Hex) zahrnuje “hexagonální hodnotu”, určenou pro recordDataIdentifier, stanovený ve třetím sloupci,
- druhý sloupec (Data Element) stanovuje prvek dat z dodatku 1, na kterém je založen záznam recordDataIdentifier (někdy je potřebné překódování),
- třetí sloupec (Description – popis) stanovuje odpovídající název recordDataIdentifier,
- čtvrtý sloupec (Mnemonic – symbol) stanovuje pro tento recordDataIdentifier příslušný symbol.

Tabulka 28
Definice hodnot recordDataIdentifier

Hex	Prvek dat	Název recordDataIdentifier (viz formát v části 8.2)	Symbol
F90B	CurrentDateTime	TimeDate	RDI_TD
F912	HighResOdometer	HighResolutionTotalVehicleDistance	RDI_HRTVD
F918	K-ConstantOfRecordingEquipment	Kfactor	RDI_KF
F91C	L-TyreCircumference	LfactorTyreCircumference	RDI_LF
F91D	W-VehicleCharacteristicConstant	WvehicleCharacteristicFactor	RDI_WVCF
F921	TyreSize	TyreSize	RDI_TS
F922	nextCalibrationDate	NextCalibrationDate	RDI_NCD
F92C	SpeedAuthorized	SpeedAuthorized	RDI_SA
F97D	vehicleRegistrationNation	RegisteringMemberState	RDI_RMS
F97E	VehicleRegistrationNumber	VehicleRegistrationNumber	RDI_VRN
F190	VehicleIdentificationNumber	VIN	RDI_VIN

CPR_054 Parametr dataRecord (DREC_) se užije při zprávě o kladné odezvě ReadDataByIdentifier k tomu, aby hodnoty dat záznamu identifikovány klientovi (zkušebnímu zařízení) pomocí recordDataIdentifier. Formáty dat jsou stanoveny v části 8. Mohou být zavedena volitelná dataRecords dalších uživatelů včetně zvláštního vstupu celku ve vozidle, vnitřních a výstupních dat, ta však nejsou definována v tomto dokumentu.

6.2 Služba WriteDataByIdentifier

6.2.1 Popis zprávy

CPR_056 Služba WriteDataByIdentifier užívá klient k zápisu hodnot záznamu dat na serveru. Data jsou identifikována pomocí recordDataIdentifier. Je na odpovědnosti výrobce celku ve vozidle, aby byly při výkonu této služby splněny podmínky serveru. Pro obnovení parametrů uvedených v tabulce 28 musí být celek ve vozidle v módu KALIBRACE.

6.2.2 Formát zprávy

CPR_057 Formáty zpráv pro WriteDataByIdentifier-primitives jsou rozepsány v níže uvedených tabulkách:

Tabulka 29
Zpráva o požadavku WriteDataByIdentifier

Byt #	Název parametru	Hexagonální hodnota	Symbol
#1	Formátový byt – fyzikální adresa	80	FMT
#2	Byt cílové adresy	EE	TGT
#3	Byt adresy zdroje	tt	SRC
#4	Byt dodatečné délky	m+3	LEN
#5	Služba Id požadavku WriteDataByIdentifier	2E	WDBI
#6 a #7	recordDataIdentifier = (hodnota z tabulky 28)	xxxx	RDI...
#8 až #m+7	dataRecord() = (data#1 data#m)	xx ... xx	DREC_DATA1 ... DREC_DATAm
#m+8	Kontrolní součet	00-FF	CS

Tabulka 30
Zpráva o kladné odezvě WriteDataByIdentifier

Byt #	Název parametru	Hexagonální hodnota	Symbol
#1	Formátový byt – fyzikální adresa	80	FMT
#2	Byt cílové adresy	tt	TGT
#3	Byt adresy zdroje	EE	SRC
#4	Byt dodatečné délky	03	LEN
#5	Služba Id kladné odezvy WriteDataByIdentifier	6E	WDBIPR
#6 a #7	RecordDataIdentifier = (stejná hodnota, jako byty #6 a #7 v tabulce 25)	xxxx	RDI_...
#8	Kontrolní součet	00-FF	CS

Tabulka 31
Zpráva o záporné odezvě WriteDataByIdentifier

Byt #	Název parametru	Hexagonální hodnota	Symbol
#1	Formátový byt – fyzikální adresa	80	FMT
#2	Byt cílové adresy	tt	TGT
#3	Byt adresy zdroje	EE	SRC
#4	Byt dodatečné délky	03	LEN
#5	Služba Id záporné odezvy	7F	NR
#6	Služba Id požadavku WriteDataByIdentifier	22	WDBI
#7	ResponseCode = (requestOutOfRande incorrectMessageLength conditionsNotCorrect')	31 13 22	RC_ROOR RC_IML RCCNC
#8	Kontrolní součet	00-FF	CS

6.2.3 Definice parametru

Parametr recordDataIdentifier (RDI_) je definován v tabulce 28.

Parametr dataRecord (DREC_) je využíván zprávou o požadavku WriteDataByIdentifier pro zajištění záznamu hodnot dat do serveru (VU), identifikovaných pomocí recordDataIdentifier. Formáty dat jsou stanoveny v části 8.

7. řízení zkušebních impulsů – řídicí funkční celek vstup/výstup

Dostupné služby jsou rozepsány v níže uvedených tabulkách:

Tabulka 32
Řídicí funkční celek vstup/výstup

Název služby	popis
InpuOutputControlByIdentifier	Klient požaduje řízení vstupu/výstupu, patřícího serveru.

7.1 Popis zprávy

7.1.1 Popis zprávy

Existuje propojení přes přední konektor, které umožňuje zkušebním impulsům, aby byly řízeny nebo monitorovány užitím vhodného zkušebního zařízení.

CPR_058 Toto kalibrační I/O (vstup/výstup) signální spojení může být konfigurováno příkazem z K-vedení užitím služby InputControlByIdentifier k volbě požadované funkce vstupu nebo výstupu pro spojení. Dostupné stavy spojení jsou:

- neaktivní
- speedSignalInput, kdy je signální spojení kalibrace I/O užito pro vstup rychlostního signálu (zkušební signal), který nahrazuje rychlostní signal snímače pohybu,
- realTimeSpeedSignalOutputSensor, kdy je signální spojení kalibrace I/O užito pro výstup rychlostního signálu ze snímače pohybu.
- RTCOutput, kdy je kalibrační signální spojení I/O užito pro výstup hodinového signálu UTC.

CPR_059 Do celku ve vozidle musí být vloženo seřizovací jednání a celek musí být v módu KALIBRACE, aby konfiguroval stav spojení. Na výstupu seřizovacího jednání nebo módu KALIBRACE musí celek ve vozidle zajistit, aby se kalibrační spojení signálu I/O vrátilo do stavu „neaktivní“ (neplatný).

CPR_060 Pokud jsou rychlostní impulsy přijaty na vstupu signálního spojení v reálném čase v době, kdy je kalibrační signální spojení I/O nastaveno na vstup, pak musí být kalibrační signální spojení I/O nastaveno na výstup nebo musí být vráceno do neaktivního stavu.

CPR_061 Sled musí:

- zajistit komunikaci službou StartCommunication,

- zahájit seřizovací jednání službou StartDiagnosticSession a být v pracovním módu KALIBRACE (pořadí těchto dvou operací není důležité),
- změnit stav výstupu pomocí služby InputOutputControlByIdentifier.

7.1.2 Formát zprávy

CPR_062 Formáty zpráv pro InputOutputControlByIdentifier-primitives jsou rozepsány v níže uvedených tabulkách:

Tabulka 33
Zpráva o požadavku InputOutputControlByIdentifier

Byt #	Název parametru	Hexagonální hodnota	Symbol
#1	Formátový byt – fyzikální adresa	80	FMT
#2	Byt cílové adresy	EE	TGT
#3	Byt adresy zdroje	tt	SRC
#4	Byt dodatečné délky	xx	LEN
#5	Služba Id požadavku InputOutputControlByIdentifier	2F	IOCBI
#6 a #7	InputOutputIdentifier = (CalibrationInputOutput)	F960	IOI_CIO
#8 nebo #8 až #9	ControOptionRecord() = (InputOutputControlParameter - jedna z hodnot v tabulce 36 controlState – jedna z hodnot v tabulce 38 (viz níže)	xx ... xx	COR_... IOCP CS_...
#9 nebo #10	Kontrolní součet	00-FF	CS

Tabulka 34
Zpráva o kladné odezvě InputOutputControlByIdentifier

Byt #	Název parametru	Hexagonální hodnota	Symbol
#1	Formátový byt – fyzikální adresa	80	FMT
#2	Byt cílové adresy	tt	TGT
#3	Byt adresy zdroje	EE	SRC
#4	Byt dodatečné délky	xx	LEN
#5	Služba Id kladné odezvy InputOutputControlByIdentifier	6F	IOCBIPR
#6 a #7	inputOutputIdentifier = (CalibrationInputOutput)	F960	IOI_CIO
#8 nebo #8 až #9	controlStatusRecord = (InputOutputControlParameter - stejná hodnota jako #8 v tabulce 33 controlState – stejná hodnota jako #9 v tabulce 33 (pokud lze užít)	xx xx	CSR_ IOCP_ CS_
#9 nebo #10	Kontrolní součet	00-FF	CS

Tabulka 35
Zpráva o záporné odezvě InputOutputControlByIdentifier

Byt #	Název parametru	Hexagonální hodnota	Symbol
#1	Formátový byt – fyzikální adresa	80	FMT
#2	Byt cílové adresy	tt	TGT
#3	Byt adresy zdroje	EE	SRC

#4	Byt dodatečné délky	03	LEN
#5	Služba Id záporné odezvy	7F	NR
#6	Služba Id požadavku InputOutputControlByIdentifier	2F	IOCB
#7	responseCode = (incorrectMessageLength conditionsNotCorrect requestOutOfRange deviceControlLimitExceeded)	13 22 31 7A	RC_IML RC_CNC RC_ROOR RC_DCLE
#8	Kontrolní součet	00-FF	CS

7.1.3 Definice parametrů

CPR_064 Parametr inputOutputControlParameter (IOCP_) je definován v následující tabulce:

Tabulka 36
Definice hodnot inputOutputControlParameter

Hex	Popis	Symbol
00	ReturnControlToECU Tato hodnota musí indikovat serveru (celku ve vozidle), že zkušební zařízení již neřídí signální spojení kalibrace I/O.	RCTECU
01	ResetToDefault Tato hodnota musí indikovat serveru (celku ve vozidle), že se od něj požaduje nastavení signálního spojení kalibrace I/O do neaktivního stavu.	RTD
03	ShortTermAdjustment Tato hodnota musí indikovat serveru (celku ve vozidle), že se požaduje nastavení signálního spojení kalibrace I/O na hodnotu, obsaženou v parametru controlState.	STA

CTR_065 Parametr controlState je přítomen pouze tehdy, když je inputOutputControlParameter nastaven na ShortTermAdjustment, a parametr je definován v následující tabulce:

Tabulka 37
Definice hodnot controlState

Mód	Hex	Popis
neaktivní	00	I/O spojení je blokováno (stav neplatný)
aktivní	01	Umožňuje kalibrační spojení I/O jako speedSignalInput
aktivní	02	Umožňuje kalibrační spojení I/O jako realTimeSpeedSignalOutputSensor
aktivní	03	Umožňuje kalibrační spojení I/O jako RTCTOutput

8. formáty datarecords

Tato část uvádí:

- obecná pravidla, která se mají užít k uspořádání parametrů, přenesených celkem ve vozidle do zkušebního zařízení,

- formáty, které mají být užity u dat převedených pomocí služby přenosu dat, popsané v části 6.

CPR_067 Veškeré identifikované parametry musí být podporovány celkem ve vozidle.

CPR_068 Data, přenesená celkem ve vozidle do zkušebního zařízení jako odezva na zprávu o požadavku musí být typu změřeného (tj. musí to být současná hodnota požadovaného parametru, změřeného nebo zjištěného celkem ve vozidle).

8.1 Rozsahy přenášených parametrů

CPR_069 Tabulka 38 definuje rozsah, užitý ke stanovení platnosti přenesených parametrů.

CPR_070 Hodnota v rozsahu “error indicator” (indikátor závady) zajišťuje pro celek ve vozidle prostředek pro okamžitou indikaci, že v důsledku nějakého typu závady v záznamovém zařízení nejsou běžně dostupná platná parametrická data.

CPR_071 Hodnoty v rozsahu „not available“ (nedostupné) zajišťují celku ve vozidle prostředek pro přenos zprávy, která obsahuje parametr, který není tímto modulem dostupný nebo který jím není podporován. Hodnoty v rozsahu „not available“ (nedostupné) zajišťují pro zařízení prostředek pro přenos zprávy o povelu a které identifikují tyto parametry tam, kde se nepředpokládá od cílového zařízení žádná odezva.

CPR_072 Pokud závada některé součásti brání přenosu platných dat parametru, je možné místo dat parametru užít indikaci závady podle popisu v tabulce 38. Pokud však měřená nebo vypočtená data poskytují současně platnou hodnotu, která převyšuje definovaný rozsah parametru, neměl by být indikátor závady využit. Data by měla být přenesena využitím přiměřené minimální nebo maximální hodnoty parametru.

Tabulka 38
Rozsahy dataRecords

Název rozsahu	1 byt (hexagonální hodnota)	2 byty (hexagonální hodnota)	4 byty (hexagonální hodnota)	ASCII
Platný signál	00 až FA	0000 až FEFF	00000000 až FFFFFFFF	1 až 254
Indikátor pro parametr	FB	FB00 až FBFF	FB000000 až FBFFFFFF	žádný
Reservní rozsah pro budoucí indikační bity	FC až FD	FC00 až FDFF	FC000000 až FDFFFFFF	žádný
Indikátor závady	FE	FE00 až FEFF	FE000000 až FEFFFFFF	0
Nedostupné nebo nepožadované	FF	FF00 až FFFF	FF000000 až FFFFFFFF	FF

CPR_073 Pro parametry, kódované v ASCII, je ASCII symbol “*” rezervován jako oddělovací znak.

8.2 Formáty dataRecords

Níže uvedené tabulky 39 až 42* rozepisují formáty, které musí být užity při službách ReadDataByIdentifier a WriteDataByIdentifier.

CPR_074 Tabulka 39 uvádí délku, rozložení a pracovní rozsah každého z parametrů, identifikovaných pomocí jeho recordDataIdentifier.

Tabulka 39
Formáty dataRecord

Název parametru	Délka dat (byty)	Rozložení	Pracovní rozsah
TimeDate	8	Detaily viz tabulku 40	
HighResolutionTotalVehicleDistance	4	nárůst 5 m/bit výchozí hodnota 0 m	0 až +21055406 km
Kfactor	2	nárůst 0,001 imp./m/bit výchozí hodnota 0	0 až 64,255 imp./m
LfactorTyreCircumference	2	nárůst 0,125 10 ⁻³ /bit výchozí hodnota 0	0 až 8031 m
WvehicleCharacteristicFactor	2	nárůst 0,001 imp./m/bit výchozí hodnota 0	0 až 64,255 imp./m
TyreSize	15	ASCII	ASCII
NextCalibrationDate	3	Detaily viz tabulku 41	
SpeedAuthorized	2	nárůst 1/256 km/h/bit výchozí hodnota 0	0 až 250996 km/h
RegisteringMemberState	3	ASCII	ASCII
VehicleRegistrationNumber	14	Detaily viz tabulku 42	
VIN	17	ASCII	ASCII

CPR_075 Tabulka 40 rozepisuje formáty různých bytů parametru TimeDate:

Tabulka 40
Rozeepsaný formát TimeDate (recordDataIdentifier, hodnota # F00B)

Byt	Definice parametru	Rozložení	Pracovní rozsah
1	Sekundy	nárůst 0,25 s/bit výchozí hodnota 0 s	0 až 59,75 s
2	Minuty	nárůst 1 min/bit výchozí hodnota 0 min.	0 až 59 min.
3	Hodiny	nárůst 1 h/bit výchozí hodnota 0 h	0 až 23 h
4	Měsíc	nárůst 1 měsíc/bit výchozí hodnota 0 měsíce	1 až 12 měsíců
5	Den	nárůst 0,25 dne/bit výchozí hodnota 0 dne	0,25 až 31,75 dne
6	Rok	nárůst 1 rok/bit + výchozí hodnota +1985 (viz pozn. pod tab. 41)	1985 až r. 2235
7	Místní výchozí hodnota minut	nárůst 1 min./bit výchozí hodnota -125 min.	-59 až 59

* Pozn. překl.: V anglickém textu je chyba v číslování tabulek – překlad upraven podle textu německého.

8	Místní výchozí hodnota hodiny	nárůst 1 h/bit výchozí hodnota -125	-23 až +23 h.
---	-------------------------------	--	---------------

CPR_076 Tabulka 41 rozepisuje formáty různých bytů parametru NextCalibrationDate:

Tabulka 41

Rozepsaný formát NextCalibrationDate (recordDataIdentifier, hodnota # F022)

Byt	Definice parametru	Rozložení	Pracovní rozsah
1	Měsíc	nárůst 1 měsíc/bit výchozí hodnota 0 měsíce	1 až 12 měsíců
2	Den	nárůst 0,25 dne/bit výchozí hodnota 0 dne (viz pozn. níže)	0,25 až 31,75 dne
3	Rok	nárůst 1 rok/bit + výchozí hodnota +1985 (viz pozn. níže)	1985 až r. 2235
<p>Poznámka týkající se užití parametru „den“:</p> <ol style="list-style-type: none"> Hodnota 0 je pro datum nulou. Hodnoty 1,2,3 a 4 se užívají k identifikaci prvního dne v měsíci; 5, 6, 7 a 8 identifikují druhý den v měsíci; atd. Tento parametr neovlivňuje nebo nemění výše uvedený parametr hodin. <p>Poznámka týkající se užití parametru „rok“:</p> <p>Hodnota 0 identifikuje rok 1985; hodnota 1 identifikuje rok 1986; atd.</p>			

CPR_078 Tabulka 42 rozepisuje formáty různých bytů parametru
VehicleRegistrationNumber:

Tabulka 42

Rozepsaný formát VehicleRegistrationNumber (recordDataIdentifier, hodnota #
F07E)

Byt	Definice parametru	Rozložení	Pracovní rozsah
1	Stránka kódu (podle definice v dodatku 1)	ASCII	01 až 0A
2 až 14	Registrační číslo vozidla (podle definice v dodatku 1)	ASCII	ASCII

Dodatek 9

**SCHVÁLENÍ TYPU -
SEZNAM MINIMÁLNÍHO ROZSAHU POŽADOVANÝCH ZKOUŠEK**

OBSAH

OBSAH	267
1. ÚVOD	268
1.1 Schválení typu	268
1.2. Referenční dokumenty	268
2. Funkční zkoušky celku ve vozidle	271
3. FUNKČNÍ ZKOUŠKY SNÍMAČŮ pohybu	275
4. FUNKČNÍ ZKOUŠKY KARET TACHOGRAFU	278
5. ZKOUŠKY VZÁJEMNÉ OPERAČNÍ SOUČINNOSTI	279

1. 1. ÚVOD

1.1. Schválení typu

EHS schválení typu se pro záznamové zařízení (nebo jeho součást) nebo pro kartu tachografu zakládá na:

- certifikaci bezpečnosti, kterou zajišťuje orgán ITSEC vůči bezpečnostním úkolům zcela v souladu s dodatkem 10 této přílohy;
- certifikaci funkčnosti, zajišťovanou orgánem členského státu, která potvrzuje, že zkoušená položka splňuje požadavky této přílohy z hlediska prováděných funkcí, přesnosti měření a ekologických charakteristik;
- certifikaci vzájemné operační součinnosti, zajišťovanou oprávněnou organizací, která potvrzuje, že záznamové zařízení (nebo karta tachografu) je plně provozuschopná s příslušným modelem karty tachografu (nebo záznamového zařízení) (viz kapitolu VIII této přílohy).

Tato příloha stanoví formou minimálních požadavků, jaké zkoušky musí provést orgán členského státu během funkčních zkoušek a jaké oprávněná organizace během zkoušek vzájemné operační součinnosti. Postup při zkouškách ani typy zkoušek se více neurčují.

Aspekty certifikace bezpečnosti nejsou v této příloze obsaženy. Pokud se některé ze zkoušek, vyžadovaných pro schválení typu, provedou v průběhu hodnocení a certifikace bezpečnosti, není třeba takové zkoušky opakovat. V tomto případě se mohou posuzovat jenom výsledky z těchto bezpečnostních zkoušek. Pro informaci se v tomto dodatku značkou „*“ doprovázejí požadavky, u nichž se očekává, že budou testovány (nebo blíže vázány ke zkouškám, jejichž provedení se očekává) během certifikace bezpečnosti.

V tomto dodatku se uvažuje schválení typu snímačů pohybu odděleně od celku ve vozidle, neboť jde o části záznamového zařízení. Protože není požadována vzájemná operační součinnost všech modelů snímačů pohybu se všemi modely celků ve vozidle, může se udělit schválení typu snímače pohybu jen ve spojení se schválením typu celku ve vozidle a naopak.

1.2. Referenční dokumenty

Referenční dokumenty použité v tomto dodatku:

- | | |
|------------|--|
| IEC 68-2-1 | Environmental testing – Part 2: Tests – Tests A: Cold. 1990 + Amendment 2: 1994. |
| IEC 68-2-2 | Environmental testing – Part 2: Tests – Tests B: Dry heat. 1974 + Amendment 2: 1994. |
| IEC 68-2-6 | Basic environmental testing procedures – Test methods – Test Fc and guidance: Vibration (sinusoidal). 6th edition: 1985. |

- IEC 68-2-14 Basic environmental testing procedures – Test methods –Test N: Change of temperature. Modification 1: 1986.
- IEC 68-2-27 Basic environmental testing procedures – Test methods –Test Ea and guidance: Shock. Edition 3: 1987.
- IEC 68-2-30 Basic environmental testing procedures – Test methods –Test Db and guidance: Damp heat, cyclic (12 + 12 – hour cycle). Modification 1: 1985.
- IEC 68-2-35 Basic environmental testing procedures – Test methods –Test Fda: Random vibration wide band – Reproducibility High. Modification 1: 1983.
- IEC 529 Degrees of protection provided by enclosures (IP code). Edition 2: 1989.
- IEC 61000-4-2 Electromagnetic Compatibility (EMC) – Testing and measurement techniques – Electrostatic discharge immunity test: 1995/Amendment 1: 1998.
- ISO 7637-1 Road vehicles – Electrical disturbance by conduction and coupling – Part 1: Passenger cars and light commercial vehicles with nominal 12 V supply voltage – Electrical transient conduction along supply lines only. Edition 2: 1990. *(Silniční vozidla. Elektrické rušení vedením a vazbou. Část 1: Osobní automobily a lehká komerční vozidla se stejnosměrným napájecím napětím 12 V - Šíření elektrického přechodového jevu pouze po napájecím vedení)*
- ISO 7637-2 Road vehicles – Electrical disturbance by conduction and coupling – Part 2: Commercial vehicles with nominal 24 V supply voltage – Electrical transient conduction along supply lines only. Edition 2: 1990. *(Silniční vozidla. Elektrické rušení vedením a vazbou. Část 2: Komerční vozidla se stejnosměrným napájecím napětím 24 V - Šíření elektrického přechodového jevu pouze po napájecím vedení)*
- ISO 7637-3 Road vehicles – Electrical disturbance by conduction and coupling – Part 3: Vehicles with nominal 12 V or 24 V supply voltage – Electrical transient transmission by capacitive and inductive coupling via lines other than supply lines. First edition: 1995 + Cor 1: 1995. *(Silniční vozidla. Elektrické rušení vedením a vazbou. Část 3: Vozidla s jmenovitým napětím 12 V nebo 24 V - Elektrický přenos přechodových jevů kapacitní a induktivní vazbou vedeními jinými než napájecími vedeními)*
- ISO/IEC 7816-1 Identification cards – Integrated circuit(s) cards with contacts - Part 1: Physical characteristics. First edition: 1998. *(Identifikační karty. Karty s integrovanými obvody a s kontakty. Část 1: Fyzikální vlastnosti)*

ISO/IEC 7816-2 Information technology – Identification cards - Integrated circuit(s) cards with contacts- Part 2: Dimensions and location of the contacts. First edition: 1999. (*Informační technika. Identifikační karty. Karty s integrovanými obvody a s kontakty. Část 2: Rozměry a umístění kontaktů*)

ISO/IEC 7816-3 Information technology – Identification cards - Integrated circuit(s) cards with contacts- Part 3: Electronic signals and transmission protocols. Edition 2: 1997. (*Informační technika. Identifikační karty. Karty s integrovanými obvody a s kontakty. Část 3: Elektronické signály a protokoly přenosu*)

ISO/IEC 1373 Identification cards – Test methods. First edition: 1993. (*Identifikační karty. Zkušební metody*)

2. 2. FUNKČNÍ ZKOUŠKY CELKU VE VOZIDLE

Bod	Zkouška	Popis	Odpovídající požadavky
1.	Administrativní prověrka		
1.1.	Dokumentace	Správnost dokumentace	
1.2.	Výsledky zkoušek výrobce	Výsledky zkoušek provedených výrobcem při zástavbě. Předložení písemných dokladů	070, 071, 073
2.	Vizuální kontrola		
2.1.	Shoda s dokumentací		
2.2.	Identifikace / Značení		168, 169
2.3.	Materiály		163 až 167
2.4.	Plombování přístroje		251
2.5.	Vnější rozhraní		
3.	Funkční zkoušky		
3.1.	Rozsah funkcí		002, 004, 244
3.2.	Druhy provozu		006*, 007*, 008*, 009*, 106, 107
3.3.	Přístupová práva k funkcím a datům		010*, 011*, 240, 246, 247
3.4.	Dozor nad vložením a odebíráním karet		013, 014, 015*, 016*, 106
3.5.	Měření rychlosti a dráhy		017 až 026
3.6.	Měření času (zkouška při 20 ⁰ C)		027 až 032
3.7.	Sledování činností řidiče		033 až 043, 106
3.8.	Sledování průběhu řízení		044, 045, 106
3.9.	Ruční zadání řidičem		046 až 050b
3.10.	Správa podnikových uzávěrů		051 až 055

Bod	Zkouška	Popis	Odpovídající požadavky
3.11.	Sledování kontrolních činností		056, 057
3.12.	Zjišťování událostí a/nebo závad		059 až 069, 106
3.13.	Identifikační údaje jednotky instalované ve vozidle		075*, 076*, 079
3.14.	Údaje o vložení a odebrání řidičovy karty		081* až 083*
3.15.	Údaje o činnosti řidiče		084* až 086*
3.16.	Údaje o místě na začátku a konci pracovního dne		087* až 089*
3.17.	Údaje o stavu km ujetých vozidlem		090* až 092*
3.18.	Podrobné údaje o rychlosti jízdy		093*
3.19.	Údaje o událostech		094*, 095*
3.20.	Údaje o závadách		096*
3.21.	Údaje o kalibraci		097*, 098*
3.22.	Údaje o nastavení času		100*, 101*
3.23.	Údaje o kontrolní činnosti		102*, 103*
3.24.	Údaje o podnikových uzávěrech		104*
3.25.	Údaje o zavádění programů (<i>download activities</i>)		105*
3.26.	Údaje o specifických podmínkách		105a*, 105b*
3.27.	Zápis a uložení údajů na kontrolní karty		108, 109*, 109a*, 110*, 111, 112
3.28.	Zobrazení dat		072, 106, 113 až 128, PIC_001, DIS_001
3.29.	Tisk dat		072, 106, 129 až 138, PIC_001, PRT_001 až PRT_012
3.30.	Výstraha		106, 139 až 148, PIC_001
3.31.	Zavádění údajů na externí nosiče		072, 106, 149 až 151

Bod	Zkouška	Popis	Odpovídající požadavky
3.32.	Výstup údajů na přídavné externí přístroje		152, 153
3.33.	Kalibrace		154*, 155*, 156*, 245
3.34.	Nastavení času		157*, 158*
3.35.	Nenarušenost přídavných funkcí		003, 269
4.	Ekologické zkoušky		
4.1.	Teplota	<p>Prokázat provozuschopnost podle:</p> <ul style="list-style-type: none"> - IEC 68-2-1, zkouška Ad s trváním 72 hod při nižší teplotě (-20°C), 1 hod v provozu, 11 hod mimo provoz, - IEC 68-2-2, zkouška Bd s trváním 72 hod při vyšší teplotě ($+70^{\circ}\text{C}$), 1 hod v provozu, 1 hod mimo provoz, <p>Teplotní cykly: prokázat zkouškou Na, že celek ve vozidle odolá rychlým změnám okolní teploty podle IEC 68-2-14, 20 cyklů, každý se změnou teploty od dolní teploty (-20°C) k horní teplotě ($+70^{\circ}\text{C}$) a s výdrží 2 hod na každé dolní i horní teplotě.</p> <p>Snížit počet zkoušek (z těch uvedených v úseku 3 této tabulky) je přípustné s odvoláním na dolní a horní teplotu a na průběh teplotních cyklů.</p>	159
4.2.	Vlhkost vzduchu	IEC 68-2-30, zkouškou Db prokázat, že celek ve vozidle vydrží cyklickou zkoušku vlhkosti (zkoušku teplotní) o šesti 24 hod cyklech, každý se změnou teploty od $+25^{\circ}\text{C}$ do $+55^{\circ}\text{C}$ při relativní vlhkosti od 97 % při $+25^{\circ}\text{C}$ event. 93 % při $+55^{\circ}\text{C}$	160
4.3.	Kmitání	<p>1. Sinusové kmitání:</p> <p>Prokázat, že celek ve vozidle vyhoví těmto parametrům sinusového kmitání:</p> <ul style="list-style-type: none"> -konstantní výchylka dráhy mezi 5 a 11 Hz: max.10 mm -konstantní zrychlení mezi 11 a 300 Hz: 	163

Bod	Zkouška	Popis	Odpovídající požadavky
		5^0g Průkaz podle IEC 68-2-6 zkouškou Fc o délce nejméně 3x12 hod (12 hod za každou nápravu) 2. Náhodné kmitání: Prokázat, že celek ve vozidle vyhoví těmto parametrům náhodného kmitání: -Frekvence 5 až 150 Hz, úroveň 0,02 g^2/Hz Průkaz podle IEC 68-2-35 zkouškou Ffda o délce nejméně 3x12 hod (12 hod za každou nápravu), 1 hod v provozu, 1 hod mimo provoz Každá z těchto dvou zkoušek se provede na jiném vzorku zkoušeného typu přístroje	
4.4.	Ochrana proti vodě a cizím tělesům	Prokázat, že index ochrany celku ve vozidle v podmínkách podle IEC 529 dosahuje nejméně hodnoty IP 40	164, 165
4.5.	Ochrana proti přepětí	Prokázat, že celek ve vozidle vydrží tato napájecí napětí: -modely pro jmenovité napětí 24 V: 34 V při $+40^0\text{C}$ po 1 hod -modely pro jmenovité napětí 12 V: 17 V při $+40^0\text{C}$ po 1 hod	161
4.6.	Ochrana proti záměně polarity	Prokázat, že celek ve vozidle vydrží přepólování napájecího napětí	161
4.7.	Ochrana proti zkratu	Prokázat, že vstupní a výstupní signály jsou chráněny proti zkratu v živém vodiči i v uzemnění	161
5.	Zkoušky elektromagnetické slučitelnosti		

Bod	Zkouška	Popis	Odpovídající požadavky
5.1.	Vyzářené rušení a citlivost na rušení	Splnění směrnice 95/54/EEC	162
5.2.	Vybíjení elektrostatického náboje	Splnění IEC 61000-4-2, ± 2 kV (úroveň 1)	162
5.3.	Citlivost na rušení po vedení na datových vodičích	<p>Pro modely 24 V: splnění ISO 7637-2:</p> <p>Impuls 1a: $V_s = -100$ V, $R_i = 10$ Ohm</p> <p>Impuls 2: $V_s = +100$ V, $R_i = 10$ Ohm</p> <p>Impuls 3a: $V_s = -100$ V, $R_i = 50$ Ohm</p> <p>Impuls 3b: $V_s = +100$ V, $R_i = 50$ Ohm</p> <p>Impuls 4: $V_s = -16$ V, $V_a = -5$ V, $t_6 = 15$ ms</p> <p>Impuls 5: $V_s = +65$ V, $R_i = 5$ Ohm, $t_d = 100$ ms</p> <p>Impuls 5 se zkouší jen u jednotek pro instalaci v těch vozidlech, která nejsou vybavena žádnou vnější společnou ochranou pro zatížení naprázdno</p>	162

2.1.**3. 3. FUNKČNÍ ZKOUŠKY SNÍMAČŮ POHYBU**

Bod	Zkouška	Popis	Odpovídající požadavky
1.	Administrativní prověrka		
1.1.	Dokumentace	Správnost dokumentace	
2.	Vizuální kontrola		
2.1.	Shoda s dokumentací		
2.2.	Identifikace / Značení		169, 170

Bod	Zkouška	Popis	Odpovídající požadavky
2.3.	Materiály		163 až 167
2.4.	Plombování přístroje		251
3.	Funkční zkoušky		
3.1.	Identifikační údaje snímače pohybu		077*
3.2.	Párování snímače pohybu s celkem ve vozidle		099*, 155
3.3.	Záznam dráhy/rychlosti		
	Přesnost měření dráhy/rychlosti		022 až 026
4.	Ekologické zkoušky		
4.1.	Provozní teplota	Prokázat provozuschopnost (jak stanoveno ve zkoušce č.3.3) v teplotním rozsahu [-40 ⁰ C; +135 ⁰ C] podle: - IEC 68-2-1, zkouška Ad s trváním 96 hod při nejnižší teplotě To _{min} - IEC 68-2-2, zkouška Bd s trváním 96 hod při nejvyšší teplotě To _{max}	159
4.2.	Teplotní cykly	Prokázat provozuschopnost (jak stanoveno ve zkoušce č.3.3) podle IEC 68-2-14, zkouška Na, 20 cyklů, každý se změnou teploty od dolní teploty (-40 ⁰ C) k horní teplotě (+135 ⁰ C) a s výdrží 2 hod na každé dolní i horní teplotě. Snížit počet zkoušek (z těch ve zkoušce 3.3 uvedených) je přípustné s odvoláním na dolní a horní teplotu a na průběh teplotních cyklů.	159
4.3.	Vlhkostní cykly	Prokázat provozuschopnost (jak stanoveno ve zkoušce č.3.3) podle IEC 68-2-30, zkouška Db, šest 24 hod cyklů, každý se změnou teploty od +25 ⁰ C do +55 ⁰ C při relativní vlhkosti od 97 % při +25 ⁰ C event. 93 % při +55 ⁰ C	160
4.4.	Kmitání	Prokázat provozuschopnost (jak stanoveno ve zkoušce č.3.3) podle IEC 68-2-6	163

Bod	Zkouška	Popis	Odpovídající požadavky
		ve zkoušce č.3.3) podle IEC 68-2-6, zkouška Fc v trvání 100 frekvenčních cyklů: -konstantní výchylka dráhy mezi 10 a 57 Hz: max.1,5 mm -konstantní zrychlení mezi 57 a 500 Hz: 20 g	
4.5.	Mechanický náraz	Prokázat provozuschopnost (jak stanoveno ve zkoušce č.3.3) podle IEC 68-2-27, zkouška Ea, tři nárazy v obou směrech 3 vzájemně kolmých os	163
4.6.	Ochrana proti vodě a cizím tělesům	Prokázat, že index ochrany snímače pohybu, zabudovaného ve vozidle za provozních podmínek, podle IEC 529 dosahuje nejméně hodnoty IP 64	165
4.7.	Ochrana proti záměně polarity	Prokázat, že snímač pohybu vydrží přepólování napájecího napětí	161
4.8.	Ochrana proti zkratu	Prokázat, že vstupní a výstupní signály jsou chráněny proti zkratu v živém vodiči i v uzemnění	161
5.	Zkoušky elektromagnetické slučitelnosti		
5.1.	Vyzářené rušení a citlivost na rušení	Splnění směrnice 95/54/EEC	162
5.2.	Vybíjení elektrostatického náboje	Splnění IEC 61000-4-2, ± 2 kV (úroveň 1)	162
5.3.	Citlivost na rušení po vedení na datových vodičích	Splnění ISO 7637-3 (úroveň III)	162

4. FUNKČNÍ ZKOUŠKY KARET TACHOGRAFU

Bod	Zkouška	Popis	Odpovídající požadavky
1.	Administrativní prověrka		
1.1.	Dokumentace	Správnost dokumentace	
2.	Vizuální kontrola		
2.1.	Shoda s dokumentací	Přesvědčit se, že všechna bezpečnostní opatření a viditelné údaje jsou správně vytištěny na kartě a vyhovují zadání	171 až 181
3.	Fyzikální zkoušky		
3.1.		Kontrolovat rozměry a polohu kontraktů	184 ISO/IEC 7816-1 ISO/IEC 7816-2
4.	Zkoušky protokolu		
4.1.	ATR	Kontrolovat, že ATR splňuje požadavky	ISO/IEC 7816-3 TCS 304,307,308
4.2.	T=0	Kontrolovat, že protokol T=0 splňuje požadavky	ISO/IEC 7816-3 TCS 302,303,305
4.3.	PTS	Kontrolovat, že příkaz PTS při nastavení T=1 z výchozího T=0 splňuje požadavky	ISO/IEC 7816-3 TCS 309 až 311
4.4.	T=1	Kontrolovat, že protokol T=1 splňuje požadavky	ISO/IEC 7816-3 TCS 303, / 306
5.	Struktura karty		
5.1.		Přezkoušet, že struktura souboru karty splňuje požadavky. K tomu se	TCS 312 TCS 400*,401,402,403*,

Bod	Zkouška	Popis	Odpovídající požadavky
		kontroluje přítomnost povinných souborů na kartě a podmínek přístupu k nim	404,405*,406,07,408*, 409,410*,411,412,413*, 414,415*,416,417,418*, 419
6.	Funkční zkoušky		
6.1.	Normální zpracování	Pro každý příkaz přezkoušet každou přípustnou odezvu nejméně jednou (např.: zkoušet příkaz UPDATE BINARY pro CLA='00', CLA='0C', s různými parametry P1, P2 a Lc). Kontrolovat, že operace skutečně na kartě proběhly (např.: pročtením souboru, kde se provedl příkaz)c	TCS 313 to TCS 379
6.2.	Chybová hlášení	Pro každý příkaz přezkoušet každé chybové hlášení (podle specifikace v příloze 2) nejméně jednou. Každou generickou chybu je nutno nejméně jednou přezkoušet (s výjimkou chyb úplnosti (integrity) '6400' kontrolovaných během certifikace bezpečnosti)	
7.	Ekologické zkoušky		
7.1.		Přesvědčit se, že karty pracují uvnitř mezních podmínek stanovených v souladu s ISO/IEC 10373	185 až 188 ISO/IEC 7816-1

5. 5. ZKOUŠKY VZÁJEMNÉ OPERAČNÍ SOUČINNOSTI

Bod	Zkouška	Popis
1.	Vzájemné určení totožnosti	Kontrolovat, že vzájemné ověření operační součinnosti mezi celkem ve vozidle a kartou tachografu probíhá normálně

Bod	Zkouška	Popis
2.	Písemné/slovní zkoušky	Realizovat typický scénář činnosti celku ve vozidle. Scénář se musí upravit pro prověřovaný typ karty a zahrnout tolik zápisů jízd a rušení, kolik tato karta umožňuje. Prověřit nahrávkou karty, zda proběhly řádně všechny záznamy. Prověřit denními tisky z karty, zda všechny odpovídající nákresy mohou být řádně přečteny.

*Dodatek 10***VŠEOBECNÉ POŽADAVKY NA BEZPEČNOST**

Tato příloha stanovuje minimální bezpečnostní požadavky na snímače pohybu, celku ve vozidle a karty tachografu.

Pro stanovení požadavků na bezpečnost které musí být splněny při žádosti o certifikaci bezpečnosti, musí výrobci konkretizovat a vyplnit nezbytné dokumenty, aniž by v nich měnili nebo vypouštěli existující specifikace možného ohrožení bezpečnosti a cílů, skutečností a funkce zajišťující bezpečnost..

OBSAH**Všeobecné požadavky na bezpečnost snímačů pohybu**

VŠEOBECNÉ POŽADAVKY NA BEZPEČNOST	281
Všeobecné požadavky na bezpečnost snímačů pohybu	286
1. Úvod	286
2. Zkratky, definice a odkazy.....	286
2.1 Zkratky.....	286
2.2 Definice.....	286
2.1 Odkazy	287
3. Princip výrobku	287
3.1 Popis snímače pohybu a postup užití.....	287
3.2 Životnostní cyklus snímače pohybu	288
3.3 Ohrožení bezpečnosti.....	289
3.3.1 Ohrožení bezpečnosti v souvislosti s kontrolou zásahů.....	289
3.3.2 Ohrožení bezpečnosti v souvislosti s konstrukcí	289
3.3.3 Ohrožení bezpečnosti v souvislosti s provozem	290
3.4 Cíle bezpečnosti.....	290
3.5 Cíle bezpečnosti informační technologie.....	290
3.6 Prostředky fyzikální, personální a procedurální	291
3.6.1 Konstrukce zařízení	291
3.6.2 Dodávka zařízení	291
3.6.3 Generace bezpečnostních dat a jejich dodávka.....	291
3.6.4 Montáž, kalibrace a kontrola záznamového zařízení.....	291
3.6.5 Kontrola dodržování předpisů	292
3.6.6 Upgrade (modernizace) softwaru	292
4. Funkce zajišťující bezpečnost.....	292
4.1 Identifikace a prokázání totožnosti	292

4.2	Kontrola přístupu	293
4.2.1	Postup kontroly postupu	293
4.2.2	Práva přístupu k datům	293
4.2.3	Struktura souboru a podmínka přístupu	293
4.3	Možnosti přiřazení	293
4.4	Audit	293
4.5	Přesnost	294
4.5.1	Postup kontroly toku informací	294
4.5.2	Interní přenos dat	294
4.5.3	Úplnost (integrita) uložených dat	294
4.6	Spolehlivost funkce	295
4.6.1	Zkoušky	295
4.6.2	Software	295
4.6.3	Fyzická ochrana	295
4.6.4	Přerušení napájení	295
4.6.5	Obnovení nastavení (resetování)	295
4.6.6	Dostupnost dat	296
4.6.7	Vícefunkční využití	296
4.7	Výměna dat	296
4.8	Podpora šifrováním	296
5.	Definice bezpečnostních mechanismů	296
6.	Minimální pevnost bezpečnostních mechanismů	296
7.	Úroveň zajištění	297
8.	Základní principy	297
	Všeobecné požadavky na bezpečnost celku ve vozidle	299
1.	Úvod	299
2.	Zkratky, definice a odkazy	299
2.1	Zkratky	299
2.2	Definice	299
2.1	Odkazy	300
3.	Princip výrobku	300
3.1	Popis celku ve vozidle a postup užití	300
3.2	Životní cyklus celku do vozidla	302
3.3	Ohrožení bezpečnosti	303
3.3.1	Ohrožení identifikace a postupu kontroly přístupu	303
3.3.2	Ohrožení bezpečnosti v souvislosti s konstrukcí	303
3.3.3	Ohrožení bezpečnosti v souvislosti s provozem	304

3.4	Cíle bezpečnosti	304
3.5	Cíle bezpečnosti informační technologie	305
3.6	Prostředky fyzikální, personální a procedurální	305
3.6.1	Konstrukce zařízení	305
3.6.2	Dodávka a aktivace zařízení	306
3.6.3	Generace bezpečnostních dat a jejich dodávka	306
3.6.4	Dodávka karet	306
3.6.5	Montáž, kalibrace a kontrola záznamového zařízení	306
3.6.6	Provoz zařízení	306
3.6.7	Kontrola dodržování předpisů	306
3.6.7	Upgrade (modernizace) softwaru	307
4.	Funkce zajišťující bezpečnost	307
4.1	Identifikace a prokázání totožnosti	307
4.1.1	Identifikace a prokázání totožnosti snímače pohybu	307
4.1.2	Identifikace a prokázání totožnosti uživatele	307
4.2	Kontrola přístupu	309
4.2.1	Postup kontroly postupu	309
4.2.2	Práva přístupu k datům	309
4.2.3	Práva přístupu k datům	309
4.2.4	Struktura souboru a podmínka přístupu	310
4.3	Možnosti přiřazení	310
4.4	Audit	310
4.5	Obnova využití paměti	311
4.6	Přesnost	311
4.6.1	Postup kontroly toku informací	311
4.6.2	Interní přenos dat	312
4.6.3	Úplnost (integrita) uložených dat	312
4.7	Spolehlivost funkce	312
4.7.1	Zkoušky	312
4.7.2	Software	312
4.7.3	Fyzická ochrana	312
4.7.4	Přerušování napájení	313
4.7.5	Obnovení nastavení (resetování)	313
4.7.6	Dostupnost dat	313
4.7.7	Vícefunkční využití	313
4.8	Výměna dat	314
4.8.1	Výměna dat se snímačem pohybu	314
4.8.2	Výměna dat s kartou tachografu	314

4.8.3	Výměna dat s externími paměťovými médii (přenosové funkce)	314
4.9	Podpora šifrováním	314
5.	Definice bezpečnostních mechanismů	315
6.	Minimální pevnost bezpečnostních mechanismů	315
7.	Úroveň zajištění	315
8.	Základní principy	315
	Všeobecné požadavky na bezpečnost karty tachografu	320
1.	Úvod	320
2.	Zkratky, definice a odkazy	320
2.1	Zkratky	320
2.2	Definice	321
2.1	Odkazy	321
3.	Princip výrobku	322
3.1	Popis karty tachografu a postup užití	322
3.2	Životní cyklus karty tachografu	322
3.3	Ohrožení bezpečnosti	322
3.3.1	Konečné cíle	322
3.3.2	Cesty napadení	323
3.4	Cíle bezpečnosti	323
3.5	Cíle bezpečnosti informační technologie	323
3.6	Prostředky fyzikální, personální a procedurální	324
4.	Funkce zajišťující bezpečnost	324
4.1	Vyhovění ochranným profilům	324
4.2	Identifikace a prokázání totožnosti uživatele	324
4.2.1	Identifikace uživatele	324
4.2.2	Prokázání totožnosti uživatele	324
4.2.3	Selhání v prokázání totožnosti	325
4.3	Kontrola přístupu	325
4.3.1	Postup kontroly přístupu	325
4.3.2	Funkce kontroly přístupu	326
4.4	Možnost přiřazení	326
4.5	Audit	326
4.6	Přesnost	326
4.6.1	Úplnost (integritu uložených dat	326
4.6.2	Prokázání totožnosti základních dat	327
4.7	Spolehlivost funkce	327

4.7.1	Zkoušky	327
4.7.2	Software	327
4.7.3	Napájení	327
4.8	Výměna dat	327
4.8.1	Výměna dat s celkem ve vozidle	327
4.8.2	Export dat do celků mimo vozidlo (funkce převedení)	328
4.9	Podpora šifrováním	328
5.	Definice bezpečnostních mechanismů	328
6.	Minimální pevnost bezpečnostních mechanismů	328
7.	Úroveň zajištění	328
8.	Základní principy	329

VŠEOBECNÉ POŽADAVKY NA BEZPEČNOST SNÍMAČŮ POHYBU

1. Úvod

Tento dokument obsahuje popis snímače pohybu, možná ohrožení bezpečnosti, kterým musí být snímač schopen odolávat a bezpečnostních zajištění, která musí snímač mít k dispozici. Stanovuje funkce uplatňované na požadovanou bezpečnost. Stanovuje požadovanou minimální pevnost bezpečnostního mechanismu a požadovanou úroveň zajištění vývoje a hodnocení.

Požadavky, které dokument stanovuje, odpovídají hlavní části přílohy IB. V zájmu lepší srozumitelnosti může někdy docházet k duplicitě mezi požadavky hlavní části přílohy IB a požadavky záměrů bezpečnosti. V případě nejednoznačnosti požadavků bezpečnostních záměrů a požadavků hlavní části přílohy IB v oblasti požadavků bezpečnostních záměrů, jsou rozhodující požadavky hlavní části přílohy IB.

Požadavky hlavní části přílohy IB, které nejsou uvedeny v bezpečnostních záměrech, nejsou předmětem funkcí zajišťujících bezpečnost.

Pro lepší přiřazení současných pojmů k dokumentaci o vývoji a hodnocení jsou pro možná ohrožení bezpečnosti a plnění cílů, skutečností, a SEF specifikacím přidělena jednotná označení.

2. Zkratky, definice a odkazy

2.1 Zkratky

ROM Read only memory (permanentní paměť)

SEF funkce zajišťující bezpečnost

TBD To be defined (je třeba definovat)

TOE Cíl hodnocení

VU Celek ve vozidle

2.2 Definice

Digitální tachograf Záznamové zařízení

Jednotka Zařízení, připojené na snímač pohybu

Data o pohybu Data, sdílené s VU, reprezentující rychlost a ujetou vzdálenost

Fyzicky oddělené části Fyzické části snímače pohybu, které jsou rozloženy po vozidle, jako protiklad k fyzickým součástem soustředěným

v pouzdře snímače pohybu

Bezpečnostní data	Specifická data, potřebná pro podporu funkcí zajišťujících bezpečnost (např. kódovací klíče)
System	Zařízení, osoby nebo organizace, jakkoliv související se záznamovým zařízením
Uživatel	Osoba, užívající snímač pohybu (pokud není užit ve smyslu „data uživatele“)
Data uživatele	Jakákoliv data jiná než údaje o pohybu nebo bezpečnosti, zaznamenané nebo uložené snímačem pohybu

2.1 Odkazy

ITSEC Information Technology Security Evaluation Kriteria 1991 = informace o kritériích hodnocení bezpečnostní technologie 1991.

3. Princip výrobku

3.1 Popis snímače pohybu a postup užití

Snímač pohybu je určen k montáži do dopravních prostředků. Jeho účelem je zajistit vozidlu bezpečná data, reprezentativní pro rychlost a ujetou vzdálenost.

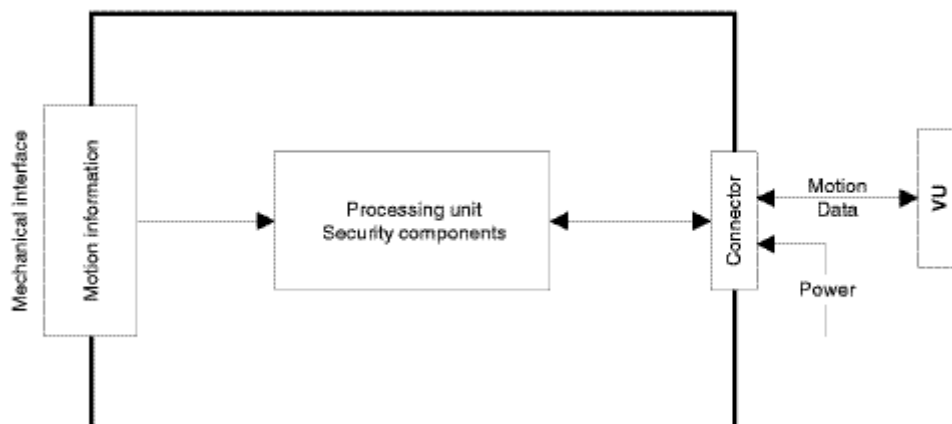
Snímač pohybu je mechanicky propojen s pohybující se částí vozidla, jejíž pohyb může být reprezentativní pro rychlost vozidla nebo pro vozidlem ujetou vzdálenost. Snímač může být umístěn v převodové skříní vozidla nebo v kterékoliv jiné konstrukční části vozidla.

V provozním stavu je snímač pohybu propojen s VU.

Snímač pohybu může být připojen na zvláštní zařízení pro provozní účely (definuje výrobce).

Typický snímač pohybu je popsán v následujícím obrázku:

Obr. 1
Typický snímač pohybu



Mechanical interface = mechanické propojení

Motion information = informace o pohybu

Processing unit = zpracovatelská jednotka

Security components = součásti zabezpečení

Connector = konektor

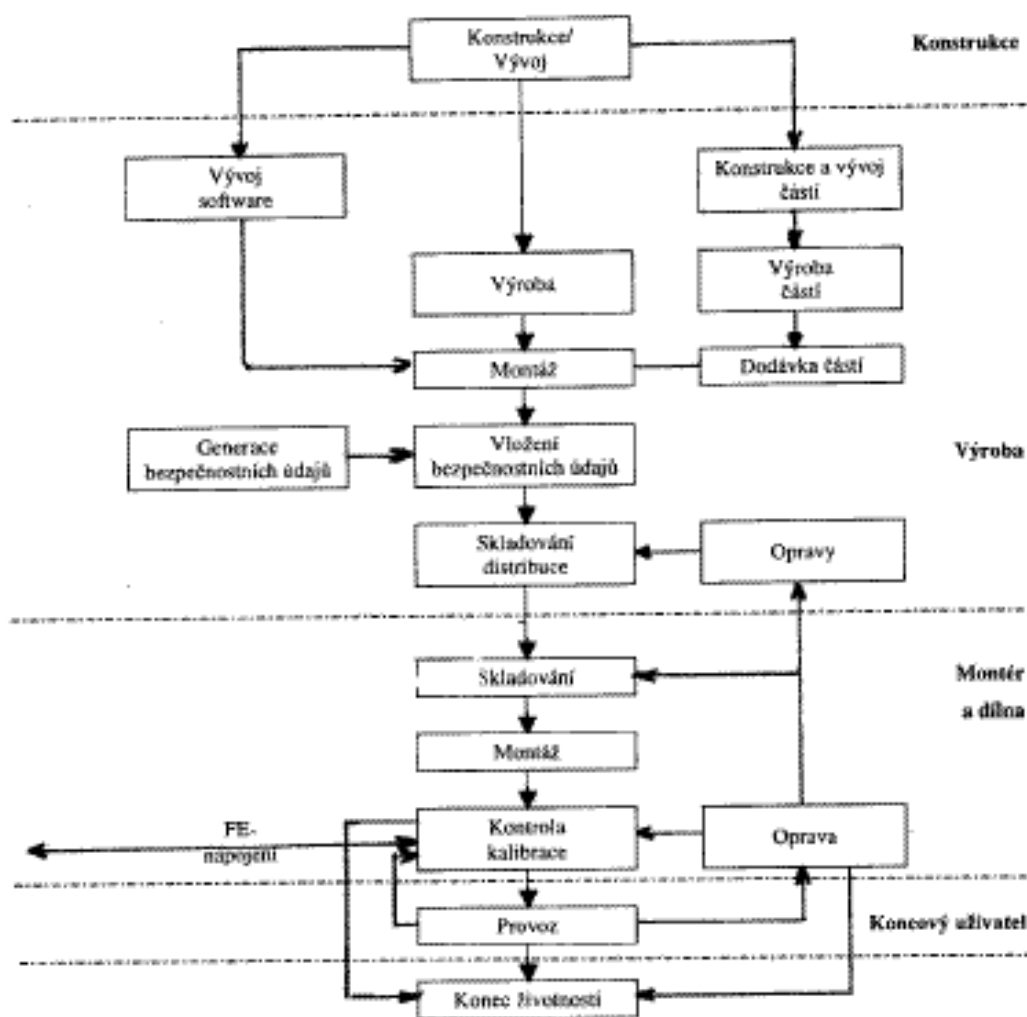
Motion data = data o pohybu

Power = napájení

5.1. 3.2 Životnostní cyklus snímače pohybu

Typický životnostní cyklus snímače pohybu popisuje následující vyobrazení:

Obr. 2
Typický životnostní cyklus snímače pohybu



3.3 Ohrožení bezpečnosti

Tento podstavec popisuje ohrožení bezpečnosti, kterým může být snímač pohybu vystaven.

3.3.1 Ohrožení bezpečnosti v souvislosti s kontrolou zásahů

T.Access Uživatel se pokusil o přístup k funkcím, ke kterým mu přístup není povolen.

3.3.2 Ohrožení bezpečnosti v souvislosti s konstrukcí

T.Faults Závady v hardware, software nebo v komunikačních postupech, které mohou snímač pohybu uvést do nepředpokládaných podmínek, ohrožujících bezpečnost.

T.Test Užití neplatných zkušebních módů nebo existující možnost „vstupu zadními dveřmi“, které mohou ovlivnit bezpečnost snímače pohybu.

T.Design Snaha uživatele o ilegální získání znalostí o konstrukci ať již z podkladů výrobce (loupeží, korupcí, atd.) nebo metodami zpětných technik.

3.3.3 *Ohrožení bezpečnosti v souvislosti s provozem*

T.Environment Ohrožení bezpečnosti snímače pohybu uživatelem vnějším vlivem (tepelně, elektromagneticky, opticky, chemicky, mechanicky atd.).

T.Hardware Pokus uživatele měnit hardware snímače pohybu.

T.Mechanical_Origin Pokus uživatele o manipulaci se snímačem pohybu (např. demontáž z převodové skříně atd.).

T.Motion_Data Pokus uživatele o manipulaci s daty o pohybu vozidla (přidání, změna, vypuštění, přehrání signálu).

T.Power_Supply Pokus uživatele o ovlivnění bezpečnostních opatření u snímače pohybu změnou napájení (rozpojení vedení, snížení nebo zvýšení napětí).

T.Security_Data Pokus uživatele o ilegální získání dat při generaci bezpečnostních údajů s průběhu generace dat, při dopravě nebo při skladování zařízení.

T.Software Pokus uživatele o modifikaci software snímače pohybu.

T.Stored_Data Pokus uživatele o změnu uložených údajů (bezpečnostní data nebo data o uživateli).

3.4 **Cíle bezpečnosti**

Hlavním cílem systému digitálního tachografu je následující:

O.Main Kontrolním orgánům musí být ke kontrole dostupná data, data musí plně a přesně udávat aktivity kontrolovaného řidiče a vozidla z hlediska doby jízdy, doby pracovní pohotovosti, doby odpočinku a rychlosti vozidla.

K cílům všeobecné bezpečnosti přispívají proto cíle bezpečnosti snímače pohybu takto:

O.Sensor_Main Data snímače pohybu musí být dosažitelné ve VU tak, aby VU mohlo plně a přesně stanovit pohyb vozidla z hlediska jeho rychlosti a jím ujeté vzdálenosti.

3.5 **Cíle bezpečnosti informační technologie**

Specifické cíle bezpečnosti informační technologie o snímání pohybu, které přispívají k jeho celkové bezpečnosti, jsou následující:

- O.Access Snímač pohybu musí řídit funkce a data připojených jednotek.
- O.Audit Snímač pohybu musí monitorovat pokusy o obcházení jeho bezpečnostních opatření a musí o nich předávat informace připojeným jednotkám.
- O.Authentication Snímač pohybu musí stanovit totožnost připojených jednotek
- O.Processing Snímač pohybu musí zajistit aby postup zpracování vstupních dat, ze kterých se odvozují data o pohybu, byl přesný.
- O.Reliability Snímač pohybu musí pracovat spolehlivě.
- O.Secured_Data_Exchange Snímač pohybu musí zabezpečit výměnu dat s VU.

3.6 Prostředky fyzikální, personální a procedurální

Tento odstavec popisuje požadavky na fyzické, personální a procedurální prostředky, které přispívají k bezpečnosti snímačů pohybu.

3.6.1 Konstrukce zařízení

- M.Development Vývojoví pracovníci snímače pohybu musí zajistit, aby přidělování odpovědností v průběhu vývoje odpovídalo IT bezpečnosti.
- M.Manufacturing Výrobci snímače pohybu musí zajistit, aby přidělování odpovědností v průběhu výroby odpovídalo IT bezpečnosti a že v průběhu výroby je snímač pohybu chráněn před fyzickými zásahy, které by mohly ovlivnit jeho IT bezpečnost.

3.6.2 Dodávka zařízení

- M.Delivery Výrobci snímače pohybu, výrobci vozidel a montéři nebo dílny musí zajistit, že zacházení se snímačem pohybu probíhá způsobem, který zachovává IT bezpečnost.

3.6.3 Generace bezpečnostních dat a jejich dodávka

- M.Sec_Data_Generation Algoritmus generace bezpečnostních dat musí být přístupný jen oprávněnému a spolehlivému personálu
- M.Sec_Data_Transport Bezpečnostní data musí být generována, transportována a vkládána do snímače pohybu způsobem, zabezpečujícím jejich příslušnou důvěrnost a celistvost.

3.6.4 Montáž, kalibrace a kontrola záznamového zařízení

- M.Approved_Workshops Montáž, kalibraci a opravy záznamového zařízení musí provádět jen oprávnění a spolehliví montéři nebo dílny.
- M.Mechanical_Interface Musí být zajištěna opatření, detekující fyzické zásahy do mechanického propojení (např. plombami).

M.Regular_Inspections Záznamové zařízení musí být periodicky kontrolováno a kalibrováno.

3.6.5 *Kontrola dodržování předpisů*

M.Controls Dodržování právních předpisů je třeba pravidelně a nahodile kontrolovat a kontrola musí zahrnovat bezpečnostní audit.

3.6.6 *Upgrade (modernizace) softwaru*

M.Software_Upgrade Před tím než je zaveden do snímače pohybu, musí mít revize software udělenou certifikaci na bezpečnost.

4. **Funkce zajišťující bezpečnost**

4.1 **Identifikace a prokázání totožnosti**

UIA_101 Snímač pohybu musí být pro každou interakci schopen stanovit identitu kterékoliv jednotky, na kterou je připojen.

UIA_102 Identitu připojené jednotky musí tvořit:

- skupinu jednotky

- VU,

- řídicí zařízení,

- ostatní

- jednotku ID (pouze u VU)

UIA_103 Jednotka ID připojeného VU je tvořena číslem schválení VU a výrobním číslem VU.

UIA_104 Snímač pohybu musí být schopen prokázat totožnost kteréhokoliv VU nebo řídicí jednotky, na které je napojen:

- při připojení jednotky,

- při obnově napájení.

UIA_105 Snímač pohybu musí být schopen periodicky obnovovat prokázání totožnosti VU, na které je napojen.

UIA_106 Snímač pohybu musí detekovat a ochraňovat data o totožnosti, která kopíroval a odesílal.

UIA_107 Po neúspěšných po sobě jdoucích pokusech o prokázání totožnosti (stanoví výrobce, ale ne více než 20) musí SEF:

- vygenerovat záznam o auditu příhody,

- varovat jednotku,
- pokračovat v generaci údajů o pohybu v nezabezpečeném módu.

4.2 Kontrola přístupu

Kontrola přístupu zabezpečuje, že informace jsou odečítány, vytvářeny nebo modifikovány v TOE pouze osobami, které jsou k tomu autorizovány.

4.2.1 Postup kontroly postupu

ACC_101 Snímač pohybu musí zkontrolovat práva přístupu k funkcím a k datům

4.2.2 Práva přístupu k datům

ACC_102 Snímač pohybu musí zajistit, aby data o identifikaci snímače pohybu mohla být napsána pouze jednou (požadavek 078).

ACC_103 Snímač pohybu musí přijmout a/nebo uložit data uživatele pouze z jednotek s prokázanou totožností

ACC_104 Snímač pohybu si vyžádá příslušná práva k přístupu ke čtení a zápisu.

4.2.3 Struktura souboru a podmínka přístupu

ACC_105 Struktura souborů aplikací a dat a podmínky přístupu musí být stanoveny v průběhu výroby a následně musí být zamčeny před jakoukoliv budoucí změnou nebo vymazáním

4.3 Možnosti přiřazení

ACT_101 Snímač pohybu musí ve své paměti podržet identifikační data snímače pohybu (požadavek 077).

ACT_102 Snímač pohybu musí ve své paměti uložit svá montážní data (požadavek 099).

ACT_103 Snímač pohybu musí mít schopnost na vyžádání jednotek s prokázanou totožností poskytnout výstup dat o možnosti přiřazení.

4.4 Audit

AUD_101 Snímač pohybu musí v případě zhoršení vlastní bezpečnosti generovat záznamy auditu o událostí.

AUD_102 Události, ovlivňující bezpečnost snímače pohybu, jsou následující:

- pokusy o poškození bezpečnosti,
 - závada v prokázání totožnosti
 - závada v celistvosti uložených dat,

- závada ve vnitřním přenosu dat,
- neoprávněné otevření pouzdra,
- manipulace s hardwarem.

- závada na snímači.

AUD_103 Záznamy o auditu musí zahrnovat následující data:

- datum a doba události,
- typ události,
- identita připojené jednotky,

pokud nejsou požadovaná data dostupná, je třeba udat indikaci chyby (stanoví výrobce).

AUD_104 Snímač pohybu musí generované záznamy auditu odeslat do VU v době jejich generace a má si je také uložit ve své paměti.

AUD_105 V případě, kdy snímač pohybu ukládá záznamy o auditu, musí snímač zajistit do vyčerpání kapacity paměti zajistit záznamy 20 auditů a musí mít možnost výstupu uložených záznamů o auditu jednotkám s prokázanou totožností na jejich vyžádání.

4.5 Přesnost

4.5.1 Postup kontroly toku informací

ACR_101 Snímač pohybu musí zajistit, že data o pohybu jsou zpracovávána a dodávána pouze z mechanického vstupu snímače.

4.5.2 Interní přenos dat

Požadavky tohoto odstavce se použijí pouze v případě, když je snímač pohybu tvořen fyzicky oddělenými částmi.

ACR_102 Pokud jsou mezi fyzicky oddělenými částmi snímače pohybu přenášena data, musí být data chráněna před jejich změnou.

ACR_103 Po zjištění závady v interním přenosu v průběhu přenosu dat musí být přenos opakován a SEF musí vygenerovat záznam auditu události.

4.5.3 Úplnost (integrita) uložených dat

ACR_104 Snímač pohybu musí ověřit data o uživateli, uložená v jeho paměti, na závady v úplnosti (integritě).

ACR_105 Po zjištění závady v úplnosti (integritě) údajů o uživateli musí SEF vygenerovat záznam auditu události.

4.6 Spolehlivost funkce

4.6.1 Zkoušky

- RLB_101 Veškeré povely, akce nebo zkušební body, specifické pro potřeby zkoušení ve fázi výroby, musí být před ukončením výroby deaktivovány nebo odstraněny. Nesmí být možné, aby byly později obnoveny.
- RLB_102 Při prvním zapojení a v průběhu normálního provozu musí snímač pohybu ověřovat svoji správnou funkci autotesty. Autotest snímače pohybu musí zahrnovat ověření úplnosti bezpečnostních dat a ověření úplnosti uloženého spouštěcího kódu (pokud není uložen na ROM).
- RLB_103 Po zjištění interní závady při autotestu musí SEF vygenerovat záznam auditu události (závada snímače).

4.6.2 Software

- RLB_104 Nesmí existovat žádný způsob jak při užívání analyzovat nebo ladit software snímače pohybu.
- RLB_105 Vstupy z vnějších zdrojů nesmí být použitelné jako spouštěcí kódy.

4.6.3 Fyzická ochrana

- RLB_106 Pokud je snímač pohybu konstruován tak, že může být otevřen, musí snímač každé otevření pouzdra po dobu minimálně 6 měsíců detekovat i když k otevření dojde při odpojení externím napájení. V takovém případě musí SEF generovat záznam auditu události (je možné, aby záznam auditu byl generován a uložen po novém připojení napájení).

Pokud je snímač pohybu konstruován tak, aby nemohl být otevřen, musí být konstruován tak, aby pokus o zásah mohl být snadno detekován (např. vizuální kontrolou).

- RLB_107 Snímač pohybu musí detekovat stanovené (bude definovat výrobce) zásahy do hardware.
- RLB_108 Ve výše popsaném případě musí SEF generovat záznam auditu a snímač pohybu musí: (bude definovat výrobce):

4.6.4 Přerušování napájení

- RLB_109 V průběhu přerušování nebo změnách napájení musí snímač pohybu zachovat bezpečný stav.

4.6.5 Obnovení nastavení (resetování)

- RLB_110 V případě přerušování napájení nebo zastavení transakce před jejím ukončením nebo při jiných podmínkách pro resetování musí být snímač pohybu zcela resetován

4.6.6 *Dostupnost dat*

RLB_111 Snímač pohybu musí zajistit v případě potřeby přístup k obsahu dat a zajistit, aby data nebyla požadována ani podržována zbytečně.

4.6.7 *Vícefunkční využití*

RLB_112 Pokud snímač pohybu zajišťuje jiné využití než jen využití pro tachograf, musí být všechna další využívání fyzikálně a/nebo logicky vzájemně oddělena. Taková využití nesmí sdílet bezpečnostní data. Pouze jedna z činností může být v jednom okamžiku funkční.

4.7 **Výměna dat**

DEX_101 Snímač pohybu musí exportovat data o pohybu do VU spolu s bezpečnostními znaky tak, aby VU bylo schopno ověřit jejich úplnost a totožnost.

4.8 **Podpora šifrováním**

Požadavky tohoto odstavce jsou použitelné pouze v případě potřeby v závislosti na užitém mechanismu bezpečnosti a na řešení výrobce.

CSP_101 Jakákoliv šifrovací operace snímače pohybu musí odpovídat stanovenému algoritmu a stanovenému klíči.

CSP_102 Pokud snímač pohybu generuje šifrovací klíče, musí tyto klíče odpovídat stanoveným algoritmům generace šifrovacích klíčů a stanovené velikosti šifrovacího klíče.

CSP_103 Pokud snímač pohybu šifrovací klíče distribuuje, musí distribuce odpovídat stanoveným postupům distribuce klíčů.

CSP_104 Pokud snímač pohybu šifrovací klíče přejímá, musí přejímání odpovídat stanoveným postupům přejímání klíčů.

CSP_105 Pokud snímač pohybu šifrovací klíče ničí, musí ničení odpovídat stanoveným postupům ničení klíčů.

5. **Definice bezpečnostních mechanismů**

Bezpečnostní mechanismus, plnící funkce zajišťující bezpečnost snímače pohybu, stanovuje výrobce snímače pohybu.

6. **Minimální pevnost bezpečnostních mechanismů**

Minimální pevnost bezpečnostního mechanismu snímače pohybu je podle ITSEC je „Vysoká“.

7. Úroveň zajištění

Cílovou úrovní zabezpečení snímače pohybu je ITSEC úroveň E3 podle definice v ITSEC.

8. Základní principy

Následující matrice podává základní principy SEF tím že udává:

- které SEF nebo prostředky působí proti kterému ohrožení,
- která SEF plní které IT cíle bezpečnosti.

	Ohrožení												IT předměty					
	Přístup	Závady	Zkoušky	Konstrukce	Okolní podmínky	Hardware	Mechanický původ	Data o pohybu	Napájení	Bezpečnostní data	Software	Illožená data	Přístup	Audit	Prokázání totožnosti	Procesing	Spolehlivost	Výměna zabezpečených dat
Procedurální prostředky fyzického personálu																		
Vývoj		x	x	x														
Výroba			x	x														
Dodávání						x					x	x						
Generace bezpečnostních dat										x								
Přenos bezpečnostních dat										x								
Schválená dílna							x											
Mechanické propojení							x											
Pravidelná kontrola						x	x		x		x							
Kontroly uplatnění zákonů					x	x	x		x	x	x							
Modernizace software											x							
Funkce zajišťující bezpečnost																		
Identifikace a prokázání totožnosti																		
UIA_101 Identifikace totožnosti jednotek	x							x					x		x			x
UIA_102 Totožnost jednotek	x												x		x			
UIA_103 Totožnost VU														x				
UIA_104 Ověření totožsti jednotek	x							x					x		x			x
UIA_105 Nové ověření totožnosti	x							x					x		x			x
UIA_106 Nepadělatelné ověření totožnosti	x							x					x		x			
UIA_107 Závada v ověření totožnosti								x						x			x	
Řízení přístupu																		
ACC_101 Zásady řízení přístupu	x									x		x	x					
ACC_102 Identifikace snímače pohybu												x	x					
ACC_103 Data uživatele												x	x					
ACC_104 Bezpečnostní data										x		x	x					
ACC_105 Struktura souborů a podmínky přístupu	x									x		x	x					

	Ohrožení												IT předměty					
	Přístup	Závady	Zkoušky	Konstrukce	Okolní podmínky	Hardware	Mechanický původ	Data o pohybu	Napájení	Bezpečnostní data	Software	Illožená data	Přístup	Audit	Prokázání totožnosti	Processing	Spolehlivost	Výměna zabezpečených dat
Možnost přiřazení																		
ACT_101 Identifikační data snímače pohybu														x				
ACT_102 Data propojení														x				
ACT_103 Data přiřazení														x				
Audit																		
AUD_101 Záznamy o auditu														x				
AUD_102 Seznam událostí auditu	x				x	x						x		x				
AUD_103 Data auditu														x				
AUD_104 Nástroje auditu														x				
AUD_105 Paměť záznamů auditu														x				
Přesnost																		
ACR_101 Postup kontroly toku informací									x							x	x	
ACR_102 Vnitřní převody																x	x	
ACR_103Vnitřní převody														x				
ACR_104 Úplnost uložených dat												x					x	
ACR_105 Úplnost uložených dat												x		x				
Spolehlivost																		
RLB_101 Zkoušky ve výrobě			x	x														x
RLB_102 Autotesty		x				x			x		x							x
RLB_103 Autotesty						x			x		x			x				
RLB_104 Analýza software				x							x							x
RLB_105 Vstup software											x					x	x	
RLB_106 Otevření pouzdra				x	x	x				x	x	x						x
RLB_107 Poškození hardware						x												x
RLB_108 Poškození hardware						x									x			
RLB_109 Přerušení napájení									x									x
RLB_110 Obnova nastavení (reset)		x																x
RLB_111 Dostupnost dat																x	x	
RLB_112 Vícenásobné využití																		x
Výměna dat																		
DEX_101 Zabezpečení exportu dat o pohybu								x										x
Podpora šifrováním																		
CSP_101 Algoritmus																		x
CSP_102 Generace klíče																		x
CSP_103 Distribuce klíče																		x
CSP_104 Přístup ke klíči																		x
CSP_105 Poškození klíče																		x

VŠEOBECNÉ POŽADAVKY NA BEZPEČNOST CELKU VE VOZIDLE

1. Úvod

Tento dokument obsahuje popis celku ve vozidle, jakým ohrožením musí odolávat a jaká bezpečnostní skutečnosti musí získat. Dokument stanovuje funkce zajišťující bezpečnost. Dokument stanovuje požadovanou minimální pevnost bezpečnostního mechanismu a požadovanou úroveň zajištění vývoje a hodnocení.

Požadavky, které dokument stanovuje, odpovídají hlavní části přílohy IB. V zájmu lepší srozumitelnosti může někdy docházet k duplicitě mezi požadavky hlavní části přílohy IB a požadavky záměrů bezpečnosti. V případě nejednoznačnosti požadavků bezpečnostních záměrů a požadavků hlavní části přílohy IB v oblasti požadavků bezpečnostních záměrů, jsou rozhodující požadavky hlavní části přílohy IB.

Požadavky hlavní části přílohy IB, které nejsou uvedeny v bezpečnostních záměrech, nejsou předmětem funkcí zajišťujících bezpečnost.

Pro lepší přiřazení současných pojmů k dokumentaci o vývoji a hodnocení jsou pro možná ohrožení bezpečnosti a plněných cílů, skutečností, a SEF specifikacím přidělena jednotná označení.

2. Zkratky, definice a odkazy

2.1 Zkratky

PIN	Osobní identifikační číslo
ROM	Read only memory (permanентní paměť)
SEF	funkce zajišťující bezpečnost
TBD	To be defined (je třeba definovat)
TOE	Cíl hodnocení
VU	Celek ve vozidle

2.2 Definice

Digitální tachograf	Záznamové zařízení
Data o pohybu	Data, sdílená se snímačem pohybu, reprezentující rychlost a ujetou vzdálenost
Fyzicky oddělené části	Fyzické části VU, které jsou rozloženy po vozidle, jako protiklad k fyzickým součástem soustředěným v pouzdře celku ve vozidle

Bezpečnostní data	Specifická data, potřebná pro podporu funkcí zajišťujících bezpečnost (např. kódovací klíče)
Systém	Zařízení, osoby nebo organizace, jakkoliv související se záznamovým zařízením
Uživatel	Uživatelem se rozumí osoba užívající zařízení. Normálními uživateli VU se rozumí řidiči, kontrolóři, dílny a společnosti.
Data uživatele	Jakákoliv data jiná než údaje o pohybu nebo bezpečnosti, zaznamenané nebo uložené ve VU a požadovaná kapitolou III.12.

2.1 Odkazy

ITSEC Information Technology Security Evaluation Kriteria 1991 = informace o kritériích hodnocení bezpečnostní technologie 1991.

3. Princip výrobku

3.1 Popis celku ve vozidle a postup užití

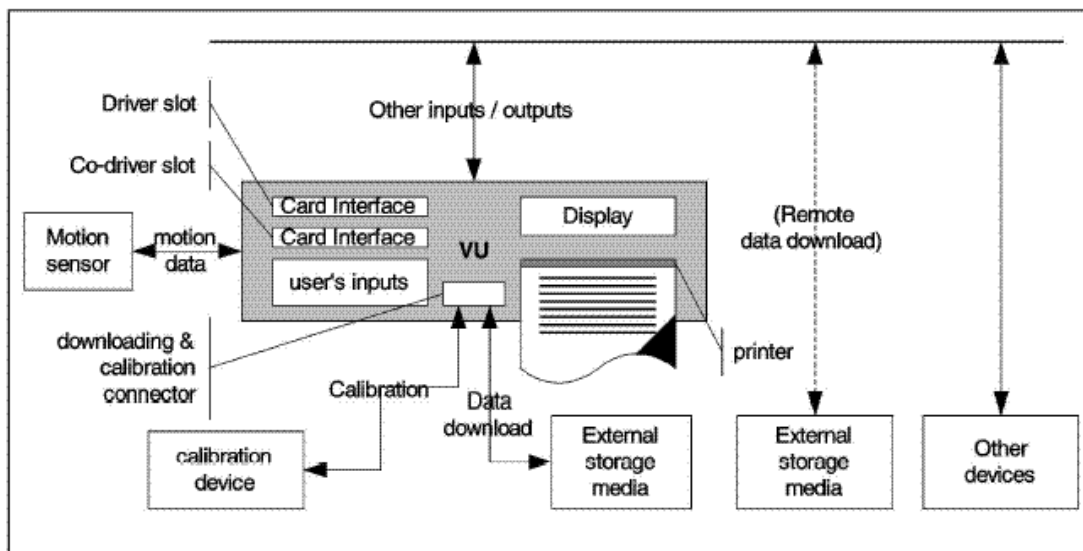
VU je určen k montáži do silničních vozidel. Jeho účelem je záznam, ukládání, zobrazení, tisk a výstup dat, souvisejících s aktivitami řidiče. VU je napojen na snímač pohybu, se kterým si sdílí data o pohybu vozidla.

Uživatelé se VU identifikují užitím svých tachografových karet.

VU poskytuje data pro zobrazení, tiskárnu a pro externí zařízení.

Pracovní prostředí celku ve vozidle po jeho montáži do vozidla je popsáno v následujícím vyobrazení:

Obr. 1
Pracovní prostředí VU



Driver slot = otvor (slot) pro kartu řidiče

co-driver slot = otvor (slot) pro kartu spoluřidiče

Other inputs/outputs = jiné vstupy/výstupy

Motion sensor = snímač pohybu

motion data = data o pohybu

Card interface = rozhraní karty

Display = zobrazení

user's inputs = vstupy uživatele

(Remote data download) = převod dat z vnějšku

downloading & calibration connector = převodní a kalibrační konektor

printer = tiskárna

Calibration = kalibrace

calibration device = kalibrační zařízení

Data download = převod dat

External storage media = vnější paměťová média

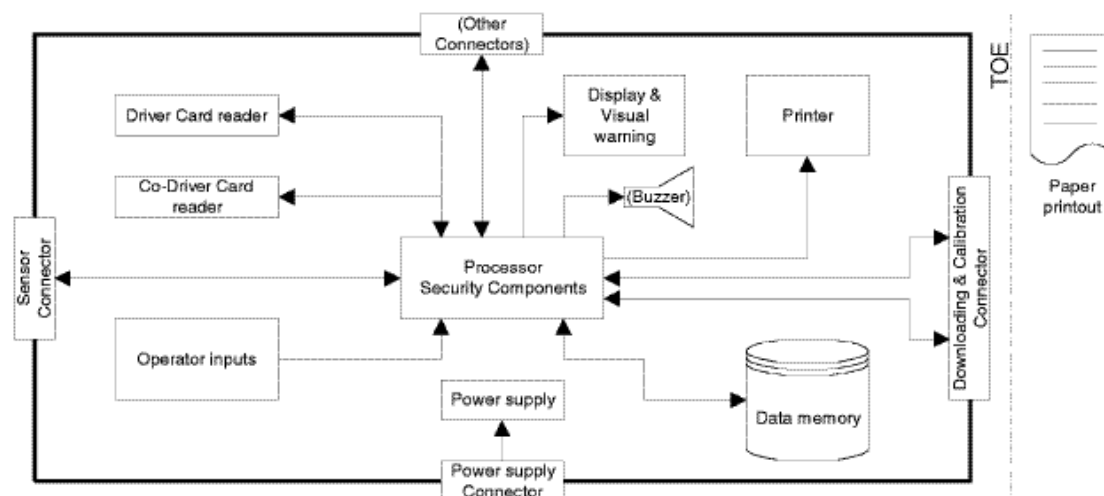
Other device = ostatní zařízení

Všeobecné vlastnosti VU, jeho funkce a více o činnosti popisuje kapitola II v příloze I B.

Funkční požadavky VU stanovuje kapitola III v příloze I B.

Typický VU je popsán v následujícím vyobrazení:

Obr. 2
Typický VU (...) volitelný



(Other connectors) = ostatní konektory

Driver card leader = čtečka karty řidiče

Display and visual warning = zobrazení a optická varování

Pointer = tiskárna

Co-driver card leader = čtečka karty spoluridiče

(Buzzer) = bzučák

Paper printout = výtisk (sjetina)

Senzor connector = konektor snímače

Procesor = procesor

Security Components = bezpečnostní části

Downloading & calibration connector = převodní a kalibrační konektor

Operator inputs = vstupy pracovníka

Power input = napájení

Data memory = paměť dat

Power supply connector = konektor napájení.

Je třeba připomenout, že i mechanismus tiskárny je součástí TOE, jednou vytištěný papírový dokument ale nikoliv.

3.2 Životní cyklus celku do vozidla

Typický životnostní cyklus VU popisuje následující vyobrazení:

T.Test Užití neplatných zkušebních módů nebo existující možnost „vstupu zadními dveřmi“, které mohou ovlivnit bezpečnost VU.

T.Design Pokus uživatele o ilegální získání znalostí o konstrukci ať již z podkladů výrobce (loupeží, korupcí, atd.) nebo metodami zpětných technik.

3.3.3 *Ohrožení bezpečnosti v souvislosti s provozem*

T.Calibration_parameters Pokus uživatele o užití vadně kalibrovaného zařízení (změnou kalibračních dat nebo organizačním nedostatkem).

T.Card_Data_Exchange Pokus uživatele o změnu dat při převodem mezi VU a kartami tachografu (přidání, změna, vypuštění, nové přehrání signálu).

T.Clock Pokus uživatele o změnu ve vnitřních hodinách.

T.Environment Ohrožení bezpečnosti VU uživatelem vnějším vlivem (tepelně, elektromagneticky, opticky, chemicky, mechanicky atd.).

T.Fake_Device Pokus uživatele o připojení padělaného zařízení na VU (snímače pohybu, programovatelné karty).

T.Hardware Pokus uživatele měnit hardware VU.

T.Motion_Data Pokus uživatele o manipulaci s daty o pohybu vozidla (přidání, změna, vypuštění, přehrání signálu).

T.Non_Activated Pokus uživatele o užití neaktivovaného zařízení.

T.Output_Data Pokus uživatele o změnu výstupu dat (tisk, zobrazení nebo převodu).

T.Power_Supply Pokus uživatele o ovlivnění bezpečnostních opatření u VU změnou napájení (rozpojení vedení, snížení nebo zvýšení napětí).

T.Security_Data Pokus uživatele o ilegální získání dat při generaci bezpečnostních údajů s průběhu generace dat, při dopravě nebo při skladování zařízení.

T.Software Pokus uživatele o modifikaci software VU.

T.Stored_Data Pokus uživatele o změnu uložených údajů (bezpečnostní data nebo data o uživateli).

3.4 **Cíle bezpečnosti**

Hlavním cílem systému digitálního tachografu je následující:

O.Main Kontrolním orgánům musí být ke kontrole dostupná data, data musí plně a přesně udávat aktivity kontrolovaného řidiče a vozidla z hlediska doby jízdy, doby pracovní pohotovosti, doby odpočinku a rychlosti vozidla.

K cílům všeobecné bezpečnosti přispívají proto cíle bezpečnosti VU takto:

O.VU_Main Měřená a zaznamenávaná data, které mají být následně ověřovány kontrolními orgány, musí být dosažitelné přesně odpovídat aktivitám kontrolovaných řidičů a vozidla z hlediska dob řízení, práce, pohotovosti a období odpočinku a z hlediska rychlosti vozidla.

O.VU_Export VU musí být schopen exportovat data do externího záznamového média tak, aby bylo možno ověřit jejich úplnost a autenticitu.

3.5 Cíle bezpečnosti informační technologie

Specifické cíle bezpečnosti informační technologie o VU, které přispívají k jeho celkové bezpečnosti, jsou následující:

O.Access VU musí řídit přístup uživatele k funkcím a datům.

O.Accountability VU musí snímat přesná data o přiřazení.

O.Audit VU musí monitorovat pokusy o obcházení jeho bezpečnostních opatření a musí o nich předávat informace postiženým uživatelům.

O.Authentication VU by měl stanovit totožnost uživatelů a připojených jednotek (pokud je třeba vytvořit mezi jednotkami spolehlivé cesty).

O.Integrity VU musí zajistit ukládání úplných dat.

O.Output VU musí zajistit, aby výstup dat odpovídal přesně měřeným a ukládaným datům.

O.Processing VU musí zajistit aby postup zpracování vstupních dat, ze kterých se odvozují data o uživateli, byl přesný.

O.Reliability VU musí pracovat spolehlivě.

O.Secured_Data_Exchange VU musí zabezpečit výměnu dat se snímačem pohybu a kartou tachografu..

3.6 Prostředky fyzikální, personální a procedurální

Tento odstavec popisuje požadavky na fyzické, personální a procedurální prostředky, které přispívají k bezpečnosti VU.

3.6.1 Konstrukce zařízení

M.Development Vývojoví pracovníci VU musí zajistit, aby přidělování odpovědností v průběhu vývoje odpovídalo IT bezpečnosti.

M.Manufacturing Výrobci VU musí zajistit, aby přidělování odpovědností v průběhu výroby odpovídalo IT bezpečnosti a že v průběhu výroby je VU chráněn před fyzickými zásahy, které by mohly ovlivnit jeho IT bezpečnost.

3.6.2 *Dodávka a aktivace zařízení*

M.Delivery Výrobci VU, výrobci vozidel a montéři nebo dílny musí zajistit, že zacházení s neaktivovaným VU probíhá způsobem, který zachovává bezpečnost VU.

M.Activation Výrobci vozidla a montéři nebo dílny musí VU aktivovat po jeho montáži dříve, než vozidla opustí provozovny, ve kterých bylo VU namontováno.

3.6.3 *Generace bezpečnostních dat a jejich dodávka*

M.Sec_Data_Generation Algoritmus generace bezpečnostních dat musí být přístupný jen oprávněnému a spolehlivému personálu

M.Sec_Data_Transport Bezpečnostní data musí být generována, transportována a vkládána do VU způsobem, zabezpečujícím jejich příslušnou důvěrnost a celistvost.

3.6.4 *Dodávka karet*

M.Card_Availibility Karty tachografu musí být dostupné a být dodávány pouze oprávněným osobám.

M.Driver_Card_Uniqueness Řidič musí mít v jednu dobu jen jedinou platnou kartu řidiče.

M.Traceability Karty musí být výrazné (bílý list, černý list), černý list se musí užívat v průběhu bezpečnostního auditu.

3.6.5 *Montáž, kalibrace a kontrola záznamového zařízení*

M.Approved_Workshops Montáž, kalibraci a opravy záznamového zařízení musí provádět důvěryhodní a schválení montéři nebo dílny.

M.Regular_Inspections Záznamové zařízení musí být periodicky kontrolováno a kalibrováno.

M.Faithful_Calibration V průběhu kalibrace musí schválení montéři nebo schválené dílny vložit do záznamového zařízení příslušné parametry vozidla

3.6.6 *Provoz zařízení*

M.Faithful_Drivers Řidiči musí dodržovat pravidla a jednat zodpovědně (např. užívat své karty řidiče, přiměřeně volit vlastní vybranou manuální aktivitu atd.)

3.6.7 *Kontrola dodržování předpisů*

M.Controls Dodržování právních předpisů je třeba pravidelně a nahodile kontrolovat a kontrola musí zahrnovat bezpečnostní audit.

3.6.7 Upgrade (modernizace) softwaru

M.Software_Upgrade Před tím než je zaveden do VU, musí mít revize software udělenou certifikaci na bezpečnost.

4. Funkce zajišťující bezpečnost

4.1 Identifikace a prokázání totožnosti

4.1.1 Identifikace a prokázání totožnosti snímače pohybu

UIA_201 VU musí být pro každou interakci schopen stanovit identitu snímače pohybu, na který je připojen.

UIA_202 Identita snímače pohybu musí sestávat z čísla schválení snímače a výrobního čísla snímače.

UIA_203 VU musí ověřit totožnost snímače pohybu, na který je připojen::

- při připojení snímače pohybu,
- při každé kalibraci záznamového zařízení,
- při obnovení napájení.

Ověření totožnosti musí být vzájemné a musí jej spouštět VU.

UIA_204 VU musí periodicky (periodu stanoví výrobce, musí ale být kratší než 1 hod.) opětovně identifikovat a prověřovat totožnost snímače pohybu ke kterému je napojen, a musí zjistit, že snímač pohybu, identifikovaný při poslední kalibraci záznamového zařízení, nebyl vyměněn.

UIA_205 VU musí zajistit a ochránit využití kopírovaných a znovu uložených údajů o prokázání totožnosti.

UIA_206 Po neúspěšných po sobě jdoucích pokusech o prokázání totožnosti (stanoví výrobce, ale ne více než 20) a/nebo po zjištění, že byla neoprávněně změněna identita snímače pohybu (tj. nikoliv při kalibraci záznamového zařízení), musí SEF:

- vygenerovat záznam o auditu události,
- varovat uživatele,
- pokračovat v přijímání a využívání údajů o pohybu, vysílaných snímačem pohybu v nezabezpečeném módu.

4.1.2 Identifikace a prokázání totožnosti uživatele

UIA_207 VU musí trvale a selektivně ověřovat identitu obou uživatelů monitorováním karet tachografu, vložených v zařízení do otvoru (slotu) pro kartu řidiče a do otvoru (slotu) pro kartu spoluřidiče.

- UIA_208 Identita uživatele musí sestávat z:
- skupiny uživatelské:
 - ŘIDIČ (karta řidiče),
 - KONTROLOR (kontrolní karta),
 - DÍLNA (karta dílny),
 - SPOLEČNOST (karta společnosti),
 - NEZNÁMÉ (není vložena žádná karta),
 - identifikace uživatele, kterou tvoří:
 - kód členského státu, který vystavil kartu a číslo karty),
 - NEZNÁMÉ, pokud je uživatelská skupina NEZNÁMÁ.
 - Identity NEZNÁMÉ mohou být implicitně nebo explicitně známé.
- UIA_209 Při vložení karty musí VU zjistit totožnost své uživatele.
- UIA_210 VU musí znovu zjistit totožnost svých uživatelů:
- při obnoveném napájení,
 - periodicky nebo po zvláštní příhodě (stanoví výrobce, musí ale být dříve než jednou denně).
- UIA_211 Prokázání totožnosti tvoří zjištění, že vložená karta je platnou kartou tachografu, na které jsou bezpečnostní data, která může distribuovat pouze systém. Prokázání totožnosti musí být vzájemné a musí být spouštěno z VU.
- UIA_212 Jako doplněk k výše uvedenému se požaduje, aby totožnost dílen byla dostatečně prokázána vložním PIN. PIN musí mít nejméně 4 znaky.
- Poznámka: V případě, kdy je PIN předáván do VU vnějším zařízením, umístěným v blízkosti VU, nemusí být PIN při přenosu ochráněn.
- UIA_213 VU musí rozeznat a zabránit využívání kopírovaných a znovu vkládaných dat o prokázání totožnosti.
- UIA_214 Po zjištění 5 neúspěšných po sobě jdoucích pokusů o prokázání totožnosti musí SEF:
- vygenerovat záznam o auditu události,
 - varovat uživatele,

- považovat uživatele za NEZNÁMÉHO a jeho kartu za neplatnou (označení z) a požadavek 007).

4.2 Kontrola přístupu

Kontrola přístupu zabezpečuje, že informace jsou odečítány, vytvářeny nebo modifikovány v TOE pouze osobami, které jsou k tomu autorizovány.

Je třeba podotknout, že data uživatele, zaznamenaná VU, která také obsahují soukromá nebo obchodně citlivá hlediska, nejsou zde důvěrné. Proto funkční požadavky, které se vztahují k přístupu ke čtení dat (požadavek 011), nejsou předmětem funkcí, zajišťujících bezpečnost.

4.2.1 Postup kontroly postupu

ACC_201 VU musí zkontrolovat práva přístupu k funkcím a k datům.

4.2.2 Práva přístupu k datům

ACC_202 VU musí uplatnit mód pravidel volby operací (požadavky 006 až 009).

ACC_203 VU musí využívat mód operací k zajištění funkce pravidel volby operací (požadavek 010).

4.2.3 Práva přístupu k datům

ACC_204 VU musí uplatnit pravidla přístupu k zapsání identifikačních dat VU (požadavek 076).

ACC_205 VU musí uplatnit pravidla k přístupu k zápisu zdvojených identifikačních dat snímače pohybu (požadavky 079 a 155).

ACC_206 Po aktivaci VU musí VU zajistit, aby do VU mohla být vkládána a ukládána do jeho datové paměti kalibrační data pouze v kalibračním módu (požadavky 154 a 156).

ACC_207 Po aktivaci VU musí VU uplatnit zápis kalibračních dat a odstranit pravidla k přístupu. (požadavek 097).

ACC_208 Po aktivaci VU musí VU zajistit, aby do VU mohlo být vkládáno a ukládáno do jeho datové paměti nastavení času pouze v kalibračním módu (požadavky 157 a 158).

ACC_209 Po aktivaci VU musí VU uplatnit zápis nastavení času a odstranit pravidla k přístupu. (požadavek 100).

ACC_210 VU musí zajistit příslušná práva ke čtení a zápisu bezpečnostních dat (požadavek 080).

4.2.4 Struktura souboru a podmínka přístupu

ACC_211 Struktura souborů aplikací a dat a podmínky přístupu musí být stanoveny v průběhu výroby a následně musí být zamčeny před jakoukoliv budoucí změnou nebo vymazáním^{4.3}

4.3 Možnosti přiřazení

ACT_201 VU musí zajistit, aby řidiči byli přiřazováni ke svým aktivitám (požadavky 081°, 084, 087, 105a, 105b, 109 a 109a).

ACT_202 VU musí trvale uchovávat identifikační data (požadavek 075).

ACT_203 VU musí zajistit, aby dílny byly přiřazovány k jejich aktivitám (požadavky 098, 101 a 109).

ACT_204 VU musí zajistit, aby kontroloři byli přiřazováni ke svým aktivitám (požadavky 102, 103 a 109).

ACT_205 VU musí zaznamenávat data měřiče ujeté vzdálenosti (požadavek 090) a detailní data o rychlosti (požadavek 093).

ACT_206 VU musí zajistit, aby jednou zaznamenaná data ve vztahu k požadavkům 081 až 093 a 102 až 105b včetně nebyla měněna, s výjimkou, kdy starší zaznamenaná data jsou nahrazována daty novými.

ACT_207 VU musí zajistit, že nebude měnit data již uložená na kartě tachografu (požadavky 109 a 109a), s výjimkou, kdy starší zaznamenaná data jsou nahrazována daty novými (požadavek 110) nebo v případě popsaném v poznámce v dodatku 1 odst. 2.1.

4.4 Audit

Schopnosti auditu jsou požadovány pouze u událostí, které mohou indikovat manipulaci nebo narušení bezpečnosti. Audit není požadován při normálním výkonu práv i pokud se týkají bezpečnosti.

AUD_201 VU musí v případech zhoršení bezpečnosti VU tyto události zaznamenat se souvisejícími daty (požadavky 094, 096 a 109).

AUD_102 Události, ovlivňující bezpečnost VU, jsou následující:

- pokusy o poškození bezpečnosti:

- závada v prokázání totožnosti snímače pohybu,
- závada v prokázání totožnosti karty tachografu,
- neoprávněná výměna snímače rychlosti,
- závada v úplnosti dat z karty,

- závada v úplnosti uložených dat uživatele,
- závada ve vnitřním přenosu dat,
- neoprávněné otevření pouzdra,
- poškození hardware,
- poslední akce s kartou nebyla správně ukončena,
- závada v datech o pohybu,
- přerušení napájení,
- vnitřní porucha VU.

AUD_203 VU musí zajistit pravidla ukládání záznamů o auditu (požadavek 094 a 096).

AUD_204 VU musí uložit do své paměti záznamy o auditu, které generuje snímač pohybu .

AUD_205 Záznamy o auditu musí být možno vytisknout, zobrazit a převádět.

4.5 Obnova využití paměti

REU_201 VU musí zajistit, aby dočasné paměti mohly být znovu užívány, aniž by tím byl vyvolán tok nepřístupných informací.

4.6 Přesnost

4.6.1 Postup kontroly toku informací

ACR_201 VU musí zajistit, aby data uživatele ve vztahu k požadavkům 081, 084, 087, 090, 093, 102, 104, 105, 105a a 109 mohla být zpracovávána pouze pokud pocházejí ze správných vstupních zdrojů:

- data o pohybu vozidla,
- řídicí hodiny VU,
- kalibrační parametry záznamového zařízení,
- karta tachografu,
- vstupy uživatele.

ACR201a VU musí zajistit, aby data uživatele ve vztahu k požadavku 109a mohly být vkládány pouze v období od posledního vyjmutí karty: do nového vložení karty (požadavek 050a).

4.6.2 Interní přenos dat

Požadavky tohoto odstavce se použijí pouze v případě, když je VU tvořen fyzicky oddělenými částmi.

ACR_202 Pokud jsou mezi fyzicky oddělenými částmi VU přenášena data, musí být data chráněna pře jejich změnou.

ACR_203 Po zjištění závady v interním přenosu v průběhu přenosu dat musí být přenos opakován a SEF musí vygenerovat záznam auditu o události.

4.6.3 Úplnost (integrita) uložených dat

ACR_204 VU musí ověřit data o uživateli, uložená v jeho paměti, na závady v úplnosti (integritě).

ACR_205 Po zjištění závady v úplnosti (integritě) údajů o uživateli musí SEF vygenerovat záznam auditu události.

4.7 Spolehlivost funkce

4.7.1 Zkoušky

RLB_201 Veškeré povely, akce nebo zkušební body, specifické pro potřeby zkoušení ve fázi výroby VU, musí být před aktivací VU deaktivovány nebo odstraněny. Nesmí být možné, aby byly později obnoveny.

RLB_202 Při prvním zapojení a v průběhu normálního provozu musí VU ověřovat svoji správnou funkci autotesty. Autotest VU musí zahrnovat ověření úplnosti bezpečnostních dat a ověření úplnosti uloženého spouštěcího kódu (pokud není uložen na ROM).

RLB_203 Po zjištění interní závady při autotestu musí SEF

- vygenerovat záznam auditu události (s výjimkou v kalibračním módu)(závada VU),
- zachovával úplnost (integritu) uložených dat.

4.7.2 Software

RLB_204 Nesmí existovat žádný způsob jak po aktivaci VU při užívání analyzovat nebo ladit software.

RLB_205 Vstupy z vnějších zdrojů nesmí být použitelné jako spouštěcí kódy.

4.7.3 Fyzická ochrana

RLB_206 Pokud je VU konstruován tak, že může být otevřen, musí VU každé otevření pouzdra po dobu minimálně 6 měsíců detekovat i když k otevření dojde při odpojení externím napájení. V takovém případě

musí SEF generovat záznam auditu události (je možné, aby záznam auditu byl generován a uložen po novém připojení napájení).

Pokud je VU konstruován tak, aby nemohl být otevřen, musí být konstruován tak, aby pokus o zásah mohl být snadno detekován (např. vizuální kontrolou).

RLB_207 VU musí po své aktivaci detekovat stanovené (bude definovat výrobce) zásahy do hardware.

RLB_208 Ve výše popsaném případě musí SEF generovat záznam auditu a VU musí: (bude definovat výrobce):

4.7.4 Přerušování napájení

RLB_209 VU musí detekovat odchylky od stanovených hodnot napájení, včetně jeho přerušování.

RLD_210 Ve výše popsaném případě, SEF musí:

- vygenerovat záznam o auditu (s výjimkou v kalibračním módu),
- zajišťovat bezpečný stav VU,
- zachovávat bezpečnostní funkce, které se vztahují k částem nebo k dosud probíhajícím procesům,
- zachovával úplnost (integritu) uložených dat.

4.7.5 Obnovení nastavení (resetování)

RLB_211 V případě přerušování napájení nebo zastavení transakce před jejím ukončením nebo při jiných podmínkách pro resetování musí být VU zcela resetován

4.7.6 Dostupnost dat

RLB_212 VU musí zajistit v případě potřeby přístup k zálohám dat a zajistit, aby záloha dat nebyla požadována ani podržována zbytečně.

RLB_213 VU musí zajistit, aby karty nemohly být vyjmuty před odpovídajícím uložením dat na kartách (požadavky 015 a 016).

RLB_214 Ve výše popsaném případě musí SEF generovat záznam auditu o události.

4.7.7 Vícefunkční využití

RLB_215 Pokud VU zajišťuje jiné využití než jen využití pro tachograf, musí být všechna další využívání fyzikálně a/nebo logicky vzájemně oddělena.

Taková využití nesmí sdílet bezpečnostní data. Pouze jedna z činností může být v jednom okamžiku funkční.

4.8 Výměna dat

Tento odstavec se vztahuje na výměnu dat mezi VU a připojenými zařízeními

4.8.1 Výměna dat se snímačem pohybu

DEX_201 VU musí ověřit úplnost (integritu) a totožnost údajů o pohybu, importovaných ze snímače pohybu.

DEX_202 Po zjištění závady v úplnosti (integritě) dat o pohybu nebo v totožnosti, SEF musí:

- vygenerovat záznam o auditu,
- pokračovat ve využívání importovaných dat.

4.8.2 Výměna dat s kartou tachografu

DEX_203 VU musí ověřit úplnost (integritu) a totožnost dat, importovaných z karty tachografu.

DEX_202 Po zjištění závady v úplnosti (integritě) dat nebo v totožnosti, SEF musí:

- vygenerovat záznam o auditu,
- data neužívat.

DEX_205 VU musí exportovat data do programovatelné karty tachografu spolu s bezpečnostními znaky tak, aby karta byla schopna ověřit jejich úplnost a totožnost.

4.8.3 Výměna dat s externími paměťovými médii (přenosové funkce)

DEX_206 VU musí generovat evidenci o původu dat přenášených do externích médií,

DEX_207 VU musí příjemci dat zajistit možnost ověření evidence o původu přenášených dat,

DEX_208 VU musí exportovat data do externího paměťového média spolu s bezpečnostními znaky tak, aby bylo možno ověřit jejich úplnost a totožnost.

4.9 Podpora šifrováním

Požadavky tohoto odstavce jsou použitelné pouze v případě potřeby v závislosti na užitém mechanismu bezpečnosti a na řešení výrobce.

- CSP_201 Jakákoliv šifrovací operace VU musí odpovídat stanovenému algoritmu a stanovenému klíči.
- CSP_202 Pokud VU generuje šifrovací klíče, musí tyto klíče odpovídat stanoveným algoritmům generace šifrovacích klíčů a stanovené velikosti šifrovacího klíče.
- CSP_203 Pokud VU šifrovací klíče distribuuje, musí distribuce odpovídat stanoveným postupům distribuce klíčů.
- CSP_204 Pokud VU šifrovací klíče přejímá, musí přejímání odpovídat stanoveným postupům přejímání klíčů.
- CSP_205 Pokud VU šifrovací klíče ničí, musí ničení odpovídat stanoveným postupům ničení klíčů.

5. Definice bezpečnostních mechanismů

Požadované bezpečnostní mechanismy jsou stanoveny v dodatku 11.

Veškeré ostatní bezpečnostní mechanismy stanoví výrobce.

6. Minimální pevnost bezpečnostních mechanismů

Minimální pevnost celku ve vozidle je podle ITSEC **Vysoká**.

7. Úroveň zajištění

Cílovou úroveň zabezpečení celku ve vozidle je ITSEC úroveň E3 podle definice v ITSEC.

8. Základní principy

Následující matrice podává základní principy SEF tím že udává:

- které SEF nebo prostředky působí proti kterému ohrožení,
- která SEF plní které IT cíle bezpečnosti.

	Ohrožení																IT předměty										
	Přístup	Identifikace	Závady	Zkoušky	Konstrukce	Parametry kalibrace	Výměna dat a karet	Hodiny	Okolní podmínky	Padělaná zařízení	Hardware	Data o pohybu	Není aktivováno	Výstupní data	Napájení	Bezpečnostní data	Software	Uložená data	Přístup	Možnost přiznání	Audit	Prokázání totožnosti	Úplnost (integrita)	Výstup	Processing	Spolehlivost	Výměna zabezpečených údajů
Procedurální prostředky fyzického personálu																											
Vývoj			x	x	x																						
Výroba				x	x																						
Dodávání												x															
Aktivace	x											x															
Generace bezpečnostních dat																x											
Přenos bezpečnostních dat																x											
Dostupnost karty		x																									
Jedna karta řidiče		x																									
Sledovatelnost karty		x																									
Schválená dílna						x		x																			
Pravidelná kontrolní kalibrace						x		x				x	x			x											
Příslušné dílny						x		x																			
Příslušní řidiči		x																									
Kontroly uplatnění zákonů		x				x		x	x		x		x		x		x	x									
Modernizace software																		x									
Funkce zajišťující bezpečnost																											
Identifikace a prokázání totožnosti																											
UIA_201 Identifikace snímače										x		x											x				x
UIA_202 Identita snímače										x		x											x				x
UIA_203 Prokázání totožnosti snímače										x		x											x				x
UIA_204 Obnovení identifikace a prokázání totožnosti snímače										x		x											x				x
UIA_205 Nepadělatelné prokázání totožnosti										x		x											x				
UIA_206 Závada v prokázání totožnosti										x		x											x				x
UIA_207 Identifikace uživatele	x	x								x										x			x				x
UIA_208 Identita uživatele	x	x								x										x			x				x
UIA_209 Prokázání totožnosti uživatele	x	x								x										x			x				x
UIA_210 Obnovené prokázání totožnosti uživatele	x	x								x										x			x				x
UIA_211 Prostředky k pokázání totožnosti	x	x								x										x			x				
UIA_212 Ověření PIN	x	x				x		x												x			x				

	Ohrožení																IT předměty										
	Přístup	Identifikace	Závady	Zkoušky	Konstrukce	Parametry kalibrace	Výměna dat a karet	Hodiny	Okolní podmínky	Padělaná zařízení	Hardware	Data o pohybu	Není aktivováno	Výstupní data	Napájení	Bezpečnostní data	Software	Uložená data	Přístup	Možnost přizpůsobení	Audit	Prokázání totožnosti	Úplnost (integrita)	Výstup	Processing	Spolehlivost	Výměna zabezpečených údajů
UIA_213	Nepadělatelné prokázání totožnosti	x	x						x											x		x					
UIA_214	Závada v prokázání totožnosti	x	x						x												x						
UIA_215	Identifikace vzdáleného uživatele	x	x															x				x					x
UIA_216	Identita vzdáleného uživatele	x	x															x				x					
UIA_217	Prokázání totožnosti vzdáleného uživatele	x	x															x				x					
UIA_218	Prostředky prokázání totožnosti	x	x															x				x					
UIA_219	Nepadělatelné prokázání totožnosti	x	x															x				x					
UIA_220	Závada v prokázání totožnosti	x	x																								
UIA_221	Identifikace zařízení vedení podniku	x	x															x				x					
UIA_222	Prokázání totožnosti zařízení vedení podniku	x	x															x				x					
UIA_223	Nepadělatelné prokázání totožnosti	x	x															x				x					
Řízení přístupu																											
ACC_201	Postup řízení přístupu	x				x	x									x		x	x								
ACC_202	Práva přístupu k funkcím	x				x	x												x								
ACC_203	Práva přístupu k funkcím	x				x	x												x								
ACC_204	Identifikace VU																	x	x								
ACC_205	Identifikace připojeného snímače								x									x	x								
ACC_206	Kalibrační data	x				x												x	x								
ACC_207	Kalibrační data					x												x	x								
ACC_208	Data nastavení času						x											x	x								
ACC_209	Data nastavení času						x											x	x								
ACC_210	Bezpečnostní data															x		x	x								
ACC_211	Struktura souborů a podmínky přístupu	x				x										x		x	x								

	Ohrožení																	IT předměty									
	Přístup	Identifikace	Závady	Zkoušky	Konstrukce	Parametry kalibrace	Výměna dat a karet	Hodiny	Okolní podmínky	Padělaná zařízení	Hardware	Data o pohybu	Není aktivováno	Výstupní data	Napájení	Bezpečnostní data	Software	Uložená data	Přístup	Možnost přiřazení	Audit	Prokázání totožnosti	Úplnost (integrita)	Výstup	Processing	Spolehlivost	Výměna zabezpečených údajů
Možnost přiřazení																											
ACT_201 Přiřazení řidiče																				x							
ACT_202 Identifikace dat VU																				x	x						
ACT_203 Přiřazení dílny																				x							
ACT_204 Přiřazení kontrolora																				x							
ACT_205 Přiřazení pohybu vozidla																				x							
ACT_206 Změna dat přiřazení																	x						x			x	
ACT_207 Změna dat přiřazení																	x						x			x	
Audit																											
AUD_201 Záznamy o auditu																					x						
AUD_202 Seznam událostí auditu	x						x			x	x		x	x				x			x						
AUD_203 Pravidla ukládání záznamů o auditu																					x						
AUD_204 Záznamy o auditu snímače																					x						
AUD_205 Nástroje auditu																					x						
Obnova užívání																											
REU_201 Obnova užívání																x									x	x	
Přesnost																											
ACR_201 Postup řízení toku informací						x			x	x															x	x	
ACR_202 Vnitřní převody														x										x	x	x	
ACR_203 Vnitřní převody														x							x						
ACR_204 Úplnost uložených dat																	x						x			x	
ACR_205 Úplnost uložených dat																	x				x						
Spolehlivost																											
RLB_201 Zkoušky při výrobě				x	x																						x
RLB_202 Autotesty			x							x				x			x										x
RLB_203 Autotesty										x				x			x				x						
RLB_204 Analýza software					x												x										x
RLB_205 Vstup software																	x							x	x	x	
RLB_206 Otevření pouzdra					x				x	x			x			x	x	x						x			x
RLB_207 Poškození hardware										x																	x
RLB_208 Poškození hardware										x												x					

	Ohrožení																IT předměty											
	Přístup	Identifikace	Závady	Zkoušky	Konstrukce	Parametry kalibrace	Výměna dat a karet	Hodiny	Okolní podmínky	Padělaná zařízení	Hardware	Data o pohybu	Není aktivováno	Výstupní data	Napájení	Bezpečnostní data	Software	Uložená data	Přístup	Možnost přiznání	Audit	Prokázání totožnosti	Úplnost (integrita)	Výstup	Processing	Spolehlivost	Výměna zabezpečených údajů	
RLB_209 Přerušení napájení															X												X	
RLB_210 Přerušení napájení															X						X							
RLB_211 Obnova nastavení (reset)			X																							X		
RLB_212 Dostupnost dat																								X	X			
RLB_213 Vysunutí karty																										X		
RLB_214 Práce s kartou nebyla správně ukončena																						X						
RLB_215 Vícenásobné užití																										X		
Výměna dat																												
DEX_201 Zabezpečený import dat o pohybu												X																X
DEX_202 Zabezpečený import dat o pohybu												X						X										
DEX_203 Zabezpečený import dat karty							X																					X
DEX_204 Zabezpečený import dat karty							X														X							
DEX_205 Zabezpečený export dat do karet							X																					X
DEX_206 Důkaz původu													X												X			
DEX_207 Důkaz původu													X												X			
DEX_208 Zabezpečený export do vnějších médií													X												X			
Podpora šifrováním																												
CSP_201 Algoritmus																										X	X	
CSP_202 Generace klíče																										X	X	
CSP_203 Distribuce klíče																										X	X	
CSP_204 Přístup ke klíči																										X	X	
CSP_205 Zničení klíče																										X	X	

VŠEOBECNÉ POŽADAVKY NA BEZPEČNOST KARTY TACHOGRAFU

1. Úvod

Tento dokument obsahuje popis karty tachografu, jakým ohrožením musí odolávat a jaká bezpečnostní skutečnosti musí získat. Dokument stanovuje funkce zajišťující bezpečnost. Dokument stanovuje požadovanou minimální pevnost bezpečnostního mechanismu a požadovanou úroveň zajištění vývoje a hodnocení.

Požadavky, které dokument stanovuje, odpovídají hlavní části přílohy IB. V zájmu lepší srozumitelnosti může někdy docházet k duplicitě mezi požadavky hlavní části přílohy IB a požadavky záměrů bezpečnosti. V případě nejednoznačnosti požadavků bezpečnostních záměrů a požadavků hlavní části přílohy IB v oblasti požadavků bezpečnostních záměrů, jsou rozhodující požadavky hlavní části přílohy IB.

Požadavky hlavní části přílohy IB, které nejsou uvedeny v bezpečnostních záměrech, nejsou předmětem funkcí zajišťujících bezpečnost.

Karta tachografu je standardní programovatelná karta určeným použitím v tachografu a musí vyhovovat současným požadavkům na funkci a zajištění bezpečnosti programovatelných karet. Tento cíl bezpečnosti proto zahrnuje jen zvláštní bezpečnostní požadavky, které jsou pro použití tachografu potřebné.

Pro lepší přiřazení současných pojmů k dokumentaci o vývoji a hodnocení jsou pro možná ohrožení bezpečnosti a plnění cílů, skutečností, a SEF specifikacím přidělena jednotná označení.

2. Zkratky, definice a odkazy

2.1 Zkratky

IC	Integrovaný obvod (elektronická součást, konstruovaná k zpracovávání dat a/nebo k funkci paměti).
OS	Operační systém
PIN	Osobní identifikační číslo
ROM	Read only memory (permanentní paměť)
SFP	Postup bezpečnostních funkcí
TBD	To be defined (je třeba definovat)
TOE	Cíl hodnocení
TSF	Bezpečnostní funkce TOE
VU	Celek ve vozidle

2.2 Definice

Digitální tachograf	Záznamové zařízení
Citlivá data	Data, uložená na kartě tachografu, která musí být ochráněny z hlediska úplnosti (integrity), neoprávněných změn a důvěrnosti (pokud je použitelné pro bezpečnostní data). Citlivá data zahrnují bezpečnostní data a data uživatele.
Bezpečnostní data	Specifické údaje, potřebné pro podporu funkcí zajišťujících bezpečnost (např. šifrovací klíče)
Systém	Zařízení, osoby nebo organizace, jakkoliv související se záznamovým zařízením
Uživatel	Jakákoliv jednotka (osoba nebo externí IT jednotka) mimo TOE, která spolupracuje s TOE (pokud se nevyužije ve smyslu „data uživatele“)
Data uživatele	Citlivá data uložená na kartě tachografu, jiná než bezpečnostní data. Data uživatele zahrnují identifikační data a data o aktivitě.
Identifikační data	Identifikační data zahrnují identifikační data karty a identifikační data držitele karty.
Identifikační data karty	Data uživatele, která se vztahují k identifikaci karty podle definice požadavků 190, 191, 192, 194, 215, 231 a 235.
Identifikační data držitele karty	Data uživatele, která se vztahují k identifikaci držitele karty podle definice požadavků 195, 196, 216, 232 a 236.
Data aktivit	Data aktivit zahrnují data aktivit, událostí, vadných dat a data kontroly aktivit držitele karty.
Data aktivity držitele karty	Data uživatele, která se vztahují k aktivitám konaným držitelem karty podle definice požadavků 197, 199, 202, 212, 212a, 217, 219, 221, 226, 227, 229, 230a, 233 a 237.
Data událostí a vadná data	Data uživatele, která se vztahují k událostem nebo závadám podle definice požadavků 204, 205, 207, 208 a 223.
Data kontroly aktivit	Data uživatele, která se vztahují ke kontrolám uplatňování práva podle definice požadavků 210 a 225.

2.1 Odkazy

ITSEC	Information Technology Security Evaluation Kriteria 1991 = informace o kritériích hodnocení bezpečnostní technologie 1991.
IC PP	Smartcard Integrated Circuit Protection Profile = integrovaný obvod ochrany programovatelné karty.

ES PP Smart Card Integrated Circuit with Embedded Software protection profile =
Integrovaný obvod programovatelné karty s vloženou ochranou software.

3. Princip výrobku

3.1 Popis karty tachografu a postup užití

Karta tachografu je programovatelná karta podle popisu v IC PP a ES PP, opatřená aplikací, určenou pro její užití se záznamovým zařízením.

Základními funkcemi karty tachografu jsou:

- uložení identifikačních dat karty a identifikačních dat držitele karty. Tato data využívá celek ve vozidle k identifikaci držitele karty, výkonu příslušných funkcí a práv přístupu k datům a k zajištění možnosti přiřazení držitele karty k jeho vlastním aktivitám;
- ukládání dat o aktivitách držitele karty, událostech a vadných datech a dat kontroly aktivit ve vztahu k držiteli karty.

Karta tachografu je proto určena k užití v zařízení rozhraní karty v celku ve vozidle. Lze ji také užít ve kterémkoliv čtecím zařízení pro karty (např. v osobním počítači), které má plná přístupová práva ke čtení kterýchkoliv dat uživatele.

V průběhu konečné fáze užití karty tachografu v jejích životnostní cyklu (fáze 7 životního cyklu podle popisu v ES PP mohou na kartu zapisovat data uživatele pouze celky ve vozidlech.

Funkční požadavky pro kartu tachografu jsou stanoveny v základním textu přílohy I B a v dodatku 2.

3.2 Životní cyklus karty tachografu

Životní cyklus karty tachografu odpovídá životnímu cyklu programovatelné karty, který je popsán v ES PP.

3.3 Ohrožení bezpečnosti

Mimo obecného ohrožení bezpečnosti programovatelné karty, popsaného v ES PP a IC PP, může být karta tachografu vystavena následujícím ohrožením bezpečnosti:

3.3.1 Konečné cíle

Konečným cílem napadajících osob bude změna dat uživatele, které jsou na TOE uloženy.

T.Ident_Data Úspěšná změna identifikačních dat, uložených na TOE (např. typu karty nebo data vypršení platnosti karty, nebo identifikačních dat držitele karty) by umožnila podvodné využití TOE a byla by hlavním bezpečnostním ohrožením obecné bezpečnosti podstaty systému.

T.Activity_Data Úspěšná změna dat o aktivitách, uložených na TOE, by byla bezpečnostním ohrožením TOE.

T.Data_Exchange Úspěšná změna dat o aktivitách (doplnění, vypuštění, změna) v průběhu importu nebo exportu by byla bezpečnostním ohrožením TOE.

3.3.2 Cesty napadení

TOE aktiva mohou být napadena takto:

- snahou o nelegální znalost konstrukce hardware a software TOE a zvláště o jejich bezpečnostních funkcích nebo bezpečnostních datech. Nelegální znalost je možno získat vstupem do materiálů konstruktéra nebo výrobce (krádež, korupce,) nebo přímým prověřením TOE (fyzikální pokusy, analýza výsledků,),
- získáním výhod z nedostatků v konstrukci nebo v realizaci TOE (využití závad v hardware, závady v software, chyby v přenosu, závady TOE vyvolané napadením prostředí, využití nedostatků v bezpečnostních funkcích, jako je postup ověřování totožnosti, data řízení přístupu, šifrovací operace,).
- změna TOE nebo jeho bezpečnostních funkcí fyzikálním, elektrickým nebo logickým napadením nebo jejich kombinací.

3.4 Cíle bezpečnosti

Hlavním cílem systému digitálního tachografu je následující:

O.Main Kontrolním orgánům musí být ke kontrole dostupné údaje, údaje musí plně a přesně udávat aktivity kontrolovaného řidiče a vozidla z hlediska doby jízdy, doby pracovní pohotovosti, doby odpočinku a rychlosti vozidla.

K cílům všeobecné bezpečnosti přispívají proto cíle bezpečnosti TOE takto:

O.Card_Identification_Data TOE Musí chránit data identifikace karty a identifikační data držitele karty, uložená v průběhu personalizace karty.

O.Card_Activity_Storage TOE musí chránit data uživatele, uložená na kartu celkem ve vozidle.

3.5 Cíle bezpečnosti informační technologie

Mimo obecného cíle bezpečnosti programovatelné karty, popsáno v ES PP a IC PP, jsou specifické IT bezpečnostní cíle TOE, které přispívají k celkovým bezpečnostním cílům v průběhu konečné fáze užití karty tachografu v jejím životnostním cyklu, tyto:

O.Data_Access TOE musí omezit přístup k zapisování dat uživatele celkům ve vozidla s prokázanou totožností,

O.Secure_Communications TOE musí být schopen podporovat bezpečnou komunikaci protokolů a postupů mezi kartou a rozhraním karty, pokud je komunikace využitím požadována.

3.6 Prostředky fyzikální, personální a procedurální

Fyzikální, personální a procedurální požadavky, které přispívají k bezpečnosti TOE jsou sepsány v ES PP a IC PP (kapitoly o cílech bezpečnosti pro okolní prostředí).

4. Funkce zajišťující bezpečnost

Tebto odstavec upřesňuje některé povolené operace, jako je přiřazení nebo volba ES PP a stanovuje doplňující SEF funkční požadavky.

4.1 Vyhovění ochranným profilům

CPP_301 TOE musí vyhovovat IC PP

CPP_302 TOE musí vyhovovat ES PPP, jak bylo dříve upřesněno.

4.2 Identifikace a prokázání totožnosti uživatele

Karta musí identifikovat jednotku, do které je vložena a musí znát, zda se jedná o ověřený celek ve vozidle nebo nikoliv. Karty má exportovat jakákoliv data uživatele do každé jednotky se kterou je propojena, s výjimkou kontrolní karty, která má exportovat identifikační data držitele karty pouze do ověřených celků ve vozidle (tak, aby kontrolor byl ujistěn, že celek ve vozidle není padělaný tím, že zjistí jeho název na displeji nebo ve výtisku).

4.2.1 Identifikace uživatele

Přiřazení (FIA_UID.1.1) *Soupis TSF zprostředkovaných akcí:* žádný.

Přiřazení (FIA_ATD.1.1) *Soupis bezpečnostních vlastností:*

USER_GROUP VEHICLE_UNIT.NON_VEHICLE_UNIT,

USER_ID registrační číslo vozidla a kód registrujícího členského státu (USER_ID je znám pouze pro USER_GROUP = VEHICLE_UNIT)

4.2.2 Prokázání totožnosti uživatele

Přiřazení (FIA_UAU.1.1) *Soupis TSF bezpečnostních akcí.*

- karta řidiče a dílenská karta: Export dat uživatele s bezpečnostními vlastnostmi (funkce převedení dat karty).
- Kontrolní karta: Export dat uživatele bez bezpečnostních vlastností s výjimkou identifikačních dat držitele karty.

UIA_301 Totožnost celku ve vozidle se prokáže pomocí zajištění, že celek ve vozidle vlastní bezpečnostní data, která by mohl distribuovat pouze systém.

Výběr (FIA_UAU.3.1 a FIA_UAU.3.2): chránit

Přiřazení (FIA_UAU.4.1) *Identifikovaný mechanismus (mechanizmy) k prokázání totožnosti*: jakýkoliv mechanismus k prokázání totožnosti.

UIA_302 Dílenská karta musí zajišťovat doplňující mechanismus k prokázání totožnosti ověřením PIN kódu (tento mechanismus je určen pro celek ve vozidle k zaručení identifikace držitele karty, není určen k ochraně obsahu dílenské karty).

4.2.3 Selhání v prokázání totožnosti

Následující přiřazení popisují reakci karty na každé jednotlivé selhání v prokázání totožnosti uživatele.

Přiřazení (FIA_AFL.1.1) *Číslo*: 1, soupis událostí při prokazování totožnosti: prokázání totožnosti rozhraní karty.

Přiřazení (FIA_AFL.1.2) *Soupis akcí*:

- varování připojené jednotky,
- označit uživatele jako NON_VEHICLE_UNIT.

Následující přiřazení popisují reakci karty v případě selhání doplňujícího mechanismu v prokazování totožnosti, požadovaného v UIA_302.

Přiřazení (FIA_AFL.1.1) *Číslo*: 5, *soupis událostí při prokazování totožnosti*: kontroly PIN (dílenská karta).

Přiřazení (FIA_AFL.1.2) *Soupis akcí*.

- varování připojené jednotky,
- zablokování postupu ověřování PIN tak, aby jakýkoliv následný pokus o ověřování PIN selhal,
- umožnit následujícímu uživateli zjistit důvod zablokování.

4.3 Kontrola přístupu

4.3.1 Postup kontroly přístupu

V průběhu konečné fáze užití karty tachografu je karta tachografu předmětem jediného postupu kontroly k přístupu k bezpečnostní funkci SFP, nazývaného AC_SFP.

Přiřazení (FDP_ACC.2.1) *Kontrola přístupu SFP*: AC_SFP.

4.3.2 Funkce kontroly přístupu

Přiřazení (FDP_ACF.1.1) *Kontrola přístupu: AC_SFP.*

Přiřazení (FDP_ACF.1.2) *Pravidla řídicí přístup mezi kontrolovanými tématy a kontrolovanými předměty užitím kontrolních operací na kontrolovaných předmětech:*

GENERAL_READ Data uživatele mohou být čtena z TOE kterýmkoliv uživatelem s výjimkou identifikačních dat uživatele, která mohou být čtena z kontrolní karty pouze celkem ve vozidle.

IDENTIF_WRITE Identifikační data je možno zapisovat pouze jednou před koncem fáze 6 životnostního cyklu karty.

ACTIVITY_WRITE Data o aktivitách mohou být zapisována do TOE pouze celkem ve vozidle.

SOFT_UPGRADE Žádný z uživatelů nemůže modernizovat (upgrade) TOE software.

FILE_STRUCTURE Struktura souborů a podmínky přístupu musí být vytvořeny před koncem fáze 6 životnostního cyklu TOE a pak musí být uzamčeny proti jakékoliv budoucí změně nebo vymazání kterýmkoliv uživatelem.

4.4 Možnost přiřazení

ACT_301 TOE musí udržovat trvalá identifikační data.

ACT_302 Musí být zajištěna indikace času a datum personalizace TOE. Indikace musí být nezaměnitelná.

4.5 Audit

TOE musí monitorovat události, které indikují možná poškození jeho bezpečnost.

Přiřazení (FAU_SAA.1.2) *Dílčí sada definovaných auditovatelných událostí.*

- selhání v prokázání totožnosti držitele karty (5 po sobě jdoucích neúspěšných ověření PIN),
- závada v autotestech,
- závada úplnosti (integrity) uložených dat,
- závada úplnosti (integrity) vstupních dat o aktivitách.

4.6 Přesnost

4.6.1 Úplnost (integrity uložených dat)

Přiřazení (FDP_SDI.2.2) *Akce, které je třeba vykonat: varování připojené jednotky.*

4.6.2 *Prokázání totožnosti základních dat*

Přiřazení (FDP_DAU.1.1) *Soupis typů předmětů nebo informací:* data o aktivitách.

Přiřazení (FDP_DAU.1.2) *Soupis témat:* jakékoliv.

Požadavky tohoto odstavce se použijí pouze v případě, když je VU tvořen fyzicky oddělenými částmi.

4.7 **Spolehlivost funkce**

4.7.1 *Zkoušky*

Výběr (FPT_TST.1.1): v průběhu počátečního nastartování, periodicky při obvyklé činnosti.

Poznámka: pojem v průběhu počátečního nastartování se rozumí dříve, než je zapracován kód (a nikoliv nezbytně v průběhu postupu Answer to Reset (odezva na obnovu nastavení/resetování)).

RLB_301 Autotest TOE musí zahrnovat ověření úplnosti jakéhokoliv kódu software, který není uložen na ROM.

RLB_302 Po zjištění závady v autotesty musí TSF varovat připojenou jednotku.

RLB_303 Poté co je zkouška OS dokončena, musí být veškeré povely specifické pro zkoušku zablokovány nebo odstraněny. Nesmí být možné tyto kontroly potlačit a obnovit je pro užívání. Povely, spojené výhradně se stavem jednoho životnostního cyklu, nesmějí být nikdy přístupné v průběhu jiného stavu.

4.7.2 *Software*

RLB_304 Nesmí existovat žádný způsob jak při užívání TOE analyzovat, ladit nebo měnit software.

RLB_305 Vstupy z vnějších zdrojů nesmí být použitelné jako spouštěcí kódy.

4.7.3 *Napájení*

RLB_306 TOE musí v průběhu přerušení napájení nebo v průběhu jeho změn uchovat bezpečný stav.

4.8 **Výměna dat**

4.8.1 *Výměna dat s celkem ve vozidle*

DEX_301 TOE musí ověřit úplnost (integritu) a totožnost dat, importovaných z celku ve vozidle.

DEX_302 Po zjištění závady v úplnosti (integritě) importovaných dat TOE musí:

- varovat jednotku, která odesílá data,

– data nevyužívat.

DEX_303 TOE musí exportovat data uživatele do celku ve vozidle spolu s bezpečnostními vlastnostmi tak, aby celek ve vozidle byl schopen ověřit úplnost (integritu) a pravost získaných dat.

4.8.2 Export dat do celků mimo vozidlo (funkce převedení)

DEX_304 TOE musí být schopno generovat důkaz o původu dat převáděných do externích médií.

DEX_305 TOE musí být schopno zajistit příjemci možnost ověření důkazu o původu převáděných dat.

DEX_306 TOE musí být schopen převádět data do externích paměťových médií společně s bezpečnostními vlastnostmi tak, aby mohla být úplnost převáděných dat ověřena.

4.9 Podpora šifrováním

CSP_301 Pokud TSF generuje šifrovací klíče, musí tyto klíče odpovídat stanoveným algoritmům generace šifrovacích klíčů a stanovené velikosti šifrovacího klíče. Generované šifrovací klíče musí mít omezený počet možných využití (definuje výrobce, ale nikoliv více než 240).

CSP_302 Pokud TSF šifrovací klíče distribuuje, musí distribuce odpovídat stanoveným postupům distribuce klíčů.

5. Definice bezpečnostních mechanismů

Požadované bezpečnostní mechanismy jsou stanoveny v dodatku 11.

Veškeré ostatní bezpečnostní mechanismy stanoví výrobce TOE.

6. Minimální pevnost bezpečnostních mechanismů

Minimální pevnost mechanismu pro kartu tachografu je podle ITSEC **Vysoká**.

7. Úroveň zajištění

Cílovou úrovní zabezpečení karty tachografu je ITSEC úroveň E3 podle definice v ITSEC.

8. Základní principy

Následující matrice podává základní principy SEF tím že udává:

– které SEF působí proti kterému ohrožení,

která SEF plní které IT cíle bezpečnosti.

	Ohrožení										IT předměty									
	T.CLON	T.DIS_ES2	T.T_ES	T.T_CMD	T.MOD_SOFT*	T.MOD_LOAD	T.MOD_EXE	T.MOD_SHARE	Ident_Data	Activity_Data	Data_Exchange	O.TAMPER_ES	O.CLON*	O.OPERATE*	O.FLAV*	ODIS_MECHANISM2	O.DIS_MEMORY*	O.MOD_MEMORY*	Data_Access	Secured_Communication
UIA_301 Prostředky prokázání totožnosti																			x	
UIA_302 Ověření PIN																			x	
ACT_301 Identifikační data																				
ACT_302 Data personalizace																				
RLB_301 Úplnost software													x	x						
RLB_302 Autotest													x	x						
RLB_303 Zkoušky při výrobě					x	x						x	x							
RLB_304 Analýza software					x		x	x				x	x							
RLB_305 Vstup software					x	x		x				x	x							
RLB_306 Napájení									x	x		x	x							
RLB_307 Obnovení nastavení												x	x							
DEX_301 Import zabezpečených dat											x									x
DEX_302 Import zabezpečených dat											x									x
DEX_303 Export zabezpečených dat do VU											x									x
DEX_304 Evidence původu											x									x
DEX_305 Evidence původu											x									x
DEX_306 Zabezpečený export do externích médií											x									x
CSP_301 Generace klíče												x								x
CSP_302 Distribuce klíče												x								x

*Dodatek 11***SPOLEČNÉ BEZPEČNOSTNÍ MECHANIZMY****OBSAH**

Společné bezpečnostní mechanismy	330
1. Všeobecně	332
1.1 Odkazy	332
1.2 Značení a zkratky	333
2. Šifrovací systém a algoritmus Šifrování	335
2.1 Šifrovací systém	335
2.2 Algoritmus šifrování	335
2.2.1 Algoritmus RSA	335
2.2.2 Algoritmus transformace	335
2.2.3 Algoritmus šifrování dat	335
3. Klíče a certifikáty	336
3.1 Generace a distribuce klíčů	336
3.1.1 Generace a distribuce klíčů RSA	336
3.1.2 Zkušební klíče RSA	337
3.1.3 Klíče snímače pohybu	338
3.1.3 Klíče snímače pohybu	338
3.2 Klíče	338
3.3 Certifikáty	339
3.3.1 Obsah certifikátu	339
3.3.2 Vydané certifikáty	341
3.3.3 Ověření a rozvinutí certifikátů	342
4. Vzájemné prokázání totožnosti	343
5. Důvěrnost přenosu dat karet VU, úplnost a mechanismus prokazování totožnosti	345
5.1 Secure Messaging (bezpečné zpracování zpráv)	345
5.2 Zacházení se závadami v secure messaging (bezpečné zpracování zpráv) ..	348
5.3 Algoritmus k výpočtu šifrovacího kontrolního součtu	348
5.4 Algoritmus výpočtu šifer pro důvěrnost DOs	349
6. Mechanizmy digitálních podpisů při stahování dat	350

6.1	Generace podpisu.....	350
6.2	Ověření podpisu.....	350

1. Všeobecně

Tento dodatek stanovuje bezpečnostní mechanismy, které zajišťují:

- vzájemné ověřování totožnosti mezi celky ve vozidlech kartami tachografu, včetně odsouhlasení užitého klíče,
- důvěrnost, úplnost a prokázání totožnosti dat, přenášených mezi celky ve vozidlech a kartami tachografu,
- úplnost a prokázání totožnosti dat, převáděných z celků ve vozidlech do externího paměťového média.
- úplnost a prokázání totožnosti dat, převáděných z karty tachografu do externího paměťového média.

1.1 Odkazy

V tomto dodatku jsou užívány následující odkazy:

SHA-1 National Institute of Standards and Technology (NIST – Národní institut pro normy a technologii), FIPS Publikace 180-1: Secure Hash Standard (Norma bezpečné transformace), duben 1995

PKCS1 RSA Laboratoriem. PKCS # 1: RSA Encryption Standard (Norma šifrování). Verze 2.9, říjen 1998.

TDES National Institute of Standards and Technology (NIST – Národní institut pro normy a technologii), FIPS Publikace 46-3:: Data encryption Standard, Draft 1999 (Norma šifrování dat, návrh 1999).

TDES-OP ANSI X9.52, Triple Data Encryption Algorithm Modes of Operation (Trojitý pracovní mód algoritmu šifrování dat). 1998.

ISO/IEC 7816-4 Informační technologie – Identifikační karty – Karty s integrovaným obvodem (obvody) s kontakty – Část 4: Vnitroprůmyslové povely pro vnitřní výměnu. Prvá edice: 1993 + Změna 1: 1997.

ISO/IEC 7816-6 Informační technologie – Identifikační karty – Karty s integrovaným obvodem (obvody) s kontakty – Část 6: Vnitroprůmyslové prvky dat. Prvá edice: 1996 + Oprava 1: 1998.

ISO/IEC 7816-8 Informační technologie – Identifikační karty – Karty s integrovaným obvodem (obvody) s kontakty – Část 8: Vnitroprůmyslové povely ve vztahu k bezpečnosti. Prvá edice: 1999.

ISO/IEC 9796-2 Informační technologie – Bezpečnostní technika – Schemata digitálních podpisů, poskytující obnovu zprávy – Část 2: Mechanismus s využitím transformační funkce: 1997.

ISO/IEC 9798-3 Informační technologie – Bezpečnostní technika – Mechanismus ověření totožnosti jednotky – Část 2: Ověřování totožnosti s užitím algoritmu obecného klíče. Druhé vydání: 1998.

ISO 16844-3 Silniční vozidla – Systémy tachografů – Část 3: Rozhraní snímače pohybu.

1.2 Značení a zkratky

V tomto dodatku jsou užity následující značení a zkratky:

(K_a, K_b, K_c) balíček klíče pro užití trojitého algoritmu šifrování dat,

CA certifikační orgán,

CAR odkaz na certifikační orgán,

CC kontrolní součet šifry,

CG šifrovaný záznam,

CH hlavička příkazu,

CHA autorizace držitele certifikátu,

CHR odkaz na držitele certifikátu,

D() dešifrování pomocí DES

DE prvek dat,

DO předmět dat,

d neveřejný klíč RSA, neveřejný zmocněnec,

e obecný klíč RSA, obecný zmocněnec,

E() šifrování pomocí DES,

EQT zařízení,

Hash() hodnota transformace, výstup transformace,

Hash transformační funkce,

KID identifikátor klíče,

K_m klíč TDES. Hlavní klíč podle definice ISO 16844-3,

K_{m_{vu}} klíč TDES, vložený do celku ve vozidle,

K_{m_{wc}} klíč TDES, vložený do dílenské karty,

m	celé číslo mezi 0 a $n-1$, reprezentující zprávu,
n	klíče RSA, modul,
PB	doplňkové byty,
PI	indikační doplňkový byt (užití v šifře pro důvěrnost DO),
PV	jednoduchá hodnota,
s	představitel podpisu, celé číslo mezi 0 a $n-1$,
SSC	odeslání údaje čítače posloupnosti,
SM	bezpečné zpracování zpráv,
TCBC	TDEA blok číslic svazující operační módy,
TDEA	trojitý algoritmus šifrování dat,
TLV	hodnota délky jmenovky,
VU	celek ve vozidle,
X.C	certifikát uživatele X, vydaný certifikačním orgánem,
X.CA	certifikující orgán uživatele X,
X.CA.PK _o X.C	operace rozbalení certifikátu pro vyjmutí obecného klíče. Je to zaváděcí operátor, jehož levý operand je obecným klíčem certifikačního orgánu a jehož pravý operand je certifikátem, vydaným certifikačním orgánem. Výstupem je obecný klíč uživatele X, jeho certifikát je pravým operandem,
X.PK	obecný klíč uživatele X,
X.PK[I]	RSA zašifrování některých informací I při užití obecného klíče uživatele X,
X.SK	RSA neveřejný klíč uživatele X,
X.SK[I]	RSA zašifrování některých informací I při užití neveřejného klíče uživatele X,
'xx'	hexadecimální hodnota,
	operátor kaskádového spojení.

6. 2. ŠIFROVACÍ SYSTÉM A ALGORITMUS ŠIFROVÁNÍ

2.1 Šifrovací systém

CSM_001 celky ve vozidle a karty tachografu musí užívat klasický šifrovací systém RSA obecného klíče k tomu, aby vytvořily následující bezpečnostní mechanismy:

- prokazování totožnosti mezi celky ve vozidlech a kartami,
- převod trojitých DES klíčů jednání mezi celky ve vozidlech a karet tachografů,
- digitální podpis dat převedených z celků ve vozidlech nebo karet tachografu do externích médií.

CSM_002 celky ve vozidle a karty tachografu musí užívat trojitý DES symetrický šifrovací systém k tomu, aby v průběhu výměny dat uživatele mezi celky ve vozidlech a kartami tachografu vytvořily mechanismus pro udržení úplnosti dat a aby popřípadě zajistily důvěrnost výměny dat mezi celky ve vozidlech a kartami tachografu.

2.2 Algoritmus šifrování

2.2.1 Algoritmus RSA

CSM_003 Algoritmus RSA je plně definován následujícími rovnicemi:

$\begin{aligned} \text{X.SK}[m] &= s = m^d \bmod n \\ \text{X.PK}[s] &= m = s^e \bmod n \end{aligned}$
--

Obsažnější popis funkce RSA lze nalézt v odkazu (PKCS1).

Obecný exponent e pro výpočet RSA bude odlišný od čísla 2 ve všech generovaných RSA klíčích

2.2.2 Algoritmus transformace

CSM_004 mechanismus digitálního podpisu musí užívat algoritmus SHA-1 podle definice v odkazu (SHA-1).

2.2.3 Algoritmus šifrování dat

CSM_005 algoritmus, založený na DES musí být užit v operačním módu „Cipher Block Chaining“.

3. Klíče a certifikáty

3.1 Generace a distribuce klíčů

3.1.1 Generace a distribuce klíčů RSA

CSM_006 klíče RSA musí být generovány prostřednictvím tří funkčních úrovní:

- evropská úroveň,
- úroveň členského státu,
- úroveň zařízení.

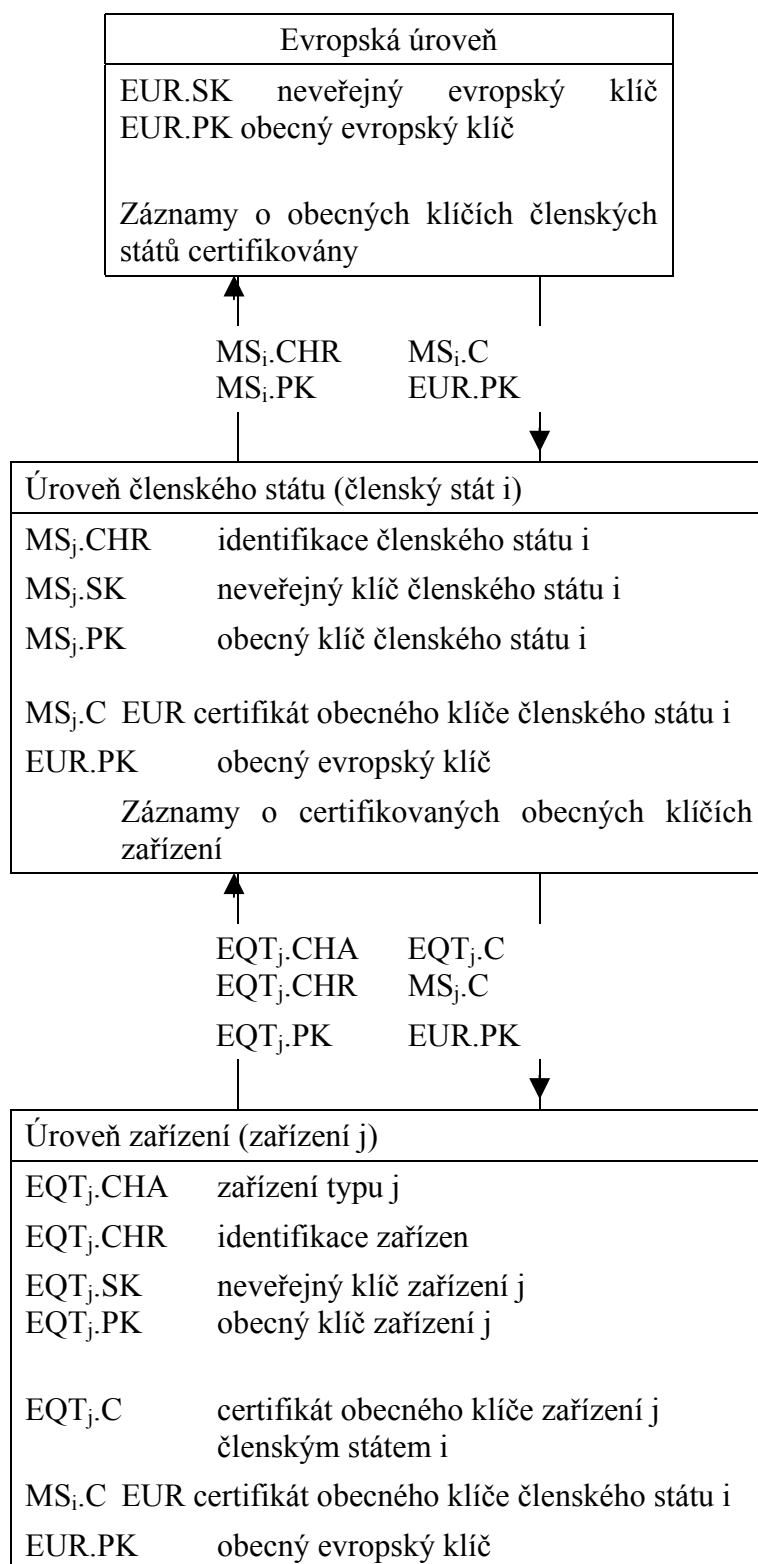
CSM007 na evropské úrovni musí být generován jediný pár evropských klíčů (EUR.SK a EUR.PK). Evropský neveřejný klíč musí být užíván k certifikaci obecných klíčů členských států. Musí být udržovány záznamy o všech certifikovaných klíčích. Tento cíl musí zajišťovat Evropská certifikační organizace pod pravomocí a odpovědností Evropské komise.

CSM_008 na úrovni členského státu musí být generován pár klíčů (MS.SK a MS.PK). Neveřejné klíče členských států musí být certifikovány Evropskou certifikační organizací. Neveřejný klíč členského státu se musí užívat k certifikaci obecných klíčů, které se mají vkládat do zařízení(celek ve vozidle nebo karta tachografu). Musí být udržovány záznamy o všech certifikovaných obecných klíčích spolu s identifikací zařízení, pro která jsou určeny. Tento cíl musí zajišťovat certifikační organizace členského státu. Členský stát může pravidelně svůj pár klíčů měnit.

CSM_009 na úrovni zařízení musí být generován pár klíčů (EQT.SK a EQT.PK) a musí být vložen do každého zařízení. Obecné klíče zařízení musí být certifikovány certifikační organizací členského státu. Tyto povinnosti mají být zajištěny výrobcí zařízení, adresáty zařízení nebo organizacemi členského státu. Tento pár klíčů se užívá pro prokazování totožnosti, digitální podpis a šifrovací služby.

CSM_010 během generace, dopravy (popřípadě) a skladování musí být zachována důvěrnost neveřejných klíčů.

Následující vyobrazení shrnuje tok dat v tomto procesu:



3.1.2 Zkušební klíče RSA

CSM_011 Pro zkoušení zařízení (včetně zkoušek vzájemné spolupráce) musí Evropská certifikační organizace generovat odlišný jediný evropský pár zkušebních klíčů a nejméně dva páry zkušebních klíčů členských států, z nich musí být obecné klíče certifikovány neveřejným evropským

zkušební klíčem. Výrobci musí do zařízení, které je podrobeno zkoušce schválení typu, vložit zkušební klíče, certifikované jedním z těchto zkušebních klíčů členského státu.

3.1.3 Klíče snímače pohybu

Důvěrnost níže uvedených tří klíčů TDES musí být příslušně zachována v průběhu generace, dopravy (popřípadě) a skladování.

Pro podporu vyhovění záznamového zařízení normě ISO 16844, musí Evropská certifikační organizace a dále certifikační orgány členských států zajistit následující:

CSM_036 Evropská certifikační organizace musí generovat $K_{m_{VU}}$ a $K_{m_{WC}}$, dva nezávislé a jedinečné klíče Triple DES a generovat K_m jako:

$$K_m = K_{m_{VU}} \text{ XOR } K_{m_{WC}}$$

Evropská certifikační organizace musí tyto klíče za příslušných bezpečných postupů předat na vyžádání členských států jejich certifikační orgánům.

CSM_037 certifikační organizace členských států musí:

- užít K_m k šifrování dat snímače pohybu podle požadavku výrobce snímače pohybu (Data, která mají být šifrována pomocí K_m definuje ISO 16844-3),
- předat $K_{m_{VU}}$ výrobcům celků ve vozidlech pro vložení do celků ve vozidlech za příslušně zabezpečených postupů,
- zajistit, aby $K_{m_{WC}}$ bylo v průběhu personalizace karty vloženo do všech dílenských karet (SensorInstallationSecData do základního souboru Sensor_Installation_Data).

3.1.3 Klíče snímače pohybu

CSM_012 celky ve vozidle a karty tachografu musí jako součást postupu vzájemného prokázání totožnosti generovat a vzájemně si vyměnit data potřebná pro vypracování společného klíče Triple DES. Důvěrnost této výměny dat musí být ochráněna šifrovacím mechanismem relace RSA.

CSM_013 tento klíč musí být užit u všech následujících šifrovacích operacích za užití opatření pro zabezpečení. Jeho platnost končí ukončením relace (odejmutí karty nebo obnovením nastavení karty) a/nebo po 240 užití (jedno užití klíče = jeden povel, užívající bezpečnostní zpracování zprávy odeslané na kartu a odpovídající odezva).

3.2 Klíče

CSM_014 klíče RSA musí mít (na kterékoliv úrovni) následující délku: modul n 1024 bitů, obecný exponent e 64 bitů maximálně, neveřejný exponent d 1024 bitů.

CSM_015 klíče Triple DES musí mít tvar (K_a , K_b , K_a), kde K_a a K_b jsou nezávislé klíče, dlouhé 64 bitů. Nenastavují se žádné bity pro detekci závad v paritě.

3.3 Certifikáty

CSM_016 certifikáty RSA obecných klíčů musí být certifikáty „non self-descriptive“ (nepopisné) „Card Verifiable“ (ověřující kartu).

3.3.1 Obsah certifikátu

CSM_017 certifikáty obecných klíčů RSA jsou tvořeny dále uvedenými daty a následujícím pořadím:

Data	Formát	Bytů	Předmět
CPI	INTEGER	1	Identifikátor profilu certifikátu (pro tuto verzi '01')
CAR	OCTET STRING	8	Odkaz na certifikující organizaci
CHA	OCTET STRING	7	Autorizace držitele certifikátu
EOV	TimeReal	4	Konec platnosti certifikátu. Volitelné, 'FF' pokud se neužije
CHR	OCTET STRING	8	Odkaz na držitele certifikátu
n	OCTET STRING	128	Obecný klíč (modul)
e	OCTET STRING	8	Obecný klíč (obecný exponent)
		164	

Poznámky:

1. „Identifikátor profilu certifikátu“ (CPI) stanovuje přesnou strukturu certifikátu prokázání totožnosti. Může být užit jako interní identifikátor zařízení pro odpovídající návěští, které popisuje slučování prvků dat v certifikátu.

Návěští spojené s obsahem certifikátu je následující:

'4D'	'16'	'5F 29'	'01'	'42'	'08'	'5F 4B'	'07'	'5F 24'	'04'	'5F 20'	'08'	'7F 49'	'05'	'81'	'81 80'	'82'	'08'
Rozšířené návěští jmenovky	Délka návěští	Jmenovka CPI	Délka CPI	Jmenovka CAR	Délka CAR	Jmenovka CHA	Délka CHA	Jmenovka EOV	Délka EOV	Jmenovka CHR	Délka CHR	Jmenovka obecného klíče (sestrojit)	Délka následujících DO	Jmenovka modulu	Délka modulu	Jmenovka obecného exponentu	Délka obecného exponentu

2. „Odkaz na certifikující organizaci“ (CAR) má za účel identifikovat orgán vydávající certifikát (CA) tak, aby prvek dat mohl být užit současně jako identifikátor klíče organizace pro odkaz na obecný klíč certifikující organizace (pro kódování, viz níže Identifikátor klíče).
3. „Autorizace držitele certifikátu“ (CHA – užívá se k identifikaci práv držitele certifikátu. Je tvořeno identifikací (ID) použití tachografu a typem zařízení, ke kterému je certifikát určen (podle prvku dat EquipmentType, „00“ pro členský stát.)).
4. „Odkaz na držitele certifikátu“ (CHR) má za účel jednoznačně identifikovat držitele certifikátu tak, aby mohl být užit Data Element (prvek dat) současně jako Subjekt Key Identifier (identifikátor předmětu klíče) jako odkaz na Public Key (obecný klíč) držitele certifikátu.
5. Key Identifiers (Identifikátory klíčů) jednoznačně identifikují držitele certifikátu nebo certifikační organizace. Ty jsou kódovány takto:

5.1 Zařízení (celek ve vozidle nebo karta)

Data	Výrobní číslo zařízení	Datum	Typ	Výrobce
Délka	4 byty	2 byty	1 byt	1 byt
Hodnota	Celé číslo	kódování mm yy BCD	Specifické podle výrobce	Kód výrobce

Při požadování certifikátu pro celek ve vozidle může nebo nemusí výrobce znát identifikaci zařízení, do kterého bude klíč vložen.

V prvním případě zašle výrobce identifikaci zařízení s obecným klíčem certifikační organizací svého členského státu. Certifikát bude v takovém případě zahrnovat identifikaci zařízení a výrobce musí zajistit, že klíče a certifikáty budou vloženy do uvažovaného zařízení. Key Identifier (identifikátor klíče) má tvar uvedený výše.

Ve druhém případě musí výrobce jednoznačně identifikovat každý požadavek na certifikát a musí po instalaci klíče do zařízení zaslat tuto identifikaci s obecným klíčem certifikační organizaci svého členského státu spolu s klíčem přiřazení pro zařízení (tj. identifikaci požadavku certifikace, identifikaci zařízení). Identifikátor klíče má následující tvar:

Data	Pořadové číslo požadavku o certifikaci	Datum	Typ	Výrobce
Délka	4 byty	2 byty	1 byt	1 byt
Hodnota	BCD kódování	kódování mm jj BCD	'FF'	Kód výrobce

5.2 Certifikační organizace

Data	Identifikace organizace	Pořadové číslo klíče	Přídavné informace	Identifikátor
Délka	4 byty	1 byt	2 byty	1 byt
Hodnota	1 byt vnitrostátní číselný kód 3 byty vnitrostátní alfanumerický kód	Celé číslo	Doplňující kódování (specifické pro CA) 'FF FF', pokud se nevyužije	'01'

Pořadové číslo klíče se užívá pro rozlišení různých klíčů členského státu v případě, kdy je klíč měněn.

- Ověřovatel certifikátu musí bezpodmínečně znát, že obecný certifikovaný klíč je RSA klíč platný pro ověřování totožnost, ověření digitálního podpisu a šifrovaný pro důvěrnost služeb (certifikát nezahrnuje žádný Object Identifier (identifikátor předmětu), který jej specifikuje).

3.3.2 Vydané certifikáty

CSM_018 Vydaný certifikát je digitálním podpisem s částečnou obnovou obsahu podle ISO/IEC 9796-2 s připojeným „Certification Authority Reference“ (odkaz na certifikační organizaci).

$$X.C = X.CA.SK[6A] || C_r || Hash(C_c) || BC || C_n || X.CAR$$

Kde je obsah certifikátu = $C_c =$ C_r || C_n
106 bytů || 58 bytů

Poznámky:

1. Tento certifikát je dlouhý 194 bytů.
2. Podpisem překrytá CAR je také k podpisu připojena tak, že obecný klíč certifikační organizace může být pro ověření certifikátu vybrán.
3. Ověřovatel certifikátu musí bezpodmínečně znát algoritmus, užívaný certifikační organizací k podpisování certifikátu.
4. Návěští spojené s obsahem certifikátu je následující:

'7F 21'	'09'	'5F 37'	'81 80'	'5F 38'	'3A'	'42'	'08'
Jmenovka certifikátu CV (sestrojena)	Délka následujících DO	Jmenovka podpisu	Délka podpisu	Ostatní jmenovka	Ostatní délka	Jmenovka CAR	Délka CAR

3.3.3 Ověření a rozvinutí certifikátů

Ověření a rozvinutí certifikátů zahrnuje ověření podpisu podle ISO/IEC 9796-2, vyhledání obsahu certifikátu a obecného klíče, který zahrnuje: $X.PK = X.CA.PK_0X.C$, a ověření platnosti certifikátu.

CSM_019 zahrnuje následující kroky:

Ověřte podpis a vyvolejte obsah:

- z X.C vyvolejte Sign, C_n' a CAR':

$$X.C = \begin{array}{|c|c|c|} \hline \text{Sign} & C_n' & \text{CAR} \\ \hline \text{'128 bytů'} & \text{58 bytů} & \text{8 bytů} \\ \hline \end{array}$$
- z CAR' vyberte příslušný obecný klíč certifikační organizace (pokud nebylo již vybráno jinými prostředky,
- otevřete Sign pomocí obecného klíče CA: $Sr' = X.CA.PK [\text{Sign}]$,
- ověření Sr' začíná na '6A' a končí na 'BC',
- Vypočítejte Cr' a H' ze vztahu:

$$Sr' = \begin{array}{|c|c|c|c|} \hline \text{'6A'} & C_r' & H' & \text{'BC'} \\ \hline \text{'106 bytů'} & & \text{20 bytů} & \\ \hline \end{array}$$
- obnovte obsah certifikátu $C' = C_r' || C_n'$,

- ověřte $Hash(C') = H'$.

Pokud jsou ověření v pořádku (OK), je certifikát pravý a jeho obsahem je C' .

Ověřte platnost $Z C'$:

- pokud je použitelné, ověřte datum ukončení platnosti,

$Z C'$ vyvolejte a uložte obecný klíč, Key Identifier (identifikátor klíče), Certificate Holder Authorization (autorizace držitele certifikátu) a Validity (platnost):

- $X.PK = n || e$,
- $X.KID = CHR$,
- $X.CHA = CHA$,
- $X.EOV = EOVS$.

4. vzájemné prokázání totožnosti

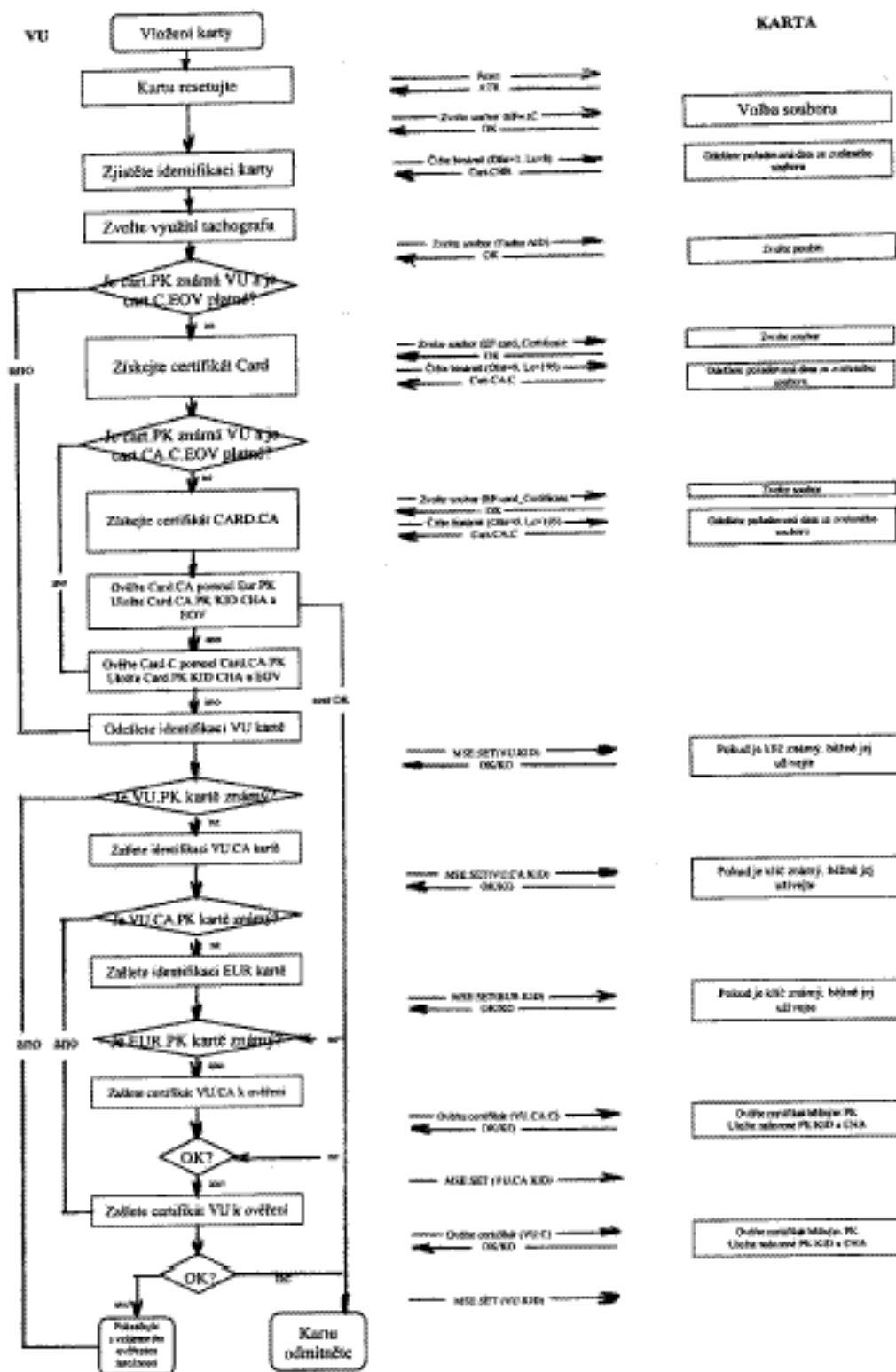
Vzájemné prokázání totožnosti mezi kartami a VU je založeno na následujícím principu:

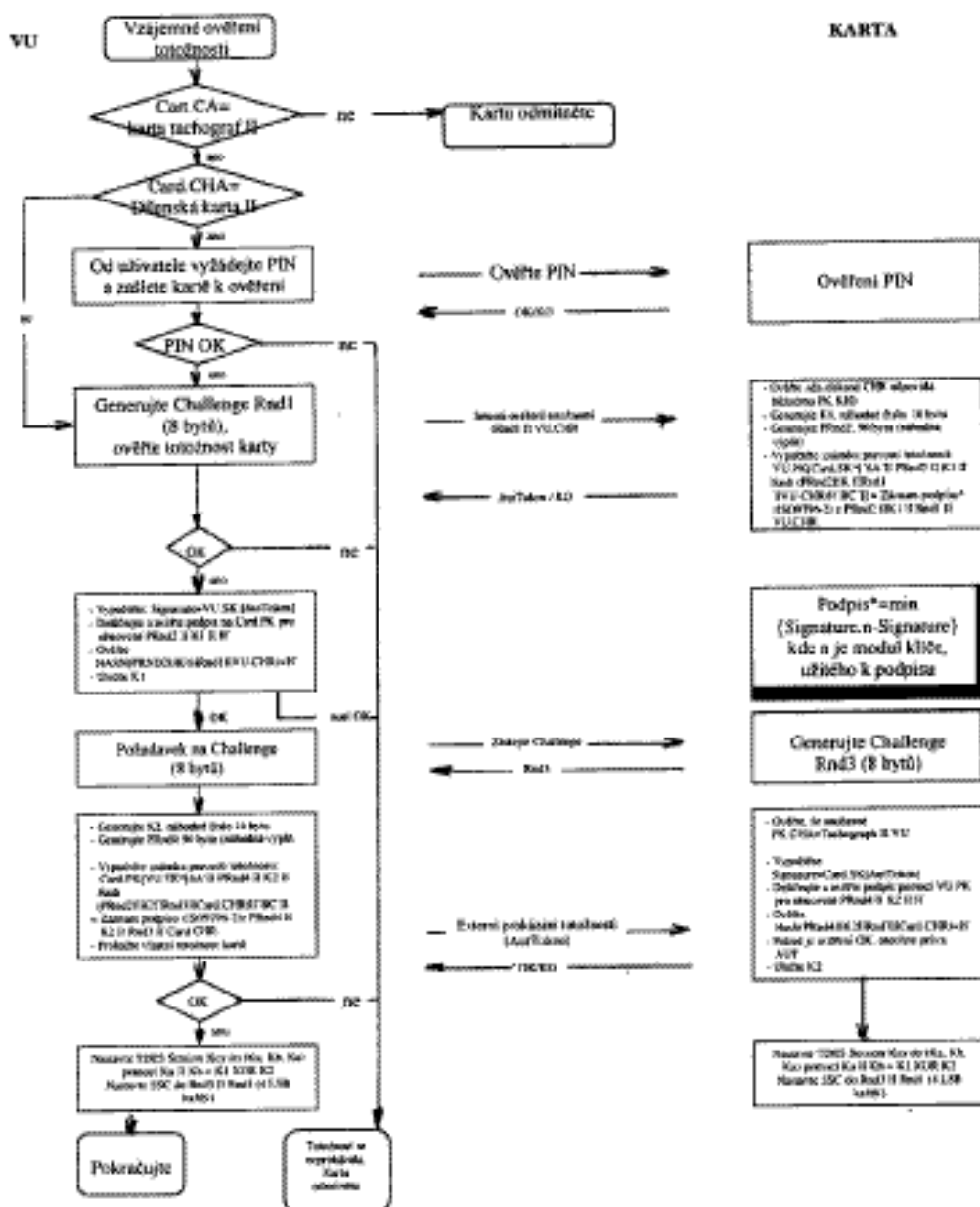
Každá strana dokládá druhé straně, že vlastní platný pár klíčů, ze kterých byl obecný klíč certifikován certifikační organizací členského státu a že sama byla certifikována Evropskou certifikační organizací.

Dokládá se podpisem s neveřejným klíčem na náhodně vybraném čísle, zaslaném druhou stranou, která musí zasílané náhodné číslo při ověřování tohoto podpisu obnovovat.

Mechanismus je spouštěn vložení karty do VU. Mechanismus začíná výměnou a rozvinutím obecného klíče a končí nastavením klíče relace.

CSM_020 použit musí být dále uvedený protokol (šipky označují povely a výměnu dat (viz dodatek 2)):





5. DŮVĚRNOST PŘENOSU DAT KARET VU, ÚPLNOST A MECHANIZMUS PROKAZOVÁNÍ TOTOŽNOSTI

5.1 Secure Messaging (bezpečné zpracování zpráv)

CSM_021 úplnost přenosu dat VU karet musí být chráněna prostřednictvím Secure Messaging (bezpečné zpracování zpráv) podle odkazů ISO/IEC 7816-4 a ISO/IEC 7816-8.

CSM_022 pokud je třeba data v průběhu přenosu chránit, musí se k zasílaným příkazům nebo odezvám datových objektů připojit datový objekt „Cryptographic Checksum“ (kontrolní součet šifrovaných dat).

CSM_023 kontrolní součet šifrovaných dat zaslaných v rámci příkazumusi zahrnovat záhlaví povelu a veškeré odeslané datové objekty (\Rightarrow CLA = '0C' a a veškeré datové objekty musí být uzavřeny jmenovkou, ve které je B1 = 1).

CSM_024 pokud odezva neobsahuje datové pole, musí být stavové informační byty ochráněny kontrolním součtem šifrovaných dat.

CSM_025 kontrolní součet šifrovaných dat musí být dlouhý čtyři byty.

Struktura povelů a odezev při užití bezpečného zpracování dat je proto následující:

Užité DO jsou částečné soubory Secure Messaging DO (bezpečné zpracování DO zpráv) podle popisu v ISO/IEC 7816-4:

Jmenovka	Mnemonika	Znamená
'81'	T _{PV}	Čistá hodnota, nikoliv kódovaná data BER-TLV (chráněna pomocí CC)
'97'	T _{LE}	Hodnota Le v nechráněném povelu (chráněno pomocí CC)
'99'	T _{SW}	Status-Info (chráněn pomocí CC)
'8E'	T _{CC}	Kontrolní součet šifrovaných dat (CC)
'87'	T _{PI CG}	Padding Indicator Byte Kryptogram (čistá hodnota nekódovaná v BER-TLV)

Z nechráněného páru odezvy na povel vychází:

Záhlaví povelu	Těleso povelu
CLA INS P1 P2	(pole L _c) (pole dat) pole L _e)
4 byty	L byty, označené jako B ₁ až B _L

Těleso odezvy	Znak odezvy
(pole dat)	SW1 SW2
L _r datové byty	dva byty

Odpovídající pár zabezpečené odezvy na povel:

Zabezpečený povel:

Záhlaví povelu (CH)	Těleso povelu										
CLA INS P1 P2	Nové pole L _c	Nové pole dat									Nové pole L _e
‘OC’	Délka nového pole dat	T _{PV}	L _{PV}	PV	T _{LE}	L _{LE}	L _e	T _{CC}	L _{CC}	CC	‘00’
		‘81’	L _c	Pole dat	‘97’	‘01’	L _e	‘8E’	‘04’	CC	

Data, která mají být zahrnuta do kontrolního součtu

= CH || PB || T_{PV} || L_{PV} || PV || T_{LE} || L_{LE} || L_e || PB.

PB = doplňkové byty (80 .. 00) podle ISO/IEC 7816-4 a ISO 9797 metoda 1.

PV a LE z DO jsou přítomny pouze tehdy, pokud jsou odpovídající data umístěna v nezabezpečeném povelu.

Zabezpečená odezva:

1. Případ, kdy pole dat odezvy není prázdné a nepotřebuje být chráněno na důvěrnost:

Těleso odezvy						Znak odezvy
(Nové pole dat)						Nové SW1 SW2
T_{PV}	L_{PV}	PV	T_{CC}	L_{CC}	CC	
'81'	L_r	Pole dat	'8E'	'04'	CC	

Data zahrnutá do kontrolního součtu = T_{PV} || L_{PV} || PV || PB.

2. Případ, kdy pole dat odezvy není prázdné a potřebuje být chráněno na důvěrnost:

Těleso odezvy						Znak odezvy
(Nové pole dat)						Nové SW1 SW2
$T_{PI\ CG}$	$L_{PI\ CG}$	PI CG	T_{CC}	L_{CC}	CC	
'87'		PI CG	'8E'	'04'	CC	

Data v CG: nekódovaná data BER-TLV a doplňkové byty.

Data zahrnutá do kontrolního součtu = $T_{PI\ CG}$ || $L_{PI\ CG}$ || PI CG || PB.

3. Příklad, kdy je pole dat odezvy prázdné:

Těleso odezvy						Znak odezvy
(Nové pole dat)						Nové SW1 SW2
T _{SW}	L _{SW}	SW	T _{CC}	L _{CC}	CC	
'99'	'02'	Nové SW1 SW2	'8E'	'04'	CC	

Data zahrnutá do kontrolního součtu = T_{SW} || L_{SW} || SW || PB.

5.2 Zacházení se závadami v secure messaging (bezpečné zpracování zpráv)

CSM_026 Pokud karta tachografu při převodu příkazu zjistí závadu SM, musí být stavové byty vráceny bez SM. Podle ISO/IEC 7816-4 jsou pro závadu na SM definovány následující byty:

- '66 88' selhalo ověření šifrovacího kontrolního součtu,
- '69 87' chybí očekávané objekty dat SM,
- '69 88' objekty SM dat nesprávné.

CSM_027 pokud karta tachografu vrátí stavové byty bez SM DO nebo se závadným SM DO, musí celek ve vozidle relaci přerušit.

5.3 Algoritmus k výpočtu šifrovacího kontrolního součtu

CSM_028 šifrovací kontrolní součty jsou tvořeny užitím obvyklého MAC podle ANSI X.9.19 s DES:

- výchozí stav: výchozím zkušebním blokem y₀ je E(K_a, SSC),
- následující krok: užitím K_a se vypočtou zkušební bloky y₁, ..., y_n,
- konečný krok: šifrovací kontrolní součet se vypočte z posledního zkušebního bloku y_n takto: E(K_a, D(K_b, y_n)),

kde E() znamená šifrování s DES a D() znamená odšifrování s DES.

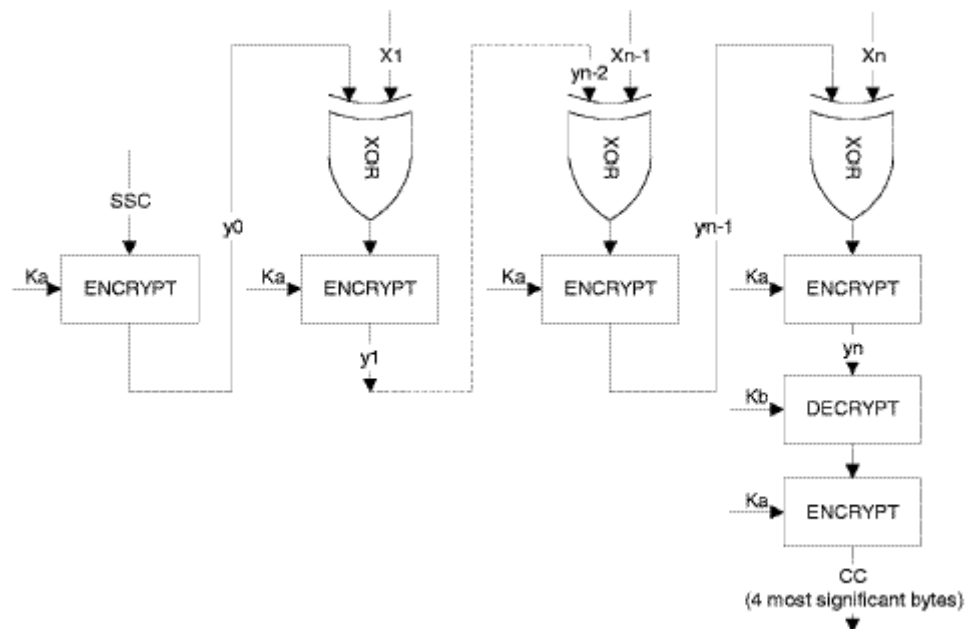
Čtyři byty s nejvyšší hodnotou šifrovacího kontrolního součtu se přenášejí.

CSM_029 v průběhu odsouhlasení klíče se „send sequence counter“ (SSC) (čítač odeslané posloupnosti) inicializuje takto:

výchozí SSC: Rnd3 (4 byty s nejnižší hodnotou) || Rnd 1 (4 byty s nejnižší hodnotou).

CSM_030 na čítači odeslané posloupnosti se hodnota zvýší o 1 před každým výpočtem MAC (tj. SSC pro první povel je výchozí SSC + 1, SSC pro prvou odezvu je výchozí SSC + 2).

Následující vyobrazení uvádí výpočet MAC:



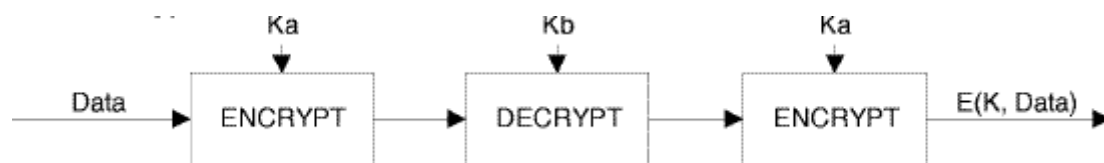
(4 most significant bytes) = 4 byty s nejvyšší hodnotou

5.4 Algoritmus výpočtu šifer pro důvěrnost DOs

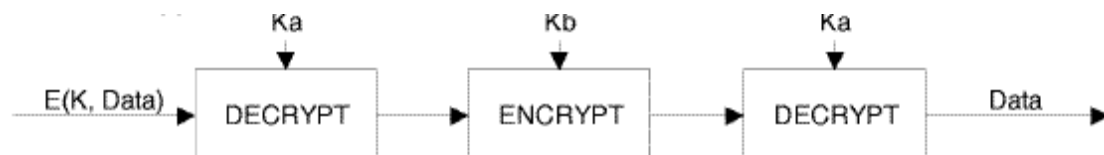
CMS_031 šifry se vypočtou užitím TDEA v módu TCBC podle odkazu (TDES) a (TDES-OP) spolu s nulovým vektorem jako výchozí bloku hodnot.

Následující vyobrazení uvádí využití klíčů v TDES:

Šifrování TDES



Dešifrování TDES



6. mechanizmy digitálních podpisů při stahování dat

CSM_032 Intelligent Dedicated Equipment (IDE) (přiřazené inteligentní zařízení) ukládá data ze zařízení (VU nebo karta) v průběhu relace stahování do jednoho fyzického souboru dat. Tento soubor musí zahrnovat certifikáty MSi.C a EQT.C Soubor obsahuje podpisy datových bloků podle ustanovení doplňku 7 - Protokoly o stahování dat.

CSM_033 Digitální podpisy stažených dat musí užívat schéma digitálního podpisu s dodatkem tak, aby stažená data mohla být v případě požadavku čtena bez jakéhokoliv dešifrování.

6.1 Generace podpisu

CSM_034 generace dat podpisu zařízením probíhá podle schématu podpisu definovaném v odkazu PKCS1 s dodatkem a s transformační funkcí SHA-1:

$$\text{Podpis} = \text{EQT.SK}[\text{'00'} || \text{'01'} || \text{PS} || \text{'00'} || \text{DER}(\text{SHA-1}(\text{Data}))]$$

PS = doplňkový řetězec oktetů s hodnotou 'F' takový, aby délka byla 128.

DER(SHA-1(M)) je kódováním algoritmu ID pro transformační funkci a hodnotou transformace ASN.1 typu *DigestInfo* (pravidla kódování):

'30' || '21' || '30' || '09' || '06' || '05' || '2B' || '0E' || '03' || '02' || '1A' || '05' || '00' || '04' || '14' || Transformační hodnota.

6.2 Ověření podpisu

CSM_035 Ověření dat podpisu stažených dat probíhá podle schématu podpisu definovaném v odkazu PKCS1 s dodatkem a s transformační funkcí SHA-1.

Evropský klíč EUR.PK musí být ověřujícímu znám z nezávislé (a důvěryhodné) strany.

Následující tabulka zobrazuje protokol, podle kterého může IDE s kontrolní kartou ověřit úplnost stažených dat a uložených na ESM (externí paměťové medium). Pro dešifrování digitálních podpisů se užije kontrolní karta. Tato funkce nemá být v tomto případě zahrnuta do IDE.

Zařízení, které data převedlo a podepsalo se označí jako EQT.

