32002R1360

NAŘÍZENÍ KOMISE (ES) č. 1360/2002

ze dne 13. června 2002,

kterým se posedmé přizpůsobuje technickému pokroku nařízení Rady (EHS) č. 3821/85 o záznamovém zařízení v silniční dopravě

(Text s významem pro EHP)

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 dopravě ([1]), naposledy pozměněné nařízením (ES) č. 2135/98 ([2]), a zejména na článek 17 a 18 uvedeného nařízení,

vzhledem k těmto důvodům:

(1) Technická ustanovení přílohy IB nařízení (EHS) č. 3821/85 by se měla přizpůsobit technickému pokroku se zvláštní pozorností na všeobecnou bezpečnost systému a na možnost vzájemné spolupráce mezi záznamovým zařízením a kartami řidiče.

(2) Přizpůsobení zařízení také vyžaduje přizpůsobení přílohy II nařízení (EHS) č. 3821/85, která definuje značky a certifikáty schválení typu.

(3) Výbor zřízený článkem 18 nařízení (EHS) č. 3821/85 nezaujal k opatřením podle návrhu stanovisko a proto Komise předložila Radě návrh vztahující se k těmto opatřením.

(4) Rada se ve lhůtě stanovené v čl. 18 odst. 5 písm. b) nařízení (EHS) č. 3821/85 neusnesla, a je proto na Komisi, aby opatření přijala,

PŘIJALA TOTO NAŘÍZENÍ:

Článek 1

Příloha nařízení (ES) č. 2135/98 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:
   — rozlišovací označení Řecka „GR“ se nahrazuje označením „23“,
   — rozlišovací označení Irska „IRL“ se nahrazuje označením „24“,
   — doplňuje se rozlišovací označení „12“ pro Rakousko,
   — doplňuje se rozlišovací označení „17“ pro Finsko,
   — doplňuje se rozlišovací označení „5“ pro Švédsko.
2. Kapitola I bod 1 druhý pododstavec se mění takto:
   — za slova „záznamového listu“ se vkládají slova „nebo karty tachografu“.
3. Kapitola I bod 2 se mění takto:
   — za slova „záznamový list“ se vkládají slova „a na každou kartu tachografu“.
4. V kapitole II se nadpisu nahrazuje tímto „CERTIFIKÁT SCHVÁLENÍ TYPU PRO VÝROBKY ODPOVÍDAJÍCÍ PŘÍLOZE I“.

([1]) Úř. věst. L 370, 31.12.1985, s. 8.
([2]) Úř. věst. L 274, 9.10.1998, s. 1.

5. Doplňuje se nová kapitola, která zní:

„III. CERTIFIKÁT SCHVÁLENÍ TYPU PRO VÝROBKY, KTERÉ ODPOVÍDAJÍ PŘÍLOZE IB

Stát po schválení typu vystavuje žadateli certifikát schválení typu podle dále uvedeného vzoru. Při informování ostatních členských států o vydaných schváleních nebo o případném odebrání schválení typu používá každý členský stát kopie tohoto certifikátu.

CERTIFIKÁT SCHVÁLENÍ TYPU PRO VÝROBKY ODPOVÍDAJÍCÍ PŘÍLOZE IB

Název příslušného správního orgánu: . . . . . .

Oznámení, týkající se ([3]):

☐ schválení typu

☐ odebrání schválení typu

☐ typu záznamového zařízení

☐ součásti záznamového zařízení ([4]) . . . . . .

☐ karty řidiče

☐ karty dílny

☐ karty podniku

☐ karty kontrolora

Schválení typu č.: . . . . . .

1. Výrobní nebo obchodní značka: . . . . . .
2. Označení typu: . . . . . .
3. Jméno výrobce: . . . . . .
4. Adresa výrobce: . . . . . .
5. Předloženo ke schválení typu dne: . . . . . .
6. Zkušební laboratoř (laboratoře): . . . . . .
7. Datum a číslo zkoušky (zkoušek): . . . . . .
8. Datum schválení typu: . . . . . .
9. Datum odebrání schválení typu: . . . . . .
10. Typ součástí záznamového zařízení, pro jejichž užití je součást konstruována: . . . . . .
11. Místo: . . . . . .
12. Datum: . . . . . .
13. Přiložená dokumentace: . . . . . .

14. Poznámky (včetně umístění případných plomb)

. . . . . .

(Podpis)

([3]) Zaškrtněte příslušné rámečky.
([4]) Uveďte součást, které se oznámení týká.“

Článek 3

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

Toto nařízení je závazné v celém rozsahu a přímo použitelné ve všech členských státech.

V Bruselu dne 13. června 2002.

Za Komisi
Loyola DE PALACIO
místopředsedkyně

PŘÍLOHA

„PŘÍLOHA IB

POŽADAVKY NA KONSTRUKCI, ZKOUŠENÍ, INSTALOVÁNÍ A INSPEKCI

OBSAH

I. DEFINICE

V této příloze se:

a) ‚**aktivací**' rozumí:

fáze, ve které se záznamové zařízení stává plně funkčním a ve které provádí veškeré funkce, včetně funkcí bezpečnostních;

aktivace záznamového zařízení vyžaduje užití karty dílky a vložení PIN kódu;

b) ‚**prokázáním totožnosti**' rozumí:

funkce, určená ke stanovení a ověření uváděné identity;

c) ‚**totožností**' rozumí:

vlastnost, že informace přichází ze strany, jejíž identitu je možno ověřit;

d) ‚**vestavěnou zkouškou**' rozumí:

zkouška, která proběhne na vyžádání, spouštěná obsluhou nebo externím zařízením;

e) ‚**kalendářním dnem**' rozumí:

den v době od 00.00 hod. do 24.00 hod. Veškeré kalendářní dny se vztahují k času UTC (koordinovaný světový čas);

f) ‚**kalibrací**' rozumí:

obnovení nebo potvrzení parametrů vozidla, které je třeba podržet v paměti údajů. Parametry vozidla zahrnují identifikaci vozidla (identifikační číslo vozidla, registrační číslo vozidla a členský stát registrace) a vlastnosti vozidla (w, k, l, rozměr pneumatik, nastavení omezovače rychlosti (pokud připadá v úvahu), současný čas UTC, současný údaj měřiče ujeté vzdálenosti);

kalibrace záznamového zařízení vyžaduje kartu dílny;

g) ‚**číslem karty**' rozumí:

šestnáctimístné alfanumerické označení, které v členském státu jednoznačně identifikuje kartu tachografu. Číslo karty zahrnuje (popřípadě) pořadový index, index náhrady a index obnovy;

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

h) ‚**pořadovým indexem karty**' rozumí:

čtrnáctimístné alfanumerické označení v čísle karty, které je užito pro rozlišení různých karet vydaných určitému podniku nebo subjektu, které mají právo na vydání více karet tachografu. Podnik nebo subjekt jsou jednoznačně identifikovány prvními třinácti znaky čísla karty;

i) ‚**indexem obnovy karty**' rozumí:

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

j) ‚**indexem náhrady karty**' rozumí:

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

k) ‚**charakteristickým koeficientem vozidla**' 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 bod 5). Charakteristický koeficient se vyjadřuje v počtu impulsů na kilometr (w = … imp/km);

l) ‚**kartou podniku**‘ rozumí:

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

karta podniku identifikuje podnik a umožňuje zobrazování a výtisk údajů uložených v záznamovém zařízení, které bylo tímto společností uzamčeno;

m) ‚**konstantou záznamového zařízení**‘ 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 = … imp/km);

n) ‚**nepřetržitá doba jízdy**‘ se vypočítává v záznamovém zařízení jako ([1]):

nepřetržitá doba jízdy, která se vypočítává jako běžná součtová doba jízdy určitého řidiče od konce jeho poslední POHOTOVOSTI nebo PŘESTÁVKY/ODPOČINKU nebo NEZNÁMÉ ([2]) doby 45 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 činnosti uložené na kartě řidiče. Pokud řidič nevložil svou 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;

o) ‚**kontrolní kartou**‘ rozumí:

karta tachografu, vydaná orgány členského státu příslušnému kontrolnímu orgánu;

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

p) ‚**souhrnnou dobou přestávek**‘ vypočítávanou v rámci záznamového zařízení rozumí **([1])**:

souhrnná doba přestávek v jízdě se vypočítá z běžných shromážděných dob POHOTOVOSTI nebo PŘESTÁVKA/ODPOČINEK nebo NEZNÁMÉ ([2]), které jsou dlouhé 45 min nebo delší (toto období může být rozděleno na několik období dlouhých 15 min nebo delších.)

Příslušné výpočty berou podle potřeby v úvahu minulé činnosti 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 svou 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;

q) ‚**pamětí údajů**‘ rozumí:

elektronické zařízení na ukládání údajů, které je vestavěné v záznamovém zařízení;

r) ‚**digitálním podpisem**‘ rozumí:

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

s) ‚**stahováním**‘ rozumí:

kopírování (spolu s digitálním podpisem) části dat nebo úplné sady dat, uložených v paměti údajů vozidla nebo v paměti karty tachografu;

stahování nemá měnit nebo vymazat jakékoliv uložené údaje;

([1]) Tento způsob výpočtu nepřetržité doby jízdy a kumulativní doby přestávek slouží v záznamovém zařízení pro výpočet varování o nepřetržité době jízdy. To však nenahrazuje právní výklad, který je třeba použít na tyto doby.

([2]) NEZNÁMÁ doba odpovídá období, kdy není do záznamového zařízení vložena karta řidiče a po které nebyl z řidičovy aktivity vložen ručně žádný údaj.

t) ‚**kartou řidiče**' rozumí:

karta tachografu, vystavená orgány členského státu určitému řidiči;

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

u) ‚**efektivním obvodem pneumatik kol**' rozumí:

průměrná vzdálenost ujetá každým z kol poháněných vozidlo (poháněná kola) v průběhu jedné ukončené otáčky. Tyto vzdálenosti jsou měřeny za normálních zkušebních podmínek (kapitola VI odst. 5) a vyjadřují se ve tvaru: l = … mm. Výrobci vozidla mohou měření těchto vzdáleností nahradit teoretickým výpočtem, který bere v úvahu rozložení hmotností na nápravy pro nenaložené vozidlo v provozním stavu ([1]). Postupy pro tyto teoretické výpočty schválí příslušný orgán členského státu.

v) ‚**událostí**' rozumí:

mimořádná činnost zjištěná záznamovým zařízením, která může pocházet z pokusu o podvod;

w) ‚**závadou**' rozumí:

mimořádná činnost zjištěná záznamovým zařízením, která může pocházet z chybné funkce nebo z poruchy zařízení;

x) ‚**instalací**' rozumí:

montáž záznamového zařízení do vozidla;

y) ‚**snímačem pohybu**' rozumí:

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

z) ‚**neplatnou kartou**' 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 uplynulo datum platnosti;

aa) ‚**mimo působnost**' rozumí:

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

bb) ‚**překročením rychlosti**' rozumí:

překročení povolené rychlosti vozidla, které je definováno jako jakékoliv období delší než 60 s, ve kterém měřená rychlost vozidla překračuje mezní hodnotu nastavení omezovače rychlosti, která bylo stanovena směrnicí Rady 92/6/EHS ze dne 10. února 1992 o montáži a použití omezovačů rychlosti u určitých kategorií motorových vozidel ve Společenství ([2]);

cc) ‚**pravidelnou kontrolou**' rozumí:

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

dd) ‚**tiskárnou**' rozumí:

součást záznamového zařízení, které zajišťuje vytištění uložených údajů;

ee) ‚**záznamovým zařízením**' 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;

([1]) Směrnice Evropského parlamentu a Rady 97/27/ES ze dne 22. července 1997 o hmotnostech a rozměrech určitých kategorií motorových vozidel a jejich přípojných vozidel a o změně směrnice 70/156/EHS (Úř. věst. L 233, 25.8.1997, s. 1).

([2]) Úř. věst. L 57, 2.3.1992, s. 27.

ff) ‚**obnovením**‘ rozumí:

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

gg) ‚**opravením**‘ rozumí:

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

hh) ‚**náhradou**‘ 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**‘ rozumí:

postup, kterým osvědčuje certifikační orgán ITSEC ([1]), že zkoumané záznamové zařízení (nebo jeho součást) nebo karta tachografu plní bezpečnostní požadavky stanovené v dodatku 10 Všeobecné požadavky na bezpečnost;

jj) ‚**autotestem**‘ rozumí:

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

kk) ‚**kartou tachografu**‘ rozumí:

čipová 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,

— karta dílny,

— karta podniku;

ll) ‚**schvalováním typu**‘ rozumí:

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

mm) ‚**rozměrem pneumatiky**‘ rozumí:

stanovení rozměrů pneumatik (vnějších hnacích kol) podle směrnice 92/23/EHS ze dne 31. března 1992 ([2]);

nn) ‚**identifikací vozidla**‘ rozumí:

čísla, která vozidlo identifikují: registrační číslo vozidla s uvedením členského státu registrace a identifikační číslo vozidla ([3]);

oo) ‚**celkem ve vozidle**‘ 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;

([1]) Doporučení Rady 95/144/ES ze dne 7. dubna 1995 o obecných kritériích pro hodnocení bezpečnosti informačních technologií (Úř. věst. L 93, 26.4.1995, s. 27).

([2]) Úř. věst. L 129, 14.5.1992, s. 95.

([3]) 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 (Úř. věst. L 24, 30.1.1976, s. 1).

pp) ‚**týdnem**' se pro spolehlivost výpočtu v záznamovém zařízení rozumí:

období od 00.00 hodin času UTC v pondělí do 24.00 hodin času UTC v neděli;

qq) ‚**kartou dílny**' rozumí:

karta tachografu, vydaná orgány členského státu výrobci záznamového zařízení, montážnímu podniku, výrobci vozidla nebo dílně schválené členským státem;

karta dílny identifikuje držitele karty a umožňuje zkoušení, kalibraci nebo stahování údajů v záznamovém zařízení.

II. OBECNÉ VLASTNOSTI A FUNKCE ZÁZNAMOVÉHO ZAŘÍZENÍ

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

1. **Obecné vlastnosti**

Účelem záznamového zařízení je zaznamenávat, ukládat, zobrazovat a tisknout údaje týkající se činností řidiče a umožnit jejich výstup.

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

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

Záznamové zařízení může být propojeno s dalšími zařízením 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 k datům a funkcím v závislosti na typu nebo identitě uživatele.

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

Toto se děje v souladu se směrnicí 95/46/ES ze 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů ([1]).

2. **Funkce**

005 Záznamové zařízení musí zajistit následující funkce:

— monitorování jednotlivých vložení a vyjmutí karty,

— měření rychlosti a ujeté vzdálenosti,

— měření času,

— monitorování činnosti řidiče,

— monitorování provozního stavu,

— údaje vkládané řidičem ručně:

  — vložení místa kde pracovního doba dne začíná nebo končí,

  — ručně vkládané údaje o činnostech řidiče,

  — záznam zvláštních podmínek,

([1]) Úř. věst. L 281, 23.11.1995, s. 31.

— využívání možnosti zámků podniků,

— monitorování kontrolních činností,

— zjišťování událostí a závad,

— vestavěné zkoušky a autotesty,

— načítání z paměti údajů,

— zaznamenávání a ukládání do paměti údajů,

— načítání z karet tachografu,

— zaznamenávání a ukládání dat na karty tachografu,

— zobrazování údajů,

— tisk,

— dávání výstrahy,

— stahování dat na externí média,

— výstup dat na přídavná externí zařízení,

— kalibraci,

— nastavení času.

3. **Provozní režimy**

006 Záznamové zařízení musí být schopno pracovat ve čtyřech režimech:

— provozní režim,

— kontrolní režim,

— kalibrační režim,

— podnikový režim.

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	Karta dílny	Karta podniku
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
	Karta dílny	Kalibrační	Kalibrační	Provozní	Kalibrační (*)	Provozní
	Karta podniku	Podnikový	Podnikový	Provozní	Provozní	Podnikový (*)

008 (*) V těchto situacích používá záznamové zařízení pouze kartu tachografu vloženou do řidičova otvoru pro vložení karty.

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 zámků podniků 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 uvedenou v požadavku 150).

011 Záznamové zařízení může předat data na displej, 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, ignorovány a jakékoliv číslo karty neodpovídající vložené kartě tachografu je částečně ignorováno (každý lichý znak odleva doprava chybí),

— 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 jiným podnikem (jak je označeno prvními 13 místy číselného kódu karty podniku),

— pokud není v záznamovém zařízené vložena žádná karta, údaje vztahující se k osobě řidiče jsou k dispozici pouze pro aktuální den a osm předcházejících dnů.

4. **Bezpečnost**

Bezpečnost systému sleduje ochranu paměti údajů záznamového zařízení takovým způsobem, aby se zabránilo neoprávněnému přístupu, manipulaci s daty a odhalení takového pokusu, stejně jako úplnost a totožnost 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 uvedené ve Všeobecných požadavcích na bezpečnost snímačů pohybu a celku ve vozidle (dodatek 10).

III. KONSTRUKČNÍ A FUNKČNÍ POŽADAVKY NA ZÁZNAMOVÉ ZAŘÍZENÍ

1. **Monitorování jednotlivých vložení a vyjmutí karty**

013 Záznamové zařízení monitoruje vkládání karty do čtecího zařízení karet a její vyjímání.

014 Při vložení karty ověřuje 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 po správném vložení do rozhraní zamčeny ve správné poloze.

016 K uvolnění karet tachografu může dojít pouze po zastavení vozidla a příslušná data jsou uložena na kartách. Uvolnění karty vyžaduje aktivní zásah uživatele.

2. **Měření rychlosti a vzdálenosti**

017 Tato funkce měří nepřetržitě a musí být schopna dodávat hodnoty ujeté vzdálenosti 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 více než 1 imp/sec po dobu nejméně pěti vteřin. 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 body 2.1 a 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 9 999 999,9km.

022 Měření vzdálenosti se pohybuje v následujících tolerancích (vzdálenosti nejméně 1 000 m):

— ± 1 % před instalací,

— ± 2 % při instalaci a pravidelné kontrole,

— ± 4 % v provozu.

023 Vzdálenost se měří s rozlišením 0,1 km nebo jemnějším.

2.2 ***Měření rychlosti***

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

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

— tolerance ± 2 km/hod u vstupních změn (proměnlivost pneumatik, …),

— tolerance ± 1 km/hod při měřeních provedených při instalaci a pravidelných kontrolách,

musí záznamové zařízení pro rychlosti ležící v rozmezí 20 až 180 km/hod a pro charakteristické koeficienty vozidla mezi 4 000 až 25 000 imp/hod měřit rychlost s tolerancí ± 1 km/hod (při konstantní rychlosti).

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

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

026 Měření rychlosti se provádí s rozlišením 1 km/hod nebo jemnějším.

3. **Měření času**

027 Funkce měření času musí měřit nepřetržitě a udávat v digitální podobě údaje o referenčním datu a času UTC.

028 Datum a čas UTC se použije pro průběžné datování záznamového zařízení (záznamy, výtisky, výměny dat, zobrazení, …).

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

030 Zpožďování 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 vnějšího elektrického napájení na dobu kratší nežli 12 měsíců v podmínkách schvalování typu.

4. **Monitorování činnosti řidiče**

033 Tato funkce musí nepřetržitě a odděleně monitorovat činnost jednoho řidiče a jednoho druhého řidiče.

034 Řidičovy činnosti jsou JÍZDA, PRÁCE, POHOTOVOST a PŘESTÁVKA/ODPOČINEK.

035 Mělo by být umožněno řidiči nebo druhému řidiči ručně navolit režimy PRÁCE, POHOTOVOST a PŘESTÁVKA/ODPOČINEK.

036 Jestliže se vozidlo pohybuje, musí se nastavit automaticky JÍZDA pro řidiče a u druhého řidiče se musí automaticky nastavit POHOTOVOST.

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 nastalé 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, je celá minuta považována za JÍZDU.

041 Pokud se v dané kalendářní minutě objeví jakákoliv činnost v režimu JÍZDA, jak v přímo předcházející, tak v přímo následující minutě, je celá tato minuta považována za JÍZDU.

042 Pokud jde o danou kalendářní minutu, která není podle předcházejících kriterií považována za JÍZDU, je celá minuta považována za stejný typ činnosti, jako nejdéle nepřetržitě trvající činnost v této minutě (nebo poslední ze stejně dlouho trvajících činností).

043 Tato funkce musí také nepřetržitě monitorovat nepřetržitý čas jízdy a načítaný čas doby přestávek řidiče.

5. **Monitorování stavu řízení vozidla**

044 Tato funkce musí nepřetržitě a automaticky monitorovat stav řízení vozidla.

045 Stav řízení vozidla POSÁDKA se musí navolit, jestliže jsou v záznamovém zařízení vloženy dvě platné karty řidiče. V každém jiném případě se navolí stav řízení vozidla SAMOTNÝ ŘIDIČ.

6. **Řidičem ručně vkládané údaje**

6.1 ***Vložení údaje o místě počátku nebo ukončení denní práce***

046 Tato funkce musí umožnit vložení údaje o počátku nebo ukončení denní práce řidiče nebo druhého řidiče.

047 Místa jsou definována jako stát a případně region.

048 V době vyjmutí karty řidiče (nebo karty dílny) 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 umožněno vložit místo začátku nebo ukončení doby denní práce bez karty nebo v jiné době nežli při vlastním vkládání nebo vyjímání karty.

6.2 ***Ruční vkládání údajů o činnostech řidiče***

050a V době vkládání karty řidiče (nebo karty dílny) 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 ponechat bez odpovědi, odpovědět kladně nebo odpovědět záporně.

— v případě, kdy držitel karty ignoroval otázku a neodpověděl, vyžádá záznamové zařízení na držiteli karty zadání ‚místa počátku doby denní práce'. Záznamové zařízení umožní ignorování tohoto požadavku. Pokud je místo vloženo, je zaznamenáno do paměti údajů, do karty tachografu a vztaženo k době vložení karty.

— v případě záporné nebo kladné odpovědi záznamové zařízení vyzve držitele karty, aby zvolil ručně typ činnosti, pouze z možností PRÁCE, POHOTOVOST nebo PŘESTÁVKA/ODPOČINEK, včetně času začátku a ukončení. Tyto údaje musí striktně odpovídat době mezi posledním vyjmutím karty a opětovným vložením, aniž by se činnosti překrývaly. Toto musí být provedeno tímto postupem:

  — v případě kladné odpovědi držitele karty na otázku záznamové zařízení vyzve držitele karty k ručnímu vložení činností v chronologickém pořadí pro dobu mezi posledním vyjmutím a současným vložením karty. Postup je ukončen v okamžiku, kdy se ručně vložený čas ukončení shoduje s časem vložení karty.

  — v případě záporné odpovědi držitele karty musí záznamové zařízení:

    — vyzvat držitele karty k ručnímu vložení činností v chronologickém pořadí 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 poznámku).

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

      — předpokládat, že doba denní práce skončila v době začátku prvního ODPOČINKU (nebo zbývajícího času NEZNÁMÝ) po vyjmutí karty nebo době vyjmutí karty, jestliže žádná doba odpočinku nebyla vyznačena (a jestliže nezbývá žádný čas NEZNÁMÝ),

      — předpokládat, že počáteční čas (viz níže) se rovná době vložení karty,

      — postupovat podle níže uvedených kroků;

    — dále, 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, je 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,

    — dále vyzve držitele karty k ‚zadání času začátku' 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 údaj o místu vložen, je zaznamenán na kartu tachografu a vztažen k časovému údaji začátku. Pokud je tento počáteční časový údaj shodný s časem vložení karty, je údaj o místě zaznamenán také do paměti údajů,

    — dále, jestliže se časový údaj začátku liší od doby vložení karty, vyzve držitele karty k ručnímu vložení činností v chronologickém pořadí od tohoto času začátku až do okamžiku vložení karty,

  — záznamové zařízení potom umožní držiteli karty pozměňovat údaj jakékoliv činnosti ručně vložené až do potvrzení volbou zvláštního příkazu, a potom již nedovolí žádné podobné úpravy,

  — takové odpovědi na počáteční otázku, po kterých nenásleduje žádné vložení činnosti, považuje záznamové zařízení za ignorování otázky držitelem karty.

V průběhu celého postupu záznamové zařízení čeká 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 nebo je vložena karta jiného řidiče (nebo karta dílny) nebo,

— jestliže se vozidlo dá do pohybu,

a 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 PŮSOBNOST' (začátek, konec);

— ‚PŘEVOZ LODÍ / PŘEVOZ VLAKEM'

Záznam ‚PŘEVOZ LODÍ / PŘEVOZ VLAKEM' se nesmí objevit, pokud je aktivovaný údaj ‚MIMO PŮSOBNOST'.

Otevřená podmínka ‚MIMO PŮSOBNOST' musí být záznamovým zařízením automaticky uzavřena při vložení nebo vyjmutí karty řidiče.

7. **Ovládání funkce zámků podniků**

051 Tato funkce umožňuje správu zámků podnikem k omezení přístupu k údajům v podnikovém režimu pouze pro tento podnik.

052 Zámky podniků spočívají ve vložení data a času (uzamčení podnikem) a data a času (odemknutí podnikem) spojeného s identifikací podniku číslem karty podniku (při uzamčení).

053 Uzamčení a odemknutí zámků podniků může být provedeno pouze v reálném čase.

054 Zámek může odemknout pouze podnik, který zámek uzamkl (identifikováno prvními 13 znaky v čísle karty podniku) nebo,

055 odemknutí se provede automaticky při uzamčení jiným podnikem.

055a V případě, že podnik provede uzamčení a předcházející uzamčení provedl táý podnik, předpokládá se, že předcházející uzamčení 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 nebo data ‚události a závady' jsou stahována z paměti údajů celku ve vozidle.

9. **Detekce událostí nebo závad**

058 Tato funkce identifikuje následující události nebo závady:

9.1 ***Vložení neplatné karty***

059 Tato událost se vyvolá vložením neplatné karty nebo karty s prošlým datem.

9.2 ***Rozpor karet***

060 Tato událost nastane, jestliže se vložením platných karet dosáhne kombinace označená v tabulce X:

Vložení neodpovídající karty		Otvor pro vložení karty řidiče				
		Bez karty	Karta řidiče	Kontrolní karta	Karta dílny	Karta podniku
Otvor pro vložení karty druhého řidiče	Bez karty					
	Karta řidiče				X	
	Kontrolní karta			X	X	X
	Karta dílny		X	X	X	X
	Karta podniku			X	X	X

9.3 ***Překrytí časových údajů***

061 Tato událost nastane, jestliže datum a čas posledního vyjmutí karty řidiče, které je přečteno na kartě je pozdější nežli aktuální datum a čas záznamového zařízení, do kterého je karta vložena.

9.4 ***Jízda bez náležité karty***

062 Tato událost nastane při jakékoliv z kombinací údajů karet tachografu označené v následující tabulce X, když se řidičova činnost mění na režim JÍZDA 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	Karta dílny	Karta podniku
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
	Karta dílny	X	X	X		X
	Karta podniku	X	X	X	X	X

9.5 ***Vložení karty v průběhu jízdy***

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

9.6 ***Nesprávně ukončené poslední vložení karty***

064 Tato událost nastane, jestliže při vložení karty záznamové zařízení zjistí, že přes opatření popsaná dále v kapitole III bodě 1 předcházející vložení karty nebylo správným způsobem ukončeno (karta byla vyjmuta dříve, nežli na ní byla uložena příslušná data). Tato událost se zjišťuje pouze při vložení karty řidiče nebo karty dílny.

9.7 ***Překročení povolené rychlosti***

065 Tato událost nastane při každém překročení povolené rychlosti.

9.8 ***Přerušení elektrického napájení***

066 Tato událost nastane při každém přerušení elektrického napájení snímače pohybu a celku ve vozidle delším nežli 200 milisekund, pokud zařízení není v kalibračním režimu. Prahovou charakteristiku hranice přerušení definuje výrobce. Pokles elektrického napájení v důsledku startování motoru vozidla nesmí být označen za tuto událost.

9.9 ***Chybné údaje o pohybu vozidla***

067 Tato událost nastane v případě přerušení normálního toku dat mezi snímačem pohybu a celkem ve vozidle nebo v případě chyby v úplnosti nebo totožnosti dat přenášených mezi snímačem pohybu a celkem ve vozidle.

9.10 ***Pokus o narušení bezpečnosti systému***

068 Tato událost nastane v jakémkoliv jiném případě, který ohrožuje bezpečnost systému snímače pohybu nebo celku ve vozidle v oblasti všeobecných bezpečnostních požadavků těchto komponentů, pokud není zařízení v kalibračním režimu.

9.11 ***Chybná karta***

069 Tato závada nastane, kdykoliv je v průběhu provozu zjištěna závada karty tachografu.

9.12 ***Chyba záznamového zařízení***

070 Tato závada nastane, pokud zařízení není v kalibračním režimu, v případě jakékoliv následující závady:

— vnitřní závada celku ve vozidle,

— závada tiskárny,

— závada zobrazovací jednotky,

— závada 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:

Testovaný subsystém	Autotest	Vestavěná zkouška
Programové vybavení		Úplnost
Paměť údajů	Přístup	Přístup, úplnost údajů
Čtení karet	Přístup	Přístup
Klávesnice		Ruční kontrola
Tiskárna	(podle výrobce)	Výtisk
Zobrazovací jednotka		Vizuální kontrola
Stahování údajů (prováděné pouze v průběhu stahování)	Správná funkce	
Snímač	Správná funkce	Správná funkce

11 **Načítání z paměti údajů**

072 Záznamové zařízení musí být schopno načíst jakékoliv údaje uložené v jeho paměti údajů.

12. **Zaznamenávání a ukládání do paměti údajů**

Pro účely tohoto odstavce

— se ‚365 dny' rozumí 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 dnů tedy obsahuje minimálně 2 190 (druhých) řidičů, 2 190 cyklů vložení a vyjmutí karty a 93 440 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 údaje o celku ve vozidle*

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

— jméno výrobce,

— adresa výrobce,

— číslo součásti,

— výrobní číslo,

— číslo verze programového vybavení,

— datum instalace aktuální verze programového vybavení,

— rok výroby zařízení,

— číslo schválení typu.

076 Identifikační údaje o celku ve vozidle jsou zaznamenány a uloženy jednou provždy výrobcem celku ve vozidle, s výjimkou údajů vztahujících se k programovému vybavení a číslo schválení typu, které se může měnit v případě aktualizace programového vybavení.

12.1.2 *Identifikační data snímače pohybu*

077 Snímač pohybu musí být schopen uložit do své paměti údajů 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 programového vybavení).

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 údajů 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,

— ukromý klíč zařízení.

Bezpečnostní prvky záznamového zařízení jsou vloženy do zařízení výrobcem celku ve vozidle.

12.3 ***Data související s vložením a vyjmutím karty řidiče***

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

— jméno(a) a příjmení držitele karty v podobě uložené na kartě,

— číslo karty, členský stát vydávající kartu a datum platnosti v podobě uložené 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 nebo ne.

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

083 Jestliže je kapacita paměti údajů vyčerpána, musí nové údaje nahradit nejstarší údaje.

12.4 ***Data o činnosti řidiče***

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

— stav řízení vozidla (POSÁDKA, SAMOTNÝ ŘIDIČ),

— otvor pro vkládání karty (ŘIDIČ, DRUHÝ ŘIDIČ),

— stav karty v příslušném otvoru pro vkládání karet (VLOŽENA, NEVLOŽENA) (viz poznámku),

— činnost (JÍZDA, POHOTOVOST, PRÁCE, PŘESTÁVKA/ ODPOČINEK),

— datum a čas změny.

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

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

12.5 ***Místa, kde začíná nebo končí doba denní práce***

087 Záznamové zařízení musí zaznamenat a uložit do své paměti údajů kdykoliv (druhý) řidič vloží místo začátku 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 a čas vztahující se ke vložení údajů, pokud byly vloženy ručně),

— typ vložených údajů (začátek a konec, podmínky vložení údajů),

— vložený údaj o zemi a regionu,

— hodnotu na měřiči ujeté vzdálenosti.

088 Paměť údajů 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 údajů vyčerpána, musí nová data nahradit nejstarší data.

12.6 ***Údaje měřiče ujeté vzdálenosti***

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

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

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

12.7 ***Podrobná data o rychlosti***

093 Záznamové zařízení musí zaznamenávat a uchovávat ve své paměti údajů 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 bodu je čas zaznamenáván s přesností jedné vteřiny.

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

Událost	Pravidla ukládání dat	Data, která se ukládají při události
Rozpor karet	— 10 posledních událostí	— datum a čas zahájení události, — datum a čas ukončení události, — typ karty, číslo a vydávající členský stát každé karty vyvolávající rozpor.
Jízda bez náležité karty	— nejdelší událost pro každý z posledních 10 dnů, kdy došlo k události, — 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 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 události.	— datum a čas události, — typ karty, číslo a vydávající členský stát, — počet podobných událostí v tomto dni.
Nesprávně ukončené poslední vložení karty	— 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 dnů (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.

Událost	Pravidla ukládání dat	Data, která se ukládají při události
Přerušení 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 nebo na konci události, — počet podobných událostí v tomto dni.
Chybné údaje o pohybu vozidla	— nejdelší událost pro každý z posledních 10 dnech 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 nebo na konci události, — počet podobných událostí v tomto dni.
Pokus o narušení bezpečnosti systému	— 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 nebo při ukončení události, — typ události.

095 ([1]) Záznamové zařízení musí také zaznamenat a uchovat ve své paměti údajů:
— 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.

([2]) Tato data mohou být zaznamenávána pouze při opětném připojení elektrického napájení, časové údaje mohou být udávány s přesností jedné minuty.

12.9 ***Údaje o závadách***

Pro účely tohoto bodu je čas zaznamenáván s přesností jedné vteřiny.

096 Záznamové zařízení se musí pokusit zaznamenat a uložit následující data pro každou zjištěnou závadu do své paměti údajů 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	— 10 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 nebo na konci závady.

12.10 ***Kalibrační údaje***

097 Záznamové zařízení musí zaznamenávat a ukládat do své paměti údajů údaje týkající se:

— známých kalibračních parametrů v okamžiku aktivace,

— jeho první kalibrace po aktivaci,

— první kalibraci v současném vozidle (identifikovaného vlastním identifikačním číslem vozidla),

— pět posledních kalibrací (Jestliže se odehraje několik kalibrací v průběhu jednoho kalendářního dne, je zaznamenána pouze poslední kalibrace).

098 Následující data se zaznamenávají pro každou z těchto kalibrací:

— důvod kalibrace (aktivace, první instalace, instalace, pravidelná kontrola),

— název a adresa dílny,

— číslo karty dílny, 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 údajů 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 údajů 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,

— datu a čas, nová hodnota,

— název a adresa dílny,

— číslo karty dílny, členský stát vydávající kartu a datum skončení platnosti karty.

12.12 ***Data o kontrolní činnosti***

102 Záznamové zařízení musí zaznamenávat a uchovávat ve své paměti údajů následující údaje týkající se posledních 20 případů kontrolní činnosti:

— datum a čas kontroly,

— číslo kontrolní karty a členský stát vydávající kartu,

— typ kontroly (zobrazování nebo tisk nebo stahování dat z celku ve vozidle nebo stahování dat z karty).

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

12.13 ***Data o zámcích podniků***

104 Záznamové zařízení musí zaznamenávat a uchovávat ve své paměti údajů následující údaje, týkající se 20 posledních případů použití zámků podniků:

— datum a čas uzamčení,

— datum a čas odemknutí,

— číslo karty podniku a členský stát vydávající kartu,

— jméno a adresa podniku.

12.14 ***Údaje o stahování dat***

105 Záznamové zařízení musí zaznamenávat a uchovávat ve své paměti údajů údaje týkající se posledního stahování dat z paměti údajů do externího média v podnikovém nebo kalibračním režimu:

— datum a čas stahování dat,

— číslo karty podniku nebo karty dílny a členský stát vydávající kartu,

— jméno podniku nebo dílny.

12.15 ***Údaje o specifických podmínkách***

105a Záznamové zařízení musí zaznamenávat ve své paměti údajů 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 údajů vyčerpána, nová data musí nahrazovat postupně nejstarší data.

13. **Čtení z karet tachografu**

106 Záznamové zařízení musí být schopno, pokud je třeba, přečíst z karet tachografu údaje nezbytné k

— identifikaci typu karty, držitele karty, předcházejícího použitého vozidla, data a času posledního vyjmutí karty a v té době navolené činnosti,

— kontrole řádného ukončení posledního použití karty,

— výpočtu dobu řidičovy nepřetržité jízdy, souhrnné doby přestávek a souhrnné doby jízdy v předchozím a probíhajícím týdnu,

— výtisku požadovaných dat zaznamenaných na kartě řidiče,

— stažení dat z karty řidiče na externí média.

107 V případě chyby načítání dat se záznamové zařízení maximálně třikrát pokusí vyplnit daný příkaz k načtení dat, a pak v případě neúspěchu vyznačí chybu karty nebo její neplatnost.

14. **Zaznamenávání a uchovávání dat na kartě tachografu**

108 Záznamové zařízení musí v kartě řidiče nebo kartě dílny nastavit režim ‚data o použití karty' okamžitě po vložení karty.

109 Záznamové zařízení musí aktualizovat data uložená na platných kartách řidiče nebo kartách dílny a kontrolních kartách o všechna data vztahující se k době, kdy byla karta vložena, a k osobě držitele karty. Údaje uložené na kartách jsou uvedené v kapitole IV.

109a Záznamové zařízení musí aktualizovat údaje o činnostech řidiče a místě (jak je uvedeno v kapitole IV bodech 5.2.5 a 5.2.6), které jsou uloženy na platných kartách řidiče nebo kartách dílny, o data týkající se činností řidiče a míst, která byla ručně vložena držitelem karty.

110 Data uložená na kartách tachografu jsou aktualizována takovým způsobem a v takovou dobu, jak je třeba s ohledem na kapacitu paměti údajů a nahrazení nejdříve uložených dat posledními daty.

111 V případě chybného zápisu se záznamové zařízení maximálně třikrát pokusí vyplnit daný příkaz k zápisu, a pak v případě neúspěchu vyznačí chybu karty nebo její neplatnost.

112 Před uvolněním karty řidiče a po uložení všech příslušných dat, která se měla na kartu uložit, nastaví záznamové zařízení znovu údaje o použití karty.

15. **Zobrazování**

113 Displej musí mít minimálně 20 znaků.

114 Minimální výška znaku musí být 5 mm a šířka 3,5 mm.

114a Zobrazovací jednotka musí podporovat sady znaků latinská abeceda 1 a řecká abeceda definovaná normou ISO 8859, část 1 a 7, jak je uvedeno v dodatku 1 kapitoly 4 ‚Sady znaků'. Zobrazovací jednotka může používat zjednodušené znaky (např. znaky s diakritikou mohou být zobrazeny bez diakritiky 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:

— implicitní údaje,

— údaje vztahující se k výstražným sdělením,

— data vztahující se k přístupovému menu,

— ostatní údaje požadované uživatelem.

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

118 Displej záznamového zařízení musí používat piktogramy nebo kombinace piktogramů uvedených v dodatku 3. Další piktogramy nebo kombinace piktogramů mohou být zobrazeny displejem za předpokladu, že jsou jasně odlišitelné od dříve uvedených piktogramů nebo kombinací piktogramů.

119 Displej musí být vždy zapnut, pokud je vozidlo v pohybu.

120 Záznamové zařízení může obsahovat ruční nebo automatickou možnost vypnutí displeje, pokud se vozidlo nepohybuje.

Formát zobrazení je uveden v dodatku 5.

15.1 ***Implicitní zobrazení***

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

— místní čas (jako výsledek referenčního času UTC + časového posunu nastaveného řidičem),

— provozní režim,

— aktuální činnost řidiče a aktuální činnost druhého řidiče,

— informace vztahující se k řidiči:

— jeho současný čas nepřetržité jízdy a jeho současná souhrnná doba přestávek, pokud je jeho současnou činností JÍZDA,

— aktuální trvání současné činnosti (od doby, kdy byla navolena) a jeho současná souhrnná doba přestávek, pokud jeho současnou činností není JÍZDA,

— 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 implicitně ukazovat informaci týkající se řidiče a musí umožnit uživateli zobrazit informaci týkající se druhého řidiče.

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

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

124a Jestliže je otevřena podmínka ‚MIMO PŮSOBNOST', potom musí displej ukázat odpovídající piktogram, že podmínka je otevřena. (Je povolené, aby zároveň nebyla zobrazena informace o současné 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 zvoleném jazyce.

15.3 ***Přístupové menu***

126 Záznamové zařízení musí nabídnout nezbytné příkazy prostřednictvím odpovídající struktury menu.

15.4 ***Ostatní zobrazované informace***

127 Mělo by být možné zobrazit selektivně podle žádosti:

— referenční datum a čas (UTC),

— provozní režim (pokud není nabízen implicitně),

— nepřetržitá doba jízdy a souhrnná doba přestávek řidiče,

— nepřetržitá doba jízdy a souhrnná doba přestávek druhého řidiče,

— souhrnná doba jízdy řidiče v předchozím a probíhajícím týdnu,

— souhrnná doba jízdy druhého řidiče v předchozím a probíhajícím týdnu,

— obsah kteréhokoliv ze šesti výtisků v témže formátu, jaký má poslední výtisk záznamů.

128 Zobrazování obsahu výtisku musí probíhat sekvenčně, řádku po řádce. Jestliže je šířka displeje menší nežli 24 znaků, musí být uživateli nabídnuta úplná informace vhodným způsobem (několik řádek, rolování…). Řádky výtisku věnované ručně zadaným informacím mohou být ze zobrazení vypuštěny.

16. **Tisk**

129 Záznamové zařízení musí být schopno vytisknout údaje z vlastní paměti údajů nebo karet tachografu v podobě následujících šesti výtisků:

— denní výtisk činnosti řidiče z karty,

— denní výtisk činnosti řidiče z celku ve vozidle,

— výtisk událostí a závad z karty,

— výtisk událostí a závad z celku ve vozidle,

— výtisk technických údajů,

— výtisk překročení povolené rychlosti.

Podrobný popis formátu a obsahu těchto výtisků je uveden v dodatku 4.

Dodatečné údaje mohou být přidány na konci těchto výtisků.

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

130 ‚Denní výtisk činnosti řidiče z karty' a ‚výtisk událostí a závad z karty' musí být k dispozici pouze, pokud je v záznamovém zařízení vložena karta řidiče nebo karta dílny. Záznamové zařízení musí aktualizovat uložená data na příslušné kartě před započetím tisku.

131 Aby se zpřístupnil záznam ‚denní výtisk činnosti řidiče z karty' a ‚výtisk událostí a závad z karty', musí záznamové zařízení:

— buď automaticky vybrat kartu řidiče nebo kartu dílny, pokud je vložena pouze jedna z nich,

— nebo nabídnout příkaz k volbě zdrojové karty nebo zvolit kartu vloženou v otvoru pro vložení karty řidiče, pokud jsou v záznamovém zařízení vloženy tyto dvě karty.

132 Tiskárna musí být schopna vytisknout 24 znaků na řádku.

133 Minimální velikost znaků musí být 2,1 mm na výšku a 1,5 mm na šířku.

133a Tiskárna musí podporovat sady znaků latinská abeceda 1 a řecká abeceda, definované normou ISO 8859, část 1 a 7, jak je popsáno v dodatku 1, kapitola 4 ‚Sady 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 typů záznamových zařízení, ve kterých jej lze používat. Výtisky musí zůstat čitelné nejméně po dobu jednoho roku za normálních podmínek skladování, pokud se týče intenzity osvětlení, vlhkosti a teploty.

137 Na tyto dokumenty by mělo být možné učinit ručně psané poznámky, např. řidičův podpis.

138 Záznamové zařízení by mělo vyřešit v průběhu tisku událost ‚došel papír' tak, že po opětovném vložení papíru je tisk restartován od úplného počátku výtisku nebo tisk pokračuje s jednoznačným odkazem na dříve vytištěnou část.

17. **Výstražná sdělení**

139 Záznamové zařízení musí dát výstražné znamení řidiči při zjištění jakékoliv události nebo závady.

140 Výstražné sdělení při přerušení elektrického napájení může být odloženo až do opětovného připojení elektrického napájení.

141 Záznamové zařízení musí dát řidiči výstražné sdělení 15 minut před uplynutím doby nepřetržité jízdy v trvání 4 hod a 30 min a při jejím překročení.

142 Výstražná sdělení musí být vizuální. Zvukové výstrahy mohou být také použity jako doplněk vizuálních výstražných sdělení.

143 Vizuální výstrahy musí být jasně rozeznatelné uživatelem, musí být umístěny v zorném poli řidiče a musí být jasně čitelné ve dne i v noci.

144 Vizuální výstrahy mohou být zabudovány v záznamovém zařízení nebo umístěny mimo záznamové zařízení.

145 Ve druhém případě musí nést symbol ‚T' a mít žlutou nebo oranžovou barvu.

146 Výstražná sdělení musí trvat nejméně 30 vteřin, pokud není uživatelem potvrzeno, že je bere na vědomí stiskem jakéhokoliv ovládacího prvku záznamového zařízení. První potvrzení nesmí smazat zobrazení příčiny výstražného sdělení v souladu s následujícím odstavcem.

147 Příčina výstrahy musí být zobrazena na záznamovém zařízení a zůstat viditelná, dokud není uživatelem potvrzeno vzetí na vědomí použitím specifického ovladače nebo vložením příkazu záznamového zařízení.

148 Další výstražná sdělení mohou být také použita, pokud nezmatou řidiče ve vztahu ke sdělením výše popsaným.

18. **Stahování dat do externích médií**

149 Záznamové zřízení musí být schopno v případě potřeby stáhnout údaje z paměti údajů nebo z karty řidiče na externí médium pro uložení dat prostřednictvím kalibračního nebo stahovacího konektoru. Záznamové zařízení před počátkem stahování dat aktualizuje údaje uložené na příslušné kartě.

150 Kromě toho jako přídavná funkce mohou být data stahována v jakémkoliv provozním režimu jiným konektorem pro podnik, který tímto kanálem prokáže svou totožnost. V tomto případě se při stahování využijí přístupová práva podniku pro stahování dat.

151 Stahování dat nesmí změnit nebo odstranit žádné uložené údaje.

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

Protokoly o stahování dat jsou uvedeny v dodatku 7.

19. **Výstupní data pro přídavná externí média**

152 Jestliže záznamové zařízení neobsahuje funkce zobrazení rychlosti nebo ujeté vzdálenosti, musí záznamové zařízení být zdrojem výstupního signálu(ů), které umožní zobrazení rychlosti (rychloměr) nebo vozidlem celkem ujeté vzdálenosti (měřič ujeté vzdálenosti).

153 Celek ve vozidle musí být také schopen dodat, prostřednictvím příslušného vyhrazeného sériového spojení nezávislého na přídavném připojení sběrnice CAN (ISO 11898 Silniční vozidla — Výměna digitálních informací — Oblast sítě řídících obvodů pro rychlou komunikaci), výstupní signál odpovídající následujícím údajům, což umožní jejich elektronické zpracování dalšími elektronickými jednotkami instalovanými ve vozidle:

— aktuální datum a čas UTC,

— rychlost vozidla,

— celková vozidlem ujetá vzdálenost (měřič ujeté vzdálenosti),

— současně navolená činnost řidiče a druhého řidiče,

— információ, amennyiben bármilyen tachográf-kártya éppen behelyezésre került a járművezetői vagy a járműkísérői kártyaolvasó egységbe, és (adott esetben), információ e kártyák azonosításáról (kártya száma és a kiállító tagállam).

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

Jestliže je zapnuto ‚zapalování' vozidla, musí být uvedená data neustále k dispozici na výstupní lince. Jestliže je ‚zapalování' vypnuto, musí být minimálně indikovány jakékoliv změny činnosti řidiče nebo druhého řidiče 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,

— digitální přizpůsobení konstanty 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 ukládaných do snímače pohybu (podle potřeby),

— kopírování potřebných identifikačních dat snímače pohybu ze snímače do celku ve vozidle.

156 Kalibrační funkce musí být schopna vložit nezbytná data prostřednictvím kalibračního nebo 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 dnů.

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 údajů 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/ES ze dne 31. října 1995 ([1]), kterou se přizpůsobuje technickému pokroku směrnice Rady 72/245/EHS ([2]) z hlediska elektromagnetické kompatibility, a mělo by být chráněno proti elektrostatickým výbojům a kolísání napájení.

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 stupni ochrany IP 64 podle normy IEC 529.

([1]) Úř. věst. L 266, 8.11.1995, s. 1.
([2]) Úř. věst. L 152, 6.7.1972, s. 15.

166 Zařízení musí vyhovovat odpovídajícím 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 údaje:

— v blízkosti údaje ujeté vzdálenosti jsou uvedeny jednotky vzdálenosti vyznačené zkratkou ‚km‘,

— v blízkosti údaje zobrazujícího rychlost je zkratka ‚km/h‘.

Záznamové zařízení může být také přepnuto, aby zobrazovalo rychlost v mílích za hodinu, a v tom případě je jednotka měřené rychlosti vyznačena zkratkou ‚mph‘.

169 Popisný štítek je připevněn na každý samostatný komponent záznamového zařízení a nese tyto 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, musí popisný štítek obsahovat alespoň jméno nebo značku výrobce a katalogové číslo komponentu.

IV. KONSTRUKČNÍ A FUNKČNÍ POŽADAVKY NA KARTY TACHOGRAFU

1. **Viditelné údaje**

Přední strana musí obsahovat:

171 slova ‚Karta řidiče‘ nebo ‚Kontrolní karta‘ nebo ‚Karta dílny‘ nebo ‚Karta podniku‘ vytištěná velkými písmeny v úředním jazyce nebo jazycích členského státu vydávajícího kartu, podle typu karty:

172 stejná slova v ostatních úředních jazycích Společenství vytištěná na zadní straně:

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

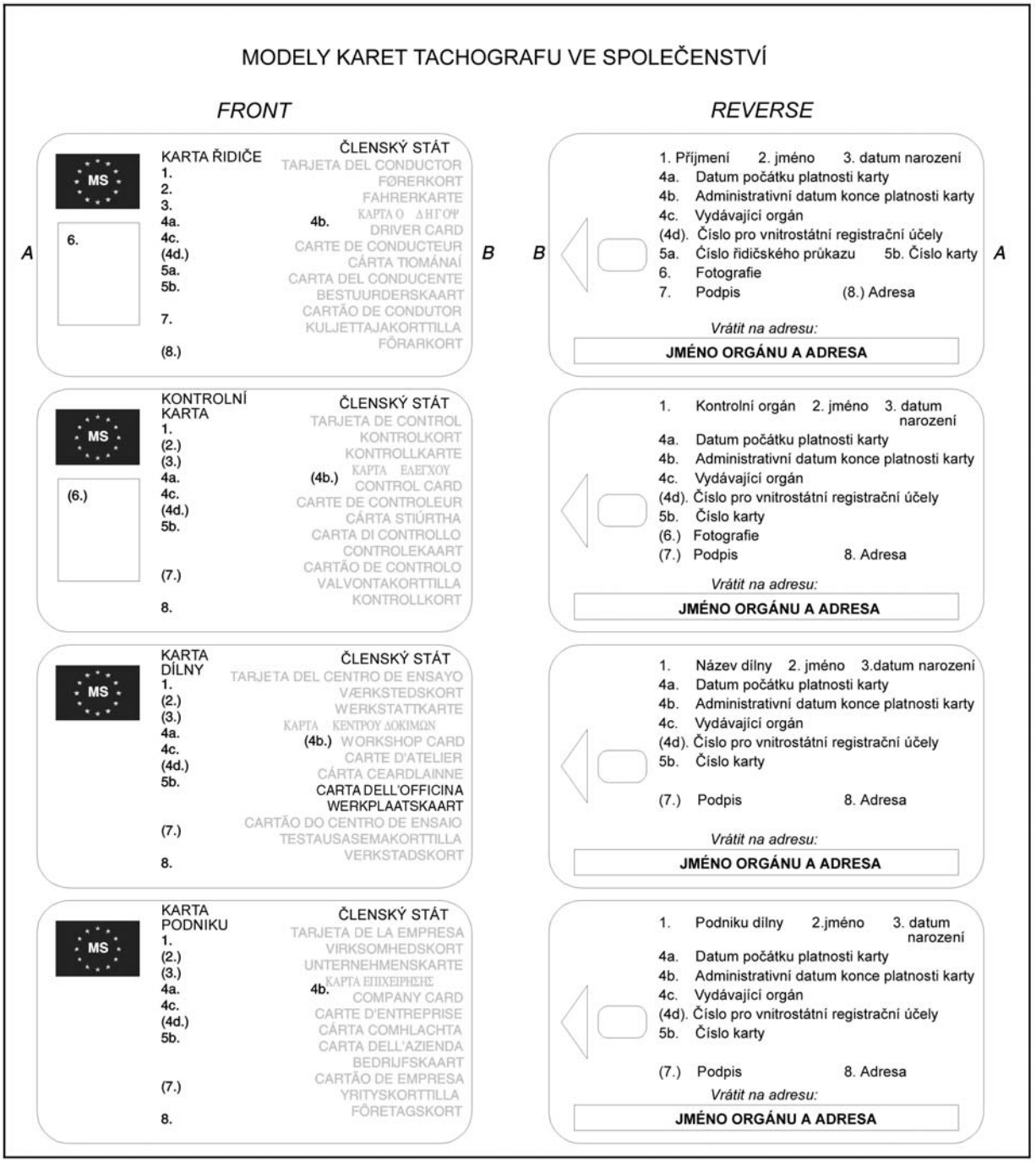
	Karta řidiče	Kontrolní karta	Karta podniku nebo karta dílny
1.	Příjmení řidiče	Jméno kontrolního orgánu	Karta podniku nebo karta dílny
2.	Jméno(a) řidiče	Příjmení kontrolora (pokud přichází v úvahu)	Příjmení držitele karty (pokud přichází v úvahu)
3.	Datum narození řidiče	Jméno(a) kontrolora (pokud přichází v úvahu)	Jméno(a) držitele karty (pokud přichází v úvahu)
4.(a)	Datum počátku platnosti karty		
(b)	Datum konce platnosti karty (pokud přichází v úvahu)		
(c)	Jméno 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 (volitelné)	—
7.	Podpis řidiče	Podpis držitele (volitelné)	
8.	Obvyklé místo pobytu nebo adresa držitele (volitelné)	Poštovní adresa kontrolního orgánu	Poštovní adresa podniku nebo dílny

176 datum musí být uváděno ve formátu ‚dd/mm/rrrr' nebo ‚dd.mm.rrrr' (den, měsíc, rok);

rubová strana musí 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, pokud nemění způsob použití daného modelu karty tachografu.



179 Karty tachografu musí být vydávány s těmito převládajícími barvami pozadí:

— karta řidiče: bílá barva

— kontrolní karta: modrá barva

— karta dílny: červená barva

— karta podniku: žlutá barva.

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

— 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 vnitrostátní 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 ve Všeobecných požadavcích na bezpečnost (dodatek 10).

183 Karty tachografu musí být čitelné dalšími zařízeními, např. osobními počítači.

3. **Normy**

184 Karty tachografu musí vyhovovat následujícím normám:

— ISO/IEC 7810 Identifikační karty — Fyzikální charakteristiky,

— ISO/IEC 7816 Identifikační karty — Integrované obvody s kontakty:

  — Část 1: Fyzikální charakteristiky,

  — Část 2: Rozměry a umístění kontaktů,

  — Část 3: Elektronické signály a přenosové protokoly,

  — Část 4: Formáty pro výměnu informací mezi průmyslovými odvětvími,

  — Část 8: Bezpečnost komunikace mezi průmyslovými odvětvími,

— ISI/IEC 10373 Identifikační karty — Zkušební postupy.

4. **Environmentální a elektrické specifikace**

185 Karty tachografu musí být schopny správné funkce za všech klimatických podmínek běžně se vyskytujících na území Společenství a nejméně v rozsahu teplot od −25 °C do +70 °C s příležitostnými špičkami do +85 °C. Příležitostnými špičkami se myslí na dobu nepřesahující 4 hodiny a ne více nežli 100krát 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/ES ze dne 31. října 1995 ([1]), vztahujícím se k elektromagnetické slučitelnosti, a musí být ochráněny proti elektrostatickým výbojům.

5. **Ukládání dat**

Pro účely tohoto odstavce

— jsou časové údaje 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 údajů jsou popsány v dodatku 2.

([1]) Úř. věst. 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 další údaje vztahující se k jiným účelům, případně vygenerované kartou, smějí být ukládány na kartu tachografu v souladu se směrnicí 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů ([1]).

5.1 ***Identifikace karty a bezpečnostní údaje***

5.1.1 *Identifikace použití*

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

— identifikace použití tachografu,

— identifikace typu karet tachografu.

5.1.2 *Identifikace čipu*

191 Karty tachografu musí být schopny ukládat následující identifikační data integrovaného obvodu:

— sériové číslo integrovaného obvodu,

— výrobní reference integrovaného obvodu.

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,

— identifikátor integrátoru,

— identifikátor integrovaného obvodu.

5.1.4 *Bezpečnostní prvky*

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

— 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,

— začátek a konec doby platnosti karty.

([1]) Úř. věst. L 281, 23.11.1995, s. 31.

5.2.2 *Identifikace držitele karty*

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

— příjmení držitele,

— jméno(a) držitele,

— datum narození,

— obvyklý jazyk držitele.

5.2.3 *Informace o řidičském průkazu*

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

— vydávající členský stát, název vydávajícího orgánu,

— číslo řidičského průkazu (ke dni vydání karty).

5.2.4 *Údaje o použitých vozidlech*

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

— datum a čas prvního použití vozidla (tzn. první vložení 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, kdy byla karta použita nebo pro který řidič vložil činnost ručně, následující údaje:

— datum,

— stav počitadla dnů od instalace jednotky do vozidla (vzroste o jednotku každý kalendářní den),

— celkovou vzdálenost ujetou řidičem v průběhu dne,

— stav řidiče v 00.00,

— kdykoliv se změní činnost řidiče nebo se změnil jeho stav nebo byla vložena nebo vyjmuta jeho karta:

  — stav posádky (POSÁDKA, SAMOTNÝ ŘIDIČ),

  — otvor pro vložení karty (ŘIDIČ, DRUHÝ ŘIDIČ),

  — stav karty (VLOŽENA, NEVLOŽENA),

  — činnost (JÍZDA, POHOTOVOST, PRÁCE, PŘESTÁVKA/ODPOČINEK),

  — čas změny.

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

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

5.2.6 *Místa, kde časy výkonu denní práce začínají nebo končí*

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

— datum a čas vložení údajů (nebo datum a čas vztahující se ke vložení údajů, pokud jsou zadávány řidičem ručně),

— typ vložených údajů (začátek nebo konec, podmínky vložení údajů),

— stát nebo region, 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 bodu je čas zaznamenáván s přesností jedné vteřiny.

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

— časové překrytí (je-li karta důvodem této události),

— vložení karty v průběhu jízdy,

— poslední použití karty nesprávně ukončeno (je-li karta důvodem této události),

— přerušení elektrického napájení,

— chyba údajů o pohybu vozidla,

— pokus o narušení bezpečnosti systému.

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 probíhala),

— datum a čas ukončení události (nebo čas vyjmutí karty, pokud událost v této době pokračovala),

— registrační číslo vozidla a členský stát, ve kterém bylo vozidlo registrováno.

Poznámka: V případě časového překrytí událostí:

— by mělo datum a čas počátku události 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 vozidlu používanému v průběhu události.

Poznámka: V případě ‚posledního nesprávně ukončeného použití':

— datum a čas počátku události by měl odpovídat datu a času vložení karty, jejíž použití bylo nesprávně ukončeno,

— datum a čas konce události by měl odpovídat datu a času vložení karty při použití, v jehož průběhu došlo k detekci události (současné použití karty),

— údaje o vozidlu by měly odpovídat vozidlu, ve kterém bylo použití karty nesprávně 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 bodu je čas zaznamenáván s přesností jedné vteřiny.

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

— chyba karty (v případě, že tato karta je předmětem události),

— chyba záznamového zařízení.

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

— kód závady,

— datum a čas počátku závady (nebo vložení karty, pokud závada v té době již probíhá),

— datum a čas ukončení závady (nebo vyjmutí karty, jestliže závada v té době pokračuje),

— registrační číslo vozidla a členský stát registrace vozidla, ve kterém závada nastala.

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

5.2.9 *Údaje o kontrolních činnostech*

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

— datum a čas provedení kontroly,

— číslo kontrolní karty a členský stát vydávající kartu,

— typ kontrolní činnosti (zobrazení nebo vytištění nebo stahování celku ve vozidle nebo stahování karty (viz poznámku)),

— dobu stahování dat, pokud k němu došlo,

— registrační číslo vozidla a členský stát registrace vozidla, u kterého kontrolní činnost proběhla.

Poznámka: Bezpečnostní požadavky implicitně předpokládají, že stahování karty 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:

— a kapcsolat megndatum a čas otevření použití karty (tzn. vložení karty) s rozlišovací schopností jedné vteřiny,yitásának (kártyabehelyezés) dátuma és időpontja, egy másodperces pontossággal,

— registrační číslo vozidla a členský stát registrace.

5.2.11 *Údaje o specifických podmínkách*

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

— datum a čas zadání dat,

— druh zvláštní podmínky.

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

5.3 ***Karta dílny***

5.3.1 *Bezpečnostní prvky*

213 Karta dílny musí být schopna uložit osobní identifikační číslo (PIN-kód).

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

5.3.2 *Identifikace karty*

215 Karta dílny musí být schopna uložit následující identifikační data karty:

— číslo karty,

— vydávající členský stát, název vydávajícího orgánu, datum vydání,

— datum počátku platnosti karty, datum konce platnosti.

5.3.3 *Identifikace držitele karty*

216 Karta dílny musí být schopna uložit následující identifikační data držitele karty:

— název dílny,

— adresa dílny,

— příjmení držitele,

— jméno(a) držitele,

— obvyklý jazyk držitele.

5.3.4 *Údaje o použitých vozidlech*

217 Karta dílny musí být schopna uložit záznamy o použitých vozidlech stejným způsobem jako karta řidiče.

218 Karta dílny musí být schopna uložit minimálně 4 takové záznamy.

5.3.5 *Údaje o řidičových činnostech*

219 Karta dílny musí být schopna uložit údaje o řidičových činnostech stejným způsobem, jako karta řidiče.

220 Karta dílny musí být schopna uchovat data minimálně o jednom průměrném dni řidičových činností.

5.3.6 *Začátek nebo ukončení doby denní činnosti řidiče*

221 Karta dílny musí být schopna uložit záznamy dat o začátcích a ukončeních denní práce stejným způsobem jako karta řidiče.

222 Karta dílny musí být schopna uchovat minimálně tři páry takových záznamů.

5.3.7 *Údaje o událostech a závadách*

223 Karta dílny musí být schopna uložit údaje o událostech a závadách stejným způsobem jako karta řidiče.

224 Karta dílny musí být schopna uložit údaje o třech posledních událostech každého typu (tzn. 18 událostí) a šest posledních záznamů o závadách každého typu (tzn. 12 závad).

5.3.8 *Údaje o kontrolních činnostech*

225 Karta dílny musí být schopna uložit údaje o kontrolních činnostech stejným způsobem jako karta řidiče.

5.3.9 *Údaje o kalibraci a nastavování času*

226 Karta dílny musí být schopna uchovat záznamy o kalibracích nebo nastavování času provedených v době, kdy je karta vložena v záznamovém zařízení.

227 Každý kalibrační záznam musí být schopen uchovat následující údaje:

— důvod kalibrace (první instalace, instalace, pravidelná kontrola),

— 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 Karta dílny musí být schopna uložit minimálně 88 takových záznamů.

229 Karta dílny musí mít počitadlo celkového počtu kalibrací provedených s kartou.

230 Karta dílny musí mít počitadlo počtu kalibrací provedených od posledního stahování dat.

5.3.10 *Údaje o specifických podmínkách*

230a Karta dílny musí být schopna uložit data týkající se specifických podmínek stejným způsobem jako karta řidiče. Karta dílny 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 konce 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,

— jméno(a) držitele,

— obvyklý jazyk držitele.

5.4.3 *Údaje o kontrolních činnostech*

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

— datum a čas kontroly,

— typ kontroly (zobrazení nebo vytištění nebo stahování dat záznamového zařízení nebo stahování dat karty),

— 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 kartu řidiče.

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

5.5 ***Karta podniku***

5.5.1 *Identifikace karty*

235 Karta podniku musí být schopna uložit následující identifikační data:

— číslo karty,

— vydávající členský stát, název vydávajícího orgánu, datum vydání,

— datum počátku platnosti karty, datum konce platnosti (pokud přichází v úvahu).

5.5.2 *Identifikace držitele karty*

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

— jméno podniku,

— adresa společnosti.

5.5.3 *Údaje o činnosti podniku*

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

— datum a čas činnosti,

— typ činnosti (uzamčení celku ve vozidle nebo odemknutí, nebo stahování dat záznamového zařízení 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 podniku musí být schopna uložit nejméně 230 takových záznamů.

V. INSTALACE ZÁZNAMOVÉHO ZAŘÍZENÍ

1. **Instalace**

239 Nové záznamové zařízení musí být dodáno schválené servisní dílně nebo výrobci vozidla neaktivované, se všemi kalibračními parametry, jak je uvedeno v kapitole III bodě 20, a s nastavenými příslušnými platnými implicitními hodnotami. V případě, že žádná specifická hodnota není považována za ‚příslušnou', měly by se alfanumerické parametry nastavit na ‚?' a numerické parametry na ‚0'.

240 Záznamového zařízení musí před aktivací umožnit přístup ke kalibrační funkci, dokonce i když není v kalibračním režimu.

241 Záznamového zařízení nesmí před aktivací zaznamenávat nebo ukládat údaje vztahující se ke kapitole III bodům 12.3 až 12.9 a 12.12 až 12.14 včetně.

242 V průběhu instalace musí výrobce přednastavit všechny známé parametry.

243 Výrobce vozidla nebo schválená 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 karty dílny do kteréhokoliv rozhraní.

245 Specifické úkony párování potřebné mezi snímačem pohybu a celkem ve vozidle, pokud je instalován, musí proběhnout automaticky před 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 přístup ke všem funkcím z jeho sedadla.

2. **Instalační štítek**

249 Po provedení prohlídky záznamového zařízení, která následuje po instalaci, se umístí na záznamové zařízení, do něj nebo vedle něj instalační štítek tak, aby byl dobře viditelný a snadno přístupný. Po každé prohlídce provedené schváleným montérem nebo dílnou musí být původní štítek nahrazen novým.

250 Štítek musí obsahovat alespoň následující údaje:

— jméno, adresu a obchodní název schváleného montéra nebo servisní dílny,

— charakteristický součinitel vozidla ve formě ‚w = … imp/km‘,

— konstantu záznamového zařízení ve formě ‚k = … imp/km‘,

— efektivní obvod pneumatik kol ve formě ‚l = … mm‘,

— rozměr pneumatiky,

— datum, kdy byl stanoven charakteristický součinitel vozidla a kdy byl měřen efektivní obvod pneumatik kol,

— 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 štítek musí být umístěn tak, aby nebylo možné jej sejmout bez zničení jeho popisu.

252 Výše uvedené pečetě 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 nadále spolehlivě a správně funguje a bude opětovně zapečetěno schváleným montérem nebo servisní dílnou (v souladu s kapitolou VI) okamžitě po namontování omezovače rychlosti nebo jiného zařízení přispívajícího k bezpečnosti silničního provozu nebo v průběhu sedmi dnů v ostatních případech.

253 V každém případě, kdy jsou porušeny tyto pečetě, musí být vyhotoven písemný zápis se zdůvodněním celé události a musí být předán příslušnému orgánu.

VI. KONTROLY, INSPEKCE A OPRAVY

Požadavky týkající se okolností, za kterých mohou být odstraněny pečetě uváděné v článku 12.5 nařízení (EHS) č. 3821/85 naposledy pozměněného nařízením (ES) č. 2135/98, jsou definované v kapitole V(3) této přílohy.

1. **Schvalování montérů nebo servisních dílen**

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

— instalací,

— kontrol,

— inspekcí,

— oprav.

V rámci čl. 12 odst. 1 tohoto nařízení se vydávají karty, kromě řádně odůvodněných případů, pouze servisům nebo dílnám oprávněným k aktivaci nebo kalibraci záznamových zařízení v souladu s touto přílohou:

— které nejsou oprávněny k použití karty podniku,

— a jejichž další profesní činnosti nepředstavují potenciální střet zájmů z hlediska celkové bezpečnosti systému definovaného v dodatku 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 bodech 2.1 a 2.2, zapečetění v souladu s kapitolou V bodem 3 a kalibraci.

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 bodech 2.1 a 2.2.

4. **Pravidelné kontroly**

256 Pravidelná kontrola zařízení instalovaného do vozidla musí proběhnout po každé opravě záznamového zařízení, po jakékoliv změně charakteristického součinitele vozidla, efektivního obvodu pneumatik kol, 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,

— je připevněn instalační štítek,

— pečetě na záznamovém zařízení a dalších instalovaných částech jsou nedotčené,

— odpovídají rozměr a efektivní obvod pneumatik kol.

258 Tyto kontroly musí obsahovat kalibraci

5. **Měření chyb**

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 obvyklém provozním stavu,

— tlak v pneumatikách souhlasí s pokyny výrobce,

— opotřebení pneumatiky je v toleranci povolené vnitrostátními právními předpisy,

— pohyb vozidla:

  — vozidlo se pohybuje vlastní silou po přímé a vodorovné trati rychlostí 50 ± 5 km/hod. Měřená vzdálenost je minimálně 1 000 m,

— za předpokladu, že je zajištěna srovnatelná 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 dotyčnému dopravnímu podniku.

261 Schválení montéři a servisní dílny musí dopravnímu podniku vydat potvrzení o nestáhnutelnosti dat, pokud špatná funkce záznamového zařízení brání stažení dříve zaznamenaných dat i v případě, že oprava byla prováděna v téže dílně. Servisní dílny musí archivovat kopie vydaných potvrzení 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 třeba), index náhrady a index obnovy, které jsou nastaveny na hodnotu ‚0'.

263 Čísla karet všech neosobních karet tachografu, které byly vydány témuž kontrolnímu orgánu, téže dílně nebo témuž dopravnímu podniku, 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 náhrady, který se zvedne o jednotku (v pořadí 0, …, 9, A, …, Z).

265 Karta tachografu, která se vydává jako náhrada již existující karty, musí mít shodné datum konce platnosti jako nahrazovaný exemplář.

266 Karta tachografu vydávaná při obnovení již existující karty musí mít stejné číslo karty jako obnovovaný exemplář s výjimkou indexu náhrady, který je nastaven na hodnotu ‚0', a indexu obnovy, který je zvýšen o jednotku (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 ve stejném členském státě, nebo podle pravidel pro první vydání karty, pokud probíhá v jiném členském státě.

268 ‚Příjmení držitele karty' u neosobních karet nebo kontrolních karet musí být vyplněno názvem dílny nebo kontrolního orgánu.

VIII. SCHVÁLENÍ TYPU ZÁZNAMOVÉHO ZAŘÍZENÍ A KARET TACHOGRAFU

1. **Obecná ustanovení**

Pro účely této kapitoly se ‚záznamovým zařízením' rozumí ‚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 přídavnými zařízeními.

270 Postup schvalování typu záznamového zařízení a karet tachografu musí zahrnovat zkoušky bezpečnostních opatření, funkční zkoušky a zkoušky vzájemné operační součinnosti. Pozitivní výsledky těchto zkoušek se potvrdí vhodnými osvědčeními.

271 Orgány příslušné pro schvalování typu členských států nevydají certifikát schválení typu v souladu s článkem 5 tohoto nařízení, pokud neobdrží:

— osvědčení o bezpečnosti zařízení,

— osvědčení o funkčnosti,

— a osvědčení o vzájemné operační součinnosti

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

272 Jakákoliv úprava týkající se programového nebo technického vybavení zařízení nebo povahy materiálu použitého pro jeho výrobu musí být před zavedením oznámena orgánem vydávajícím schválení typu zařízení. Tento orgán potvrdí výrobci rozšíření schválení typu nebo může požadovat aktualizaci nebo potvrzení osvědčení o funkčnosti, o bezpečnosti nebo o vzájemné operační součinnosti.

273 Postup aktualizace programového vybavení instalovaného v záznamovém zařízení musí být schválen orgánem, který vydal schválení typu pro záznamové zařízení. Aktualizace programového vybavení nesmí změnit ani vymazat žádné údaje o činnosti řidiče uložená v záznamovém zařízení. Programové vybavení může být aktualizováno pouze na odpovědnost výrobce zařízení.

2. **Osvědčení o bezpečnosti**

274 Zkoušky bezpečnosti se provedou v souladu s podmínkami dodatku 10 této přílohy.

3. **Osvědčení o funkčnosti**

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

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

277 Orgán příslušný pro schvalování typu vydá osvědčení o funkčnosti. Toto osvědčení musí obsahovat, kromě jména příjemce osvědčení a identifikace modelu, podrobný seznam provedených zkoušek a dosažených výsledků.

4. **Osvědčení o vzájemné operační součinnosti**

278 Zkoušky vzájemné operační součinnosti se provádějí v jediné zkušebně schválené a podléhající Evropské komisi.

279 Zkušební laboratoř zaznamenává požadavky výrobců o zkoušky vzájemné operační součinnosti v pořadí, v jakém byly doručeny.

280 Požadavky jsou úředně registrovány pouze tehdy, jestliže zkušebně již byly dodány:

— úplná sada materiálů a dokumentů nezbytných pro takové zkoušky vzájemné operační součinnosti,

— související osvědčení o bezpečnosti,

— související osvědčení o funkčnosti.

Datum registrace žádosti musí být oznámeno výrobci.

281 Žádné zkoušky vzájemné operační součinnosti zkušebna neprovádí u záznamového zařízení nebo karty tachografu, ke kterým nebyla poskytnuta osvědčení o bezpečnosti a funkčnosti.

Každý výrobce požadující zkoušky vzájemné operační součinnosti se zaváže ponechat zkušební laboratoři, která odpovídá za provedení zkoušek, úplnou sadu materiálů a dokumentace, které byly ke zkouškám dodány.

Zkoušky vzájemné operační součinnosti musí být provedeny v souladu s odstavcem 5 dodatku 9 této přílohy postupně se všemi typy záznamových zařízení a karet tachografu:

— jejichž schválení typu je dosud platné nebo

— jejichž schválení typu bylo pozastaveno, ale mají platné osvědčení o vzájemné operační součinnosti.

284 Osvědčení o vzájemné operační součinnosti musí být laboratoří doručeno výrobci teprve tehdy, až jsou úspěšně absolvovány všechny požadované zkoušky vzájemné operační součinnosti.

285 Jestliže zkoušky vzájemné operační součinnosti nejsou úspěšné s jedním nebo několika záznamovými zařízeními nebo kartami tachografu podle požadavku 283, osvědčení o vzájemné operační součinnosti není vydáno, pokud výrobce žádající o schválení neprovede nezbytné úpravy a neabsolvuje úspěšně zkoušky vzájemné operační součinnosti. Zkušebna identifikuje důvod problému s pomocí příslušného výrobce a pokusí se mu pomoci nalézt technické řešení. V případě, že výrobce již upravil svůj výrobek, musí zajistit od příslušných orgánů potvrzení platnosti svého osvědčení o bezpečnosti a funkčnosti.

286 Osvědčení o vzájemné operační součinnosti je platné šest měsíců a postup musí být opakován na konci tohoto období, pokud výrobce neobdržel odpovídající schválení typu. Osvědčení doručí výrobce orgánu příslušnému pro schvalování typu členského státu, který vydal osvědčení o funkčnosti.

287 Jakýkoliv prvek, který by mohl způsobit závadu vzájemné operační součinnosti, nesmí být použit pro vytvoření zisku a nesmí vést k získání dominantního postavení.

5. **Certifikát schválení typu**

288 Orgán členského státu příslušný pro schvalování typu může vydat certifikát schválení typu, jakmile obdrží tři požadovaná osvědčení.

289 Orgán příslušný pro schvalování typu předá kopii certifikátu schválení typu zkušebně pověřené prováděním zkoušek vzájemné operační součinnosti v době vydání certifikátu výrobci.

290 Zkušebna pověřená prováděním zkoušek vzájemné operační součinnosti musí udržovat internetové stránky, na kterých je aktualizovaný seznam modelů záznamových zařízení a karet tachografu:

— pro které byla zaregistrována žádost o zkoušky vzájemné operační součinnosti,

— které obdržely osvědčení o vzájemné operační součinnosti (i dočasné),

— které získaly schválení typu.

6. **Výjimečný postup: první osvědčení o vzájemné operační součinnosti**

291 V průběhu čtyř měsíců po osvědčení prvního páru záznamového zařízení a karet tachografu (řidiče, dílny, kontrolní a podniku) z hlediska vzájemné operační součinnosti je jakékoliv vydané osvědčení o vzájemné operační součinnosti (včetně úplně prvního) týkající se žádostí registrovaných v tomto období považováno za dočasné.

292 Jestliže na konci tohoto období budou všechny uvažované výrobky vzájemně operačně součinné, stanou se všechna tato osvědčení definitivními.

293 Jestliže budou v tomto období zjištěny závady z hlediska vzájemné operační součinnosti, musí zkušebna pověřená prováděním zkoušek vzájemné operační součinnosti identifikovat za pomoci všech zúčastněných výrobců zdroje obtíží a vyzve výrobce k provedení nezbytných úprav.

294 Jestliže na konci tohoto období budou problémy vzájemné operační součinnosti přetrvávat, musí odpovědná zkušebna ve spolupráci se zúčastněnými výrobci a orgány příslušnými pro schvalování typu, které vydaly související osvědčení o funkčnosti, zjistit důvody obtíží a stanovit nezbytné úpravy, které musí provést zúčastnění výrobci. Hledání technického řešení smí trvat maximálně dva měsíce, po kterých v případě nenalezení odpovídajícího řešení rozhodne Komise po konzultaci se zkušebnou pověřenou prováděním zkoušek vzájemné operační součinnosti, která zařízení nebo karty obdrží definitivní osvědčení vzájemné operační součinnosti, a zdůvodní proč.

295 Jakákoliv žádost o zkoušky vzájemné operační součinnosti registrovaná mezi koncem čtyřměsíčního období, kdy byla vydána dočasná osvědčení, a datem rozhodnutí Komise podle požadavku 294 musí být odložena, dokud nebudou počáteční obtíže se vzájemnou operační součinností vyřešeny. Tyto žádosti budou potom vyřízeny v pořadí, v jakém byly registrovány.

Dodatek 1

SLOVNÍK DAT

OBSAH

1. ÚVOD

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

1.1 **Podklad pro definice typů dat**

Tento dodatek používá k definování typů dat Abstract Syntax Notation One (ASN.1). To umožňuje, že jednoduchá a strukturovaná data jsou definována bez toho, že by zahrnovala jakoukoliv zvláštní přenosovou skladbu (kódovací pravidla), která by byla závislá na aplikaci a systémovém prostředí.

Konvence názvů typů ASN.1 jsou provedeny v souladu s ISO/IEC 8824-1. To znamená, že:

— tam, kde je to možné, je význam typu dat naznačen přiřazenými názvy,

— tam, kde typ dat je skladba jiných typů dat, je název typu dat 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, ve kterém jsou data uložena a funkcí vztahující se k datům.

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

K umožnění několika typů kódovacích pravidel jsou některé ASN.1 typy v tomto dodatku omezeny identifikátory rozsahu hodnoty. Identifikátory rozsahu hodnot jsou definovány v bodě 3.

1.2 **Odkazy**

V tomto dodatku jsou použity tyto normy:

ISO 639	Kód pro názvy 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 1 (ASN.1): Specifikace základní notace. Druhé vydání: 1998
ISO/IEC 8825-2	Informační technika — ASN.1 kódovací pravidla: Specifikace zhuštěných kódovacích pravidel (PER — Packed Encoding Rules). Druhé vydání: 1998
ISO/IEC 8859-1	Informační technika — Sady grafických znaků kódované jedním 8bitovým bajtem — Část 1: Latinská abeceda 1, První vydání: 1998
ISO/IEC 8859-7	Informační technika — Sady grafických znaků kódované jedním 8bitovým bajtem — Část 7: Latinská a řecká abeceda. První vydání: 1987
ISO 16844-3	Silniční vozidla — Systémy tachografů — Rozhraní snímače pohybu. WD 3-20/05/99.

2. DEFINICE TYPU DAT

Pro každý z následujících typů dat spočívá standardní hodnota pro ‚neznámý' nebo ‚bezpředmětný' obsah v naplnění daného datového článku bajty ‚FF'.

2.1 **ActivityChangeInfo**

Tento typ dat dává možnost kódovat uvnitř dvoubajtového slova status otvoru pro kartu v 00.00 nebo status řidiče v 00.00 nebo změny činnosti nebo změny statusu řízení 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 — Oktetové uspořádání: 'scpaatttttttttttt'B (16 bitů)

Pro záznamy do paměti údajů (nebo status otvoru pro kartu):

's'B Otvor pro kartu:

'0'B: ŘIDIČ,

'1'B: ŘIDIČ,

'c'B Status řízení vozidla:

'0'B: SAMOTNÝ ŘIDIČ,

'1'B: POSÁDKA,

'p'B Status karty řidiče (nebo karty dílny) v příslušném otvoru pro kartu:

'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,

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

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

's'B Otvor pro kartu (nepoužije 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: SAMOTNÝ ŘIDIČ, '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 (nepoužije se, jestliže 'p' = 1 a 'c' = 0 kromě dále uvedené poznámky):

'00'B: PŘESTÁVKA/ODPOČINEK,

'01'B: POHOTOVOST,

'10'B: PRÁCE,

'11'B: ŘÍZENÍ VOZIDLA,

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

Poznámka pro případ ‚vyjmutí karty':

Je-li karta vyjmuta:

— 's' použije se a je určen otvor pro kartu, 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 ručního 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 notaci ‚hstring'. 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 4bitové skupiny v prvním oktetu nulové 4bitové skupiny.

Přípustné číslice jsou: 0, 1, … 9.

2.4 **CalibrationPurpose**

Kód k objasnění, proč byl soubor kalibračních parametrů 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,

'02'H první instalace: první kalibrace celku ve vozidle po jeho aktivaci,

'03'H instalace: první kalibrace celku ve vozidle v běžném vozidle,

'04'H pravidelná 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 bajtech. Nejvyšší hodnota je dána délkou OCTET STRING obsahující tyto záznamy (viz CardActivityLengthRange bod 3). Jestliže tento záznam je nejdelší denní záznam, musí být hodnota activityPreviousRecordLength nastavena na 0.

activityRecordLength je celková délka tohoto záznamu v bajtech. 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 bajtů v kartě řidiče nebo v kartě dílny, které jsou dostupné k uložení záznamů o činnosti řidiče.

```
CardActivityLengthRange ::= INTEGER(0..2^16-1)
```

Přiřazení hodnoty: viz bod 3.

2.7 **CardApprovalNumber**

Číslo schválení typu karty.

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

Přiřazení hodnoty: Není specifikováno.

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 kartě dílny 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 a členský stát registrace vozidla, ve 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 kartě dílny 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 bajtů od začátku řetězce) nejstaršího úplného denního záznamu v řetězci activityDailyRecords. Maximální hodnota je dána délkou řetězce.

activityPointerNewestRecord je určení začátku paměťového místa (počet bajtů od začátku řetězce) nejnovějšího 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 oktetový řetězec je cyklicky plněn záznamy CardActivityDailyRecord. Při prvním použití začíná ukládání do paměti údajů na prvním bajtu řetězce. Všechny nové záznamy jsou připojeny na konec předchozího. Když je řetězec plný, ukládání pokračuje na prvním bajtu 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, musí být activityPointerOldestDayRecord 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 orgán vydávající řidičský průkaz.

drivingLicenceIssuingNation je stát orgánu vydávajícího řidičský průkaz.

drivingLicenceNumber je číslo řidičského průkazu.

2.15 **CardEventData**

Informace uložené na kartě řidiče nebo kartě dílny 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).

cardEventRecords Text fehlt

2.16 **CardEventRecord**

Informace uložené na kartě řidiče nebo kartě dílny 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 a členský stát registrace vozidla, ve kterém událost nastala.

2.17 **CardFaultData**

Informace uložené na kartě řidiče nebo kartě dílny 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 kartě dílny 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 a členský stát registrace vozidla, ve kterém závada nastala.

2.19 **CardIccIdentification**

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

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

clockStop je mód Clockstop dle EN 726-3.

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

cardApprovalNumber je číslo schválení typu karty.

cardPersonaliserID je individuální identifikátor karty — dle definice v EN 726-3.

embedderIcAssemblerId je identifikátor výrobce karty nebo sestavovataele integrovaného obvodu dle EN 726-3.

icIdentifier je identifikátor integrovaného obvodu na kartě a výrobce integrovaného obvodu 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 orgánu vydávajícího kartu.

cardIssueDate je datum vydání karty současnému držiteli.

cardValidityBegin je datum počátku 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 podniku 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 karty dílny, kontrolní karty a karty podniku.

2.22 **CardPlaceDailyWorkPeriod**

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

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

placePointerNewestRecord je index posledního 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 otvory pro kartu celku ve vozidle.

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

Přiřazení hodnoty: Není specifikováno.

2.28 **CardSlotsStatus**

Kód udávající typ karet vložených do dvou otvorů pro kartu celku ve vozidle.

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

Přiřazení hodnoty — oktetové uspořádání: 'ccccdddd'B:

'cccc'B Identifikace typu karty vložené do otvoru pro kartu druhého řidiče,

'dddd'B Identifikace typu karty vložené do otvoru pro kartu řidiče,

s těmito identifikačními kódy:

'0000'B není vložena žádná karta,

'0001'B je vložena karta řidiče,

'0010'B je vložena karta dílny,

'0011'B je vložena kontrolní karta,

'0100'B je vložena karta podniku.

2.29 **CardStructureVersion**

Kód udávající 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 bajtem.

2.30 **CardVehicleRecord**

Informace uložené na kartě řidiče nebo kartě dílny 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 a členský stát registrace vozidla.

vuDataBlockCounter je hodnota VuDataBlockCounter při posledním výpisu doby použití vozidla.

2.31 **CardVehiclesUsed**

Informace uložené na kartě řidiče nebo kartě dílny 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': podpis (128 bajt.) || zbytek veřejného klíče (58 bajtů) || název certifikačního orgánu (8 bajtů).

2.33 **CertificateContent**

(Čistý) obsah certifikátu veřejného klíče podle dodatku 11 ‚Společné bezpečnostní mechanismy'.

```
CertificateContent ::= SEQUENCE {
   CertificateProfileIdentifier             INTEGER(0..255),
   CertificationAuthorityReference          KeyIdentifier,
   CertificateHolderAuthorisation           CertificateHolderAuthorisation,
   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..2^32-1)
   RequestMonthYear                       BCDString(SIZE(2))
   crIdentifier                           OCTET STRING(SIZE(1))
   manufacturerCode                       ManufacturerCode
}
```

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

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 certifikačního orgánu (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 dvoubajtové 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 podniku 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 posledního aktualizovaného companyActivityRecord.

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

companyActivityRecords je soubor všech záznamů o činnosti podniku.

companyActivityRecord je posloupnost informací vztahujících se k jedné činnosti podniku.

companyActivityType je typ činnosti podniku.

companyActivityTime je datum a čas činnosti podniku.

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

vehicleRegistrationInformation je registrační číslo vozidla členský stát registrace vozidla, jehož data jsou stažena, zablokována nebo odblokována.

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

2.38 **CompanyActivityType**

Kód udávající činnost podniku používajícího kartu podniku.

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

2.39 **CompanyCardApplicationIdentification**

Informace uložené na kartě podniku 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 podniku, které lze na kartu uložit.

2.40 **CompanyCardHolderIdentification**

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

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

companyName je jméno podniku držitele.

companyAddress je adresa podniku držitele.

cardHolderPreferredLanguage je obvyklý pracovní 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 233).

```
ControlCardControlActivityData ::= SEQUENCE {
   ControlPointerNewestRecord              INTEGER(0..NoOfControlActivityRecords-1),
   ControlActivityRecords                  SET SIZE(NoOfControlActivityRecords) OF
     ControlActivityRecord                   SEQUENCE {
       ControlType                             ControlType,
       ControlTime                             TimeReal,
       ControlledCardNumber                    FullCardNumber,
       ControlledVehicleRegistration           VehicleRegistrationIdentification,
       ControlDownloadPeriodBegin              TimeReal,
       ControlDownloadPeriodEnd                TimeReal
     }
}
```

controlPointerNewestRecord je index posledního 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 a členský stát registrace vozidlo, ve 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 obvyklý pracovní jazyk držitele karty.

2.44 **ControlType**

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

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

Přiřazení hodnoty — Oktetové uspořádání: 'cvpdxxxx'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:

'0'B: data se nestahují z celku ve vozidle během této kontrolní činnosti,

'1'B: data se stahují z celku ve vozidle 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: Není specifikováno.

2.46 **DailyPresenceCounter**

Čítač uložený v kartě řidiče a kartě dílny přičítající jedničku pro každý kalendářní den, karta byla vložena do celku ve vozidle. 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 vyjádřené 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 žádné datum.

2.48 **Distance**

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

```
Distance ::= INTEGER(0..2^16-1)
```

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 bajtů, které jsou k dispozici pro uložení záznamů činnosti.

noOfCardVehicleRecords je počet záznamů vozidla, které může karta 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 obvyklý pracovní 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 povolené rychlosti,

'08'H	přerušení 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 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,
'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 nejnovějších 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 pěti nejvážnějších událostí během posledních 365 dní,
'06'H	první událost nebo závada, která se vyskytla po poslední kalibraci,
'07'H	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..2^32-1)
   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..2^32-1)
```

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..2^32-1)
```

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, obsahuje holderSurname stejné informace jako companyName nebo workshopName nebo controlBodyName.

holderFirstNames je jméno(a) a iniciálu (y) držitele.

2.61 **K-ConstantOfRecordingEquipment**

Konstanta záznamového zařízení (definice m)).

```
K-ConstantOfRecordingEquipment ::= INTEGER(0..2^16-1)
```

Přiřazení hodnoty: Impulsy na kilometr v provozním rozsahu 0 až 64 255 imp/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..2^16-1)
```

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

2.64 **Language**

Kód identifikující pracovní 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). Toto datum může být aktualizováno libovolným celkem ve vozidle nebo čtečkou karet.

```
LastCardDownload ::= TimeReal
```

Přiřazení hodnoty: Není 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 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, jejichž jméno začíná písmenem 'A'
'18'H .. '1F'H	vyhrazeno pro výrobce, jejichž jméno začíná písmenem 'B'
'20'H .. '27'H	vyhrazeno pro výrobce, jejichž jméno začíná písmenem 'C'
'28'H .. '2F'H	vyhrazeno pro výrobce, jejichž jméno začíná písmenem 'D'
'30'H .. '37'H	vyhrazeno pro výrobce, jejichž jméno začíná písmenem 'E
'38'H .. '3F'H	vyhrazeno pro výrobce, jejichž jméno začíná písmenem 'F'
'40'H	Giesecke & Devrient GmbH
'41'H	GEM plus
'42'H .. '47'H	vyhrazeno pro výrobce, jejichž jméno začíná písmenem 'G'
'48'H .. '4F'H	vyhrazeno pro výrobce, jejichž jméno začíná písmenem 'H'
'50'H .. '57'H	vyhrazeno pro výrobce, jejichž jméno začíná písmenem 'I'
'58'H .. '5F'H	vyhrazeno pro výrobce, jejichž jméno začíná písmenem 'J'
'60'H .. '67'H	vyhrazeno pro výrobce, jejichž jméno začíná písmenem 'K'
'68'H .. '6F'H	vyhrazeno pro výrobce, jejichž jméno začíná písmenem 'L'
'70'H .. '77'H	vyhrazeno pro výrobce, jejichž jméno začíná písmenem 'L'
'78'H .. '7F'H	vyhrazeno pro výrobce, jejichž jméno začíná písmenem 'N'
'80'H	OSCARD
'81'H .. '87'H	vyhrazeno pro výrobce, jejichž jméno začíná písmenem 'O'
'88'H .. '8F'H	vyhrazeno pro výrobce, jejichž jméno začíná písmenem 'P'
'90'H .. '97'H	vyhrazeno pro výrobce, jejichž jméno začíná písmenem 'Q'
'98'H .. '9F'H	vyhrazeno pro výrobce, jejichž jméno začíná písmenem 'R'
'A0'H	SETEC
'A1'H	SIEMENS VDO
'A2'H	STONERIDGE
'A3'H .. 'A7'H	vyhrazeno pro výrobce, jejichž jméno začíná písmenem 'S'
'AA'H	TACHOCONTROL
'AB'H .. 'AF'H	vyhrazeno pro výrobce, jejichž jméno začíná písmenem 'T'
'B0'H .. 'B7'H	vyhrazeno pro výrobce, jejichž jméno začíná písmenem 'U'
'B8'H .. 'BF'H	vyhrazeno pro výrobce, jejichž jméno začíná písmenem 'V'
'C0'H .. 'C7'H	vyhrazeno pro výrobce, jejichž jméno začíná písmenem 'W'
'C8'H .. 'CF'H	vyhrazeno pro výrobce, jejichž jméno začíná písmenem 'X'
'D0'H .. 'D7'H	vyhrazeno pro výrobce, jejichž jméno začíná písmenem 'Y'
'D8'H .. 'DF'H	vyhrazeno pro výrobce, jejichž jméno začíná písmenem '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 nebo použité v mezinárodnímu dokladu o pojištění motorového vozidla (zelená karta).

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

Přiřazení hodnoty:

' '	žádné informace k dispozici
'A'	Rakousko
'AL'	Albánie
'AND'	Andorra
'ARM'	Arménie
'AZ'	Ázerbájdžán
'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,
-- Ázerbájdžán	(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,
-- Lichtenštejnsko	(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 karta dílny uložit.

NoOfCalibrationRecords ::= INTEGER(0..255)

Přiřazení hodnoty: viz bod 3.

2.74 **NoOfCalibrationsSinceDownload**

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

NoOfCalibrationsSinceDownload ::= INTEGER(0..2^{16}-1),

Přiřazení hodnoty: Není specifikováno.

2.75 **NoOfCardPlaceRecords**

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

NoOfCardPlaceRecords ::= INTEGER(0..255)

Přiřazení hodnoty: viz bod 3.

2.76 **NoOfCardVehicleRecords**

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

NoOfCardVehicleRecords ::= INTEGER(0..2^{16}-1)

Přiřazení hodnoty: viz bod 3.

2.77 **NoOfCompanyActivityRecords**

Počet záznamů činnosti podniku, které může karta podniku uložit.

NoOfCompanyActivityRecords ::= INTEGER(0..2^{16}-1)

Přiřazení hodnoty: viz bod 3.

2.78 **NoOfControlActivityRecords**

Počet záznamů kontrol činnosti, které kontrolní karta může uložit.

```
NoOfControlActivityRecords ::= INTEGER(0..2^16-1)
```

Přiřazení hodnoty: viz bod 3.

2.79 **NoOfEventsPerType**

Počet událostí každého typu události, které může karta uložit.

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

Přiřazení hodnoty: viz bod 3.

2.80 **NoOfFaultsPerType**

Počet závad každého typu závady, které může karta uložit.

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

Přiřazení hodnoty: viz bod 3.

2.81 **OdometerValueMidnight**

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

```
OdometerValueMidnight ::= OdometerShort
```

Přiřazení hodnoty: Není specifikováno

2.82 **OdometerShort**

Údaj měřiče ujeté vzdálenosti vozidla ve zkrácené formě.

```
OdometerShort ::= INTEGER(0..2^24-1)
```

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

2.83 **OverspeedNumber**

Počet událostí překročení povolené rychlosti od poslední kontroly překročení povolené rychlosti.

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

Přiřazení hodnoty: 0 znamená, že se nevyskytlo žádné překročení povolené rychlosti od poslední kontroly překročení povolené rychlosti, 1 znamená, že se vyskytla událost jednoho překročení povolené rychlosti od poslední kontroly překročení povolené rychlosti … 255 znamená, že 255 nebo více událostí překročení povolené rychlosti se vyskytlo od poslední kontroly překročení povolené 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 použitém řidičem, když vkládal svou kartu do celku ve vozidle (požadavek 081).

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

vehicleRegistrationIdentification je registrační číslo vozidla a členský stát registrace vozidla.

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'`	Cataluňa
`'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	Baleares
'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 kartě dílny 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 operačního 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 ‚Společné bezpečnostní mechanismy'.

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 specifickou podmínku (požadavky 050b, 105a, 212a a 230a).

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

Přiřazení hodnoty:

'00'H	RFU
'01'H	mimo působnost — začátek
'02'H	mimo působnost — konec
'03'H	PŘEVOZ LODÍ / PŘEVOZ VLAKEM
'04'H .. 'FF'H	RFU.

2.104 **SpecificConditionRecord**

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

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

entryTime je datum a čas vstupu.

specificConditionType je kód identifikující specifickou 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 použití.

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

Přiřazení hodnoty: Není specifikováno.

2.110 **TimeReal**

Kód pro kombinované datum a časové pole, kde datum a čas jsou vyjádřeny jako sekundy 00h00m00s po 1. lednu 1970 času GMT.

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

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

Nejvyšší možný údaj datum a čas je v roce 2106.

2.111 **TyreSize**

Označení rozměrů pneumatik.

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

Přiřazení hodnoty: podle směrnice 92/23/EHS ze dne 31. 3. 1992 (Úř. věst. L 129, s. 95).

2.112 **VehicleIdentificationNumber**

Identifikační číslo vozidla 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, ve kterém je vozidlo registrováno.

vehicleRegistrationNumber je registrační číslo vozidla.

2.114 **VehicleRegistrationNumber**

Registrační číslo vozidla. 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 nebo změnami statusu řízení nebo změnami statusu karty pro daný kalendářní den (požadavek 084) a související se stavem otvorů pro kartu v 00.00 téhož dne.

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

noOfActivityChanges je počet slov ActivityChangeInfo v souboru activityChangeInfos.

activityChangeInfos je soubor slov ActivityChangeInfo uložený v celku ve vozidle pro den. Vždy obsahuje dvě slova ActivityChangeInfo dávající status dvou otvorů pro kartu v 00.00 téhož 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 její adresa.

workshopCardNumber identifikuje kartu dílny použitou během kalibrace.

workshopCardExpiryDate je datum konce platnosti karty.

vehicleIdentificationNumber je identifikační číslo vozidla.

vehicleRegistrationIdentification obsahuje registrační číslo vozidla a členský stát registrace.

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 stará a nová hodnota měřiče ujeté vzdálenosti.

oldTimeValue, newTimeValue jsou stará a nová hodnota data a času.

nextCalibrationDate je datum příští kalibrace typu určeného v CalibrationPurpose, kterou provede schválený kontrolní orgán.

2.119 **VuCardIWData**

Informace uložené v celku ve vozidle týkající se cyklů vkládání a vyjímání karet řidiče nebo karet dílny 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 karty dílny 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 je příjmení a jméno držitele karty řidiče nebo karty dílny ve tvaru, jak jsou uložené na kartě.

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

cardExpiryDate je prošlé datum platnosti karty ve tvaru, jak jsou uložené na kartě.

cardInsertionTime je datum a čas vložení karty.

vehicleOdometerValueAtInsertion je údaj měřiče ujeté vzdálenosti při vložení karty.

cardSlotNumber je otvor pro kartu, 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 ručně 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 podniku (požadavek 104).

```
VuCompanyLocksData ::= SEQUENCE {

   NoOfLocks                               INTEGER(0..20),

   VuCompanyLocksRecords                   SET SIZE(noOfLocks) OF
                                           VuCompanyLocksRecord

}
```

noOfLocks je počet zámků uvedených ve vuCompanyLocksRecords.

vuCompanyLocksRecords je soubor záznamů zámků podniku.

2.123 **VuCompanyLocksRecord**

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

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

lockInTime, lockOutTime jsou datum a čas zamčení a odemčení zámku.

companyName, companyAddress jsou jméno a adresa podniku 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 ve 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 opět 0.

2.127 **VuDetailedSpeedBlock**

Informace uložené v celku ve vozidle týkající se přesné rychlosti vozidla během jedné minuty, ve 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(0.2^16-1),
   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 nejnovější datum pro které celek ve vozidle uchovává údaje 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 data a času uložených v celku ve vozidle.

maxDownloadableTime je nejnovější vyjmutí karty nebo změny činnosti nebo místo vstupu data 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 podniku nebo dílny.

2.131 **VuEventData**

Informace uložené v celku ve vozidle týkající se událostí (požadavek 094 kromě události překročení povolené 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 povolené 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 otvoru pro kartu řidiče v začátku události.

cardNumberCodriverSlotBegin identifikuje kartu vloženou do otvoru pro kartu druhého řidiče v začátku události.

cardNumberDriverSlotEnd identifikuje kartu vloženou do otvoru pro kartu řidiče na konci události.

cardNumberCodriverSlotEnd identifikuje kartu vloženou do otvoru pro kartu druhého řidiče na konci události.

similarEventsNumber je počet podobných událostí toho dne.

Tato posloupnost může být použita pro všechny události s výjimkou událostí překročení povolené 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 otvoru pro kartu řidiče v začátku závady.

cardNumberCodriverSlotBegin identifikuje kartu vloženou do otvoru pro kartu druhého řidiče v začátku závady.

cardNumberDriverSlotEnd identifikuje kartu vloženou do otvoru pro kartu řidiče na konci závady.

cardNumberCodriverSlotEnd identifikuje kartu vloženou do otvoru pro kartu 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 programové vybavení instalované 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 povolené rychlosti od poslední kontroly překročení povolené rychlosti (požadavek 095).

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

lastOverspeedControlTime je datum a čas poslední kontroly překročení povolené rychlosti.

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

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

2.140 **VuOverSpeedingEventData**

Informace uložené v celku ve vozidle týkající se událostí překročení povolené 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 povolené rychlosti.

2.141 **VuOverSpeedingEventRecord**

Informace uložené v celku ve vozidle týkající se událostí překročení povolené 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 otvoru pro kartu řidiče na začátku události.

similarEventsNumber je počet podobných událostí během toho dne.

2.142 **VuPartNumber**

Číslo součásti 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 verze programového vybavení celku ve vozidle.

```
VuSoftInstallationDate ::= TimeReal
```

Přiřazení hodnoty: Není specifikováno.

2.149 **VuSoftwareIdentification**

Informace uložená v celku ve vozidle týkající se instalovaného programového vybavení.

```
VuSoftwareIdentification ::= SEQUENCE {

   VuSoftwareVersion                         VuSoftwareVersion,

   VuSoftInstallationDate                    VuSoftInstallationDate

}
```

vuSoftwareVersion je číslo verze programového vybavení v celku ve vozidle.

vuSoftInstallationDate je datum instalace verze programového vybavení.

2.150 **VuSoftwareVersion**

Číslo verze programového vybavení celku ve vozidle.

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

Přiřazení hodnoty: Není specifikováno.

2.151 **VuSpecificConditionData**

Informace uložené v celku ve vozidle týkající se specifických podmínek.

```
VuSpecificConditionData ::= SEQUENCE {

   NoOfSpecificConditionRecords              INTEGER(0..2^16-1)

   SpecificConditionRecords                  SET SIZE (noOfSpecificConditionRecords) OF
                                             SpecificConditionRecord

}
```

noOfSpecificConditionRecords je počet záznamů uložených v souboru specificConditionRecords.

specificConditionRecords je soubor specifických 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 ve 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 data a času.

workshopName, workshopAddress jsou název dílny a její adresa.

workshopCardNumber identifikuje kartu dílny použitou k nastavení času.

2.154 **W-VehicleCharacteristicConstant**

Charakteristický koeficient vozidla (definice k)).

```
W-VehicleCharacteristicConstant ::= INTEGER(0..2^16-1))
```

Přiřazení hodnoty: Impulsy na kilometr v provozním rozsahu 0 až 64 255 imp/km.

2.155 **WorkshopCardApplicationIdentification**

Informace uložené na kartě dílny týkající se 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 bajtů, 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 kartě dílny týkající se činnosti dílny, která byla provedena s kartou (požadavky 227 a 229).

```
WorkshopCardCalibrationData ::= SEQUENCE {
   CalibrationTotalNumber                  INTEGER(0..2^16-1),
   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 nebo informace o nastavení času.

2.157 **WorkshopCardCalibrationRecord**

Informace uložené na kartě dílny týkající se kalibrace, která byla provedena s kartou (požadavek 227).

```
WorkshopCardCalibrationRecord ::= SEQUENCE {
   CalibrationPurpose                      CalibrationPurpose,
   VehicleIdentificationNumber             VehicleIdentificationNumber,
   VehicleRegistration                     VehicleRegistrationIdentification,
   wVehicleCharacteristicConstant          W-VehicleCharacteristicConstant,
   kConstantOfRecordingEquipment           K-ConstantOfRecordingEquipment,
   lTyreCircumference                      L-TyreCircumference,
   TyreSize                                TyreSize,
```

```
   AuthorisedSpeed                    SpeedAuthorised,
   OldOdometerValue                   OdometerShort,
   NewOdometerValue                   OdometerShort,
   OldTimeValue                       TimeReal,
   NewTimeValue                       TimeReal,
   NextCalibrationDate                TimeReal,
   VuPartNumber                       VuPartNumber,
   VuSerialNumber                     VuSerialNumber,
   SensorSerialNumber                 SensorSerialNumber
}
```

calibrationPurpose je účel kalibrace.

vehicleIdentificationNumber je identifikační číslo vozidla.

vehicleRegistration obsahuje registrační číslo vozidla a členský stát registrace.

wVehicleCharacteristicConstant je charakteristický koeficient vozidla.

kConstantOfRecordingEquipment je konstanta záznamového zařízení.

lTyreCircumference je efektivní obvod pneumatiky kol.

tyreSize je označení rozměrů pneumatik montovaných na vozidlo.

authorisedSpeed je maximální dovolená rychlost vozidla.

oldOdometerValue, newOdometerValue jsou stará a nová hodnota měřiče ujeté vzdálenosti.

oldTimeValue, newTimeValue jsou stará a nová hodnota data a času.

nextCalibrationDate je datum příští kalibrace typu určeného v CalibrationPurpose, kterou provede schválený kontrolní orgán.

vuPartNumber, vuSerialNumber and **sensorSerialNumber** jsou prvky dat pro identifikaci záznamového zařízení.

2.158 **WorkshopCardHolderIdentification**

Informace uložené na kartě dílny 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 obvyklý pracovní jazyk držitele karty.

2.159 **WorkshopCardPIN**

Osobní identifikační číslo karty dílny (požadavek 213).

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

Přiřazení hodnoty: Osobní identifikační číslo (PIN) známé držiteli karty, vpravo doplněné ‚FF' bajty do 8 bajtů.

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 bajtů (28 dní 93 změn činnosti za den)	13 776 bajtů (28 dní 240 změn činnosti za den)
`NoOfCardPlaceRecords`	84	112
`NoOfCardVehicleRecords`	84	200
`NoOfEventsPerType`	6	12
`NoOfFaultsPerType`	12	24

3.2 **Definice pro kartu dílny:**

Jméno proměnné hodnoty	min.	max.
`CardActivityLengthRange`	198 bajtů (1 den 93 změn činnosti za den)	492 bajtů (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 podniku:**

Jméno proměnné hodnoty	min.	max.
`NoOfCompanyActivityRecords`	230	520

4. SADY ZNAKŮ

V řetězcích 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 { | } ~
```

Jiné řetězce znaků (adresa, jméno, registrační číslo vozidla) používají navíc znaky, které jsou definovány kódy 192 až 255 normy ISO/IEC 8859-1 (sada znaků latinská abeceda 1) nebo normy ISO/IEC 8859-7 (sada znaků řecká abeceda).

5. KÓDOVÁNÍ

Při kódování dle ASN.1 musí být všechny typy dat kódovány podle ISO/IEC 8825-2.

Dodatek 2

SPECIFIKACE KARET TACHOGRAFU

OBSAH

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 je uvedeno v normě ISO/IEC 7816-2
cc	clock cycles (hodinové impulsy)
CHV	card holder verification information (informace k ověření držitele karty)
CLA	class byte of an APDU command (bajt 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 bajt 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 (bajty 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 bezpečným zpracováním zpráv)
PTS	protocol transmission selection (výběr protokolu přenosu)
RFU	reserved for future use (vyhrazeno pro budoucí použití)

RST	reset (reset karty)
SM	secure messaging (bezpečné zpracování zpráv)
SW1-SW2	status bytes (stavové bajty)
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 se odkazuje 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: 1994.

2. ELEKTRICKÉ A FYZIKÁLNÍ VLASTNOSTI

TCS_200 Všechny elektronické signály musí být v souladu s normou ISO/IEC 7816-3, pokud není uvedeno 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 podle ISO/IEC 7816-3.

TCS_203 Karta pracuje při U_{cc} = 3 V (+/– 0,3 V) nebo při U_{cc} = 5 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 uzemněn. 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 ± 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 bajt 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. TECHNICKÉ VYBAVENÍ A PŘENOS DAT

3.1 **Úvod**

Tento odstavec popisuje nutnou funkčnost požadovanou kartami tachografu a celkem ve vozidle k zajištění správného provozu a vzájemné operační 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 Bajt pro velikost informačního pole karty bude uveden v ATR ve znaku TA3. Tato hodnota činí nejméně 'F0h' (= 240 bajtů).

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 bajtů (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 bajtů.

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 bajtů (zajištěno IFD).

— Velikost informačního pole terminálu (IFSD) je uvedena 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 bajtů.

— Karta nevyžaduje na IFS nové seřízení.

3.2.2 ***ATR***

TCS_307 Zařízení kontroluje ATR bajty podle normy ISO/IEC 7816-3. Nenásleduje 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 bajtů 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) bajt).

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 bajtu.

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 bezpečného zpracováním zpráv (viz dodatek 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 ‚0Ch' pro třídu je možné použít příkaz READ BINARY s bezpečným zpracováním zpráv, jak je uvedeno v bodě 3.6.2.

3.4 **Kódování dat**

Jestliže musí být utajení dat ochráněno proti jejich přečtení ze souboru dat, je soubor označen jako ‚zakódovaný'. Kódování se provádí použitím bezpečného zpracování zpráv (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 ENVIRONMENT: SETTING A KEY	22
PERFORM HASH OF FILE	2A

TCS_314 V každé zprávě odezvy jsou poslány zpět stavové bajty SW1 a SW2, které stav zpracování příkazů označí.

SW1	SW2	Význam
90	00	Normální zpracování
61	XX	Normální zpracování. XX = počet platných bajtů 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 bezpečného zpracování zpráv) 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 datové objekty bezpečného zpracování zpráv chybí
69	88	Nesprávné datové objekty bezpečného zpracování zpráv
6A	82	Datové soubory nenalezeny
6A	86	Chybné parametry P1 — P2
6A	88	Referenční data nenalezena
6B	00	Chybné parametry (offset mimo EF)

SW1	SW2	Význam
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 dodatku 11 ‚Společné bezpečnostní mechanismy'.

Všechny příkazy jsou popsány nezávisle na použití protokolu (T=0 nebo T=1). APDU bajty CLA, INS, P1, P2, Lc a Le jsou vždy uvedeny. Jestliže nejsou Lc a Le potřebné pro popisovaný příkaz, zůstanou odpovídající délka, hodnota a popis prázdné.

TCS_315 Jestliže délka obou bajtů (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 bajtů odpovídá požadované a Le=0 (bezpečné zpracování zpráv), 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 bajtem '61La', kde La je počet dostupných bajtů 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 omezené.

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 bezpečné zpracování zpráv. Podmínka přístupu AUT je rovněž ztracena.

TCS_319 Příkazová zpráva

Bajt	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 bajtů 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)

Bajt	Délka	Hodnota	Popis
SW	2	'XXXXh'	stavová slova (SW1, SW2)

— Pokud je příkaz úspěšný, vrací karta zpět '9000',

— pokud aplikace odpovídající AID není nalezena, je zpět poslaný stav zpracování '6A82',

— při T=1 a pokud je Le bajt přítomen, je zpět poslaný stav zpracování '6700',

— při T=0 a pokud je vyžadována odezva po příkazu SELECT FILE, je zpět poslaný stav zpracování '6900',

— jestliže je vybraná aplikace považována za poškozenou (je detekována chyba integrity uvnitř souboru atributů), je zpět poslaný stav zpracování '6400' nebo '6581'.

3.6.1.2 *Výběr elementárního souboru na základě jeho identifikátoru souboru*

TCS_321 Příkazová zpráva

Bajt	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 bajtů 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)

bajt	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, je zpět poslaný stav zpracování '6A82',

— při T=1 a pokud je Le bajt přítomen, je zpět poslaný stav zpracování '6700',

— při T=0 a pokud je vyžadována odezva po příkazu SELECT FILE, je zpět poslaný stav zpracování '6900',

— jestliže je vybraný soubor považován za poškozený (je detekována chyba integrity uvnitř souboru atributů), je zpět poslaný stav zpracování '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 omezené.

Příkaz Read Binary se používá ke čtení dat z transparentního souboru.

Odezva karty sestává z přečtených a zpět poslaných dat volitelně uzavřených ve struktuře bezpečného zpracování zpráv.

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 bezpečného zpracování zpráv*

Tento příkaz dává možnost IFD číst data z EF aktuálně vybraná bez bezpečného zpracování zpráv.

TCS_324 Čtení dat ze souboru označeného ‚zakódovaný' není možné tímto příkazem.

TCS_325 Příkazová zpráva

Bajt	Délka	Hodnota	Popis
CLA	1	'00h'	nepožaduje se bezpečné zpracování zpráv
INS	1	'B0h'	
P1	1	'XXh'	offset v bajtech od začátku souboru: nejvýznamnější bajt
P2	1	'XXh'	offset v bajtech od začátku souboru: nejméně významný bajt
Le	1	'XXh'	očekávaná délka dat, počet bajtů ke čtení

Poznámka:bit 8 z P1 musí být nastaven na 0.

TCS_326 Zpráva o odezvě

Bajt	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, je zpět poslaný stav zpracování '6986',

— jestliže řízení přístupu vybraného souboru dat není uspokojivé, příkaz je přerušen s '6982',

— jestliže offset není kompatibilní s velikostí EF (offset > EF velikost EF), je zpět poslaný stav zpracování '6B00',

— jestliže velikost dat ke čtení není kompatibilní s velikostí EF (offset + Le > velikost EF), je zpět poslaný stav zpracování '6700' nebo '6Cxx', kde 'xx' udává přesnou délku,

— jestliže je detekována chyba integrity uvnitř souboru atributů, karta považuje soubor za poškozený a obnovitelný a zpět poslaný stav zpracování je '6400' nebo '6581',

— pokud chyba integrity je detekována uvnitř uložených dat, karta vrátí požadovaná data a zpět poslaný stav zpracování je '6281'.

3.6.2.2 *Příkaz s bezpečným zpracováním zpráv*

Tento příkaz dává možnost IFD číst data z EF aktuálně vybraná s bezpečným zpracováním zpráv za účelem ověření integrity přijatých dat a ochrany utajení dat v případě, že EF je označeno jako ‚zakódovaný'.

TCS_327 Příkazová zpráva

Bajt	Délka	Hodnota	Popis
CLA	1	'0Ch'	požaduje se bezpečné zpracování zpráv
INS	1	'B0h'	INS
P1	1	'XXh'	P1 (offset v bajtech od začátku souboru): nejvýznamnější bajt
P2	1	'XXh'	P2 (offset v bajtech od začátku souboru): nejméně významný bajt
Lc	1	'09h'	délka vstupních dat pro bezpečné zpracování zpráv
#6	1	'97h'	T_{LE}: jmenovka pro specifikaci očekávané délky
#7	1	'01h'	L_{LE}: očekávaná délka
#8	1	'NNh'	specifikace očekávané délky (originál Le): počet bajtů ke čtení

Bajt	Délka	Hodnota	Popis
#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 bajty)
Le	1	'00h'	podle specifikace v ISO/IEC 7816-4

TCS_328 Zpráva o odezvě, pokud EF není označeno jako ‚zakódovaný' a jestliže je vstupní formát bezpečného zpracování zpráv správný:

Bajt	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 bajty, jestliže L_{PV} >127 bajtů
#(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 bajty)
SW	2	'XXXXh'	stavová slova (SW1, SW2)

TCS_329 Zpráva o odezvě, pokud EF není označeno jako ‚zakódovaný' a jestliže vstupní formát bezpečného zpracování zpráv je správný:

Bajt	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 bajty, jestliže $_{CG}$ > 127 bajtů
#(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	'XX..XXh'	kryptografický kontrolní součet (4 nejvýznamnější bajty)
SW	2	'XXXXh'	stavová slova (SW1, SW2)

Vrácená kódovaná data obsahují první bajt označující použitý mód doplnění. Pro aplikaci tachografu přijímá indikátor doplnění vždy hodnotu '01h' označující, že použitý mód doplnění odpovídá módu podle ISO/IEC 7816-4 (jeden bajt s hodnotou '80h' následovaný několika nulovými bajty: ISO/IEC 9797, metoda 2).

‚Regulérní' stavy zpracování popsané pro příkaz READ BINARY bez bezpečného zpracování zpráv (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 bezpečného zpracování zpráv. V takovém případě je stav zpracování jednoduše vrácen bez struktury bezpečného zpracování zpráv:

TCS_330 Zpráva o odezvě, jestliže vstupní formát bezpečného zpracování zpráv není korektní

Bajt	Délka	Hodnota	Popis
SW	2	'XXXXh'	stavová slova (SW1, SW2)

— Jestliže neexistuje žádný aktuální klíč relace, je zpět poslaný stav zpracování '6A88'. To se stane tehdy, jestliže klíč relace již není generován nebo platnost klíče relace skončila (v tomto případě musí IFD zopakovat vzájemný proces prokázání totožnosti nastavením nového klíče relace).

— Jestliže některé datové objekty (jak je uvedeno výše) ve formátu bezpečného zpracování zpráv chybějí, je zpět poslaný stav zpracování '6987'. Tato chyba se objeví, jestliže očekávaná jmenovka chybí nebo jestliže tělo příkazu neodpovídá požadavkům.

— Jestliže některé datové objekty nejsou korektní, je zpět poslaný stav zpracování '6988'. Tato chyba se objeví, jestliže všechny požadované jmenovky existují, ale některé délky se liší od očekávaných.

— Jestliže je přezkoušení kryptografického kontrolního součtu chybné, je zpět poslaný stav zpracování '6688'.

3.6.3 ***Update Binary***

Tento 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 bezpečné zpracování zpráv).

3.6.3.1 *Příkaz bez bezpečného zpracování zpráv*

Tento příkaz umožňuje IFD psát data do aktuálně vybraného EF bez toho, aby karta přezkoušela integritu přijatých dat. Tento zřetelný mód je dovolený jen tehdy, když odpovídající soubor dat není označen ‚zakódovaný'.

TCS_332 Příkazová zpráva

Bajt	Délka	Hodnota	Popis
CLA	1	'00h'	nepožaduje se bezpečné zpracování zpráv
INS	1	'D6h'	
P1	1	'XXh'	offset v bajtech od začátku souboru: nejvýznamnější bajt
P2	1	'XXh'	offset v bajtech od začátku souboru: nejméně významný bajt
Lc	1	'NNh'	Lc délka dat k aktualizaci, počet bajtů 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

Bajt	Délka	Hodnota	Popis
SW	2	'XXXXh'	stavová slova (SW1, SW2)

— pokud je příkaz úspěšný, vrací karta zpět '9000',

— pokud EF není vybrán, je zpět poslaný stav zpracování '6986',

— jestliže řízení přístupu vybraného souboru dat není uspokojivé, příkaz je přerušen s '6982',

— jestliže offset není kompatibilní s velikostí EF (offset > velikost EF), je zpět poslaný stav zpracování '6B00',

— jestliže velikost dat k zapsání není kompatibilní s velikostí EF (offset + Le > velikost EF), je zpět poslaný stav zpracování '6700',

— jestliže je detekována chyba integrity uvnitř souboru atributů, karta považuje soubor za poškozený a neopravitelný, je zpět poslaný stav zpracování '6400' nebo '6500',

— jestliže je zápis neúspěšný, je zpět poslaný stav zpracování '6581'.

3.6.3.2 *Příkaz s bezpečným zpracováním zpráv*

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

Bajt	Délka	Hodnota	Popis
CLA	1	'0Ch'	požaduje se bezpečné zpracování zpráv
INS	1	'D6h'	INS
P1	1	'XXh'	offset v bajtech od začátku souboru: nejvýznamnější bajt
P2	1	'XXh'	offset v bajtech od začátku souboru: nejméně významný bajt
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 bajty, jestliže L_{PV} > 127 bajtů
#(7+L)-#(6+L+NN)	NN	'XX..XXh'	zřetelná datová hodnota
#(7+L+NN)	1	'8Eh'	T_{CC}: jmenovka pro kryptografický kontrolní součet
#(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 bajty)
Le	1	'00h'	podle specifikace v ISO/IEC 7816-4

TCS_335 Zpráva o odezvě, jestliže je vstupní formát bezpečného zpracování zpráv správný:

Bajt	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 bajty)
SW	2	'XXXXh'	stavová slova (SW1, SW2)

‚Regulérní' stavy zpracování popsané pro příkaz UPDATE BINARY bez bezpečného zpracování zpráv (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 bezpečného zpracování zpráv. V takovém případě je stav zpracování jednoduše vrácen bez struktury bezpečného zpracování zpráv:

TCS_336 Zpráva o odezvě, jestliže je chyba v bezpečném zpracování zpráv

Bajt	Délka	Hodnota	Popis
SW	2	'XXXXh'	stavová slova (SW1, SW2)

— jestliže neexistuje žádný aktuální klíč relace, je zpět poslaný stav zpracování '6A88',

— jestliže některé datové objekty (jak je uvedeno výše) ve formátu bezpečného zpracování zpráv chybějí, je zpět poslaný stav zpracování '6987'. Tato chyba se objeví, jestliže očekávaná jmenovka chybí nebo jestliže tělo příkazu neodpovídá požadavkům,

— jestliže některé datové objekty nejsou korektní, je zpět poslaný stav zpracování '6988'. Tato chyba se objeví, jestliže všechny požadované jmenovky existují, ale některé délky se liší od očekávaných,

— jestliže je přezkoušení kryptografického kontrolního součtu chybné, je zpět poslaný stav zpracování '6688'.

3.6.4 ***Get challenge***

Tento příkaz odpovídá ustanovením ISO/IEC 7816-4, jeho použití je ale ve srovnání s příkazem definovaným normou omezené.

Příkaz GET CHALLENGE požaduje, aby karta vydala výzvu pro své použití v proceduře vztahující se k bezpečnosti, ve které jsou kryptogram nebo kódovaná data posílána na kartu.

TCS_337 Kartou vydaná výzva je platná pouze pro příští příkaz, který používá výzvu poslanou na kartu.

TCS_338 Příkazová zpráva

Bajt	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

Bajt	Délka	Hodnota	Popis
#1-#8	8	'XX..XXh'	výzva
SW	2	'XXXXh'	stavová slova (SW1, SW2)

— pokud je příkaz úspěšný, vrací karta zpět '9000'-t küld vissza,

— jestliže je Le odlišné od '08h', je zpět poslaný stav zpracování '6700',

— jestliže parametry P1 — P2 nejsou korektní, je zpět poslaný stav zpracování '6A86'.

3.6.5 ***Verify***

Tento příkaz odpovídá ustanovením ISO/IEC 7816-4, jeho použití je ale ve srovnání s příkazem definovaným normou omezené.

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 bajty ‚FFh' do délky 8 bajtů.

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

Bajt	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

Bajt	Délka	Hodnota	Popis
SW	2	'XXXXh'	stavová slova (SW1, SW2)

— pokud je příkaz úspěšný, vrací karta zpět '9000',

— pokud odkaz CHV není nalezen, je zpět poslaný stav zpracování '6A88',

— jestliže je CHV zablokován (čítač zbývajících pokusů je na nule), je zpět poslaný stav zpracování '6983'. Když je tohoto stavu dosaženo, CHV nemůže už nikdy být úspěšně prezentován,

— jestliže je srovnání neúspěšné, čítač zbývajících pokusů se sníží a zpět poslaný stav zpracování je '63CX' (X > 0 a X se rovná čítači zbývajících CHV pokusů. Jestliže X = 'F', je čítač CHV pokusů větší než 'F'),

— jestliže je odkaz CHV považován za poškozený, je zpět poslaný stav zpracování '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

Bajt	Délka	Hodnota	Popis
CLA	1	'00h'	
INS	1	'C0h'	
P1	1	'00h'	
P2	1	'00h'	
Le	1	'XXh'	počet očekávaných bajtů

TCS_345 Zpráva o odezvě

Bajt	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, je zpět poslaný stav zpracování '6900' nebo '6F00'.

— Jestliže Le překročí počet dostupných bajtů nebo jestliže je Le nula, je zpět poslaný stav zpracování '6Cxx', kde 'xx' udává přesný počet dostupných bajtů. V takovém případě připravená data jsou ještě pro následující příkaz GET RESPONSE k dispozici.

— Jestliže Le není nula a je menší než počet dostupných bajtů, jsou požadovaná data normálně poslána kartou. Zpět poslaný stav zpracování je '61xx', kde 'xx' udává počet dodatečných bajtů, 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 odpovídá ustanovením ISO/IEC 7816-8, jeho použití je ale ve srovnání s příkazem definovaným normou omezené.

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

Bajt	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 bajtů
#6-#199	194	'XX..XXh'	certifikát: zřetězení datových elementů (jak je popsáno v doplňku 11)

TCS_349 Zpráva o odezvě

Bajt	Délka	Hodnota	Popis
SW	2	'XXXXh'	stavová slova (SW1, SW2)

— Pokud je příkaz úspěšný, vrací karta zpět '9000',

— Jestliže je ověření certifikátu chybné, je zpět poslaný stav zpracování '6688'. Proces ověření a rozvinutí certifikátoru je popsán v dodatku 11.

— Jestliže v bezpečném prostředí neexistuje žádný veřejný klíč, je zpět poslaný stav zpracování '6A88',

— Jestliže se vybraný veřejný klíč (použitý k rozvinutí certifikátu) považuje za poškozený, je zpět poslaný stav zpracování '6400' nebo '6581'.

— Jestliže má vybraný veřejný klíč (použitý k rozvinutí certifikátu) CHA.LSB (`CertificateHolderAuthorisation.equipmentType`) rozdílný od '00' (např.není jedním z členských států nebo Evropy), je zpět poslaný stav zpracování '6985'.

3.6.8 ***Internal Authenticate***

Tento příkaz odpovídá ustanovením 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 totožných dat včetně K1 (první element pro dohodu klíče relace) a RND1 a 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

Bajt	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

Bajt	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, je zpět poslaný stav zpracování '6A88'.

— Jestliže neexistuje žádný soukromý klíč v bezpečném prostředí, je zpět poslaný stav zpracování '6A88'.

— Jestliže se VU.CHR neshoduje s aktuálním identifikátorem veřejného klíče, je zpět poslaný stav zpracování '6A88'.

— Jestliže je vybraný soukromý klíč považován za poškozený, je zpět poslaný stav zpracování '6400' nebo '6581'.

TCS_353 Jestliže je příkaz INTERNAL AUTHENTICATE úspěšný, je aktuální klíč relace, pokud existuje, vymazaný 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 odpovídá ustanovením ISO/IEC 7816-4.

Použitím příkazu EXTERNAL AUTHENTICATE může karta prokázat totožnost IFD.

Proces prokazování totožnosti 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 správné, podmínka přístupu AUT se otevře.

TCS_357 Vstupní zakódování nese druhý element pro dohodu klíče relace K2.

TCS_358 Příkazová zpráva

Bajt	Délka	Hodnota	Popis
CLA	1	'00h'	CLA
INS	1	'82h'	INS
P1	1	'00h'	P1
P2	1	'00h'	P2 (použitý veřejný klíč je implicitně známý a byl již dříve nastaven příkazem MSE)
Lc	1	'80h'	Lc (délka dat poslaných na kartu)
#6-#133	128	'XX..XXh'	zakódování (viz dodatek 11)

TCS_359 Zpráva o odezvě

Bajt	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, je zpět poslaný stav zpracování '6A88'.

— Jestliže CHA aktuálně nastaveného veřejného klíče není zřetězení AID aplikace tachografu a typu zařízení celku ve vozidle, je zpět poslaný stav zpracování '6F00' (viz dodatek 11).

— Jestliže žádný soukromý klíč není v bezpečném prostředí, je zpět poslaný stav zpracování '6A88'.

— Jestliže je ověření certifikátu chybné, je zpět poslaný stav zpracování '6688'.

— Jestliže příkaz bezprostředně nepředchází příkaz GET CHALLENGE, je zpět poslaný stav zpracování '6985'.

— Jestliže se vybraný soukromý klíč považuje za poškozený, je zpět poslaný stav zpracování '6400' nebo '6581'.

TCS_360 Jestliže je příkaz EXTERNAL AUTHENTICATE úspěšný a jestliže je první část klíče relace k dispozici krátce před úspěšným provedením příkazu INTERNAL AUTHENTICATE, klíč relace je nastaven pro příští příkazy při použití bezpečného zpracování zpráv.

TCS_361 Jestliže první část klíče relace není k dispozici z dřívějšího příkazu INTERNAL AUTHENTICATE, není druhá část klíče relace poslaná IFD uložena na kartu. Tento mechanismus zajistí, že je vzájemný proces prokázání totožnosti proveden v pořadí uvedeném v dodatku 11.

3.6.10 ***Manage Security Environment***

Tento příkaz je použit pro nastavení veřejného klíče k účelu prokázání totožnosti.

Tento příkaz odpovídá ustanovením ISO/IEC 7816-8, jeho použití je ale ve srovnání s příkazem definovaným normou omezené.

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

Bajt	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 podle specifikace v dodatku 11

TCS_366 Zpráva o odezvě

Bajt	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, je zpět poslaný stav zpracování '6A88'.

— Pokud chybějí některé očekávané datové objekty ve formátu bezpečného zpracování zpráv, je zpět poslaný stav zpracování '6987'. To může nastat, když chybí jmenovka '83h'.

— Jestliže některé datové objekty nejsou korektní, je zpět poslaný stav zpracování '6988'. To může nastat, když délka identifikátoru klíče není '08h'.

— Jestliže je vybraný klíč považován za poškozený, je zpět poslaný stav zpracování '6400' nebo '6581'.

3.6.11 ***PSO: Hash***

Tento příkaz slouží k přenosu výstupu tranformace určitých dat na kartu. Tento příkaz slouží pro ověření digitálních podpisů. Výstup tranformace je uložen v paměti EPROM pro následující příkaz ověření digitálního podpisu.

Tento příkaz odpovídá ustanovením ISO/IEC 7816-8, jeho použití je ale ve srovnání s příkazem definovaným normou omezené.

TCS_367 Příkazová zpráva

Bajt	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

Bajt	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), je zpět poslaný stav zpracování '6987'. To může nastat, když chybí jmenovka '90h'.

— Jestliže některé datové objekty nejsou korektní, je zpět poslaný stav zpracování '6988'. Tato chyba nastane, když potřebná jmenovka sice existuje, ale s jinou délkou než '14h'.

3.6.12 ***Perform Hash of File***

Tento příkaz neodpovídá ustanovením ISO/IEC 7816-8. Proto CLA-bajt tohoto příkazu udává, že následuje chráněné použití PERFORM SECURITY OPERATION/HASH.

TCS_369 Příkaz PERFORM HASH OF FILE je použit k transformaci rozsahu dat aktuálně vybraného transparentního souboru EF.

TCS_370 Výstup transformace 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

Bajt	Délka	Hodnota	Popis
CLA	1	'80h'	CLA
INS	1	'2Ah'	Perform Security Operation
P1	1	'90h'	jmenovka: Hash
P2	1	'00h'	P2: Transformace dat aktuálně vybraného transparentního souboru

TCS_372 Zpráva o odezvě

Bajt	Délka	Hodnota	Popis
SW	2	'XXXXh'	stavová slova (SW1, SW2)

— Pokud je příkaz úspěšný, vrací karta zpět '9000'.

— Pokud není vybrána žádná aplikace, je zpět poslaný stav zpracování '6985'.

— Jestliže je vybraný EF považován za poškozený (chyby integrity atributů souboru nebo uložených dat), je zpět poslaný stav zpracování '6400' nebo '6581'.

— Jestliže vybraný soubor není transparentní soubor, je zpět poslaný stav zpracování '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 odpovídá ustanovením ISO/IEC 7816-8, jeho použití je ale ve srovnání s příkazem definovaným normou omezené.

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

Bajt	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

Bajt	Délka	Hodnota	Popis
#1-#128	128	'XX..XXh'	podpis dříve vypočítaného výstupu transformace
SW	2	'XXXXh'	stavová slova (SW1, SW2)

— Pokud je příkaz úspěšný, vrací karta zpět '9000'.

— Jestliže se implicitně vybraný soukromý klíč považuje za poškozený, je zpět poslaný stav zpracování '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 výstup transformace je kartě znám. Algoritmus podpisu je kartě implicitně znám.

Tento příkaz odpovídá ustanovením ISO/IEC 7816-8, jeho použití je ale ve srovnání s příkazem definovaným normou omezené.

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

Bajt	Délka	Hodnota	Popis
CLA	1	'00h'	CLA
INS	1	'2Ah'	Perform Security Operation
P1	1	'00h'	
P2	1	'A8h'	jmenovka: datové pole obsahuje DO příslušný k ověření
Lc	1	'83h'	délka Lc následujícího datového pole
#28	1	'9Eh'	jmenovka pro digitální podpis
#29-#30	2	'8180h'	délka digitálního podpisu (128 bajtů, kódovaných podle ISO/IEC 7816-6)
#31-#158	128	'XX..XXh'	obsah digitálního podpisu

TCS_379 Zpráva o odezvě

Bajt	Délka	Hodnota	Popis
SW	2	'XXXXh'	stavová slova (SW1, SW2)

— Pokud je příkaz úspěšný, vrací karta zpět '9000'.

— Jestliže se ověření podpisu nezdaří, je zpět poslaný stav zpracování '6688'. Průběh ověřování je popsán v doplňku 11.

— Jestliže není vybrán žádný veřejný klíč, je zpět poslaný stav zpracování '6A88'.

— Pokud chybějí některé očekávané datové objekty (jak je uvedeno výše), je zpět poslaný stav zpracování '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), je zpět poslaný stav zpracování '6985'.

— Jestliže některé datové objekty nejsou korektní, je zpět poslaný stav zpracování '6988'. To může nastat, když jedna z požadovaných délek datových objektů není korektní.

— Jestliže je vybraný klíč považován za poškozený, je zpět poslaný stav zpracování '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` nebo `WorkshopCardPin`.

Užitečná kapacita paměti karet tachografu musí být nejméně 11 Kbajtů. 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 personalizaci vykazuje karta řidiče následující trvalou strukturu souborů a podmínek přístupu do souborů:

Soubor	ID souboru	Podmínky přístupu		
		Čtení	Aktualizace	Kódování
MF	3F00			
├─EF ICC	0002	ALW	NEV	No
├─EF IC	0005	ALW	NEV	No
└─DF Tachograph	0500			
├─EF Application_Identification	0501	ALW	NEV	No
├─EF Card_Certificate	C100	ALW	NEV	No
├─EF CA_Certificate	C108	ALW	NEV	No
├─EF Identification	0520	ALW	NEV	No
├─EF Card_Download	050E	ALW	ALW	No
├─EF Driving_Licence_Info	0521	ALW	NEV	No
├─EF Events_Data	0502	ALW	PRO SM / AUT	No
├─EF Faults_Data	0503	ALW	PRO SM / AUT	No
├─EF Driver_Activity_Data	0504	ALW	PRO SM / AUT	No
├─EF Vehicles_Used	0505	ALW	PRO SM / AUT	No
├─EF Places	0506	ALW	PRO SM / AUT	No
├─EF Current_Usage	0507	ALW	PRO SM / AUT	No
├─EF Control_Activity_Data	0508	ALW	PRO SM / AUT	No
└─EF Specific_Conditions	0522	ALW	PRO SM / AUT	No

TCS_401 Struktury všech EF jsou transparentní

TCS_402 Čtení s bezpečným zpracováním zpráv musí být možné pro všechny soubory pod DF tachograf.

TCS_403 Karta řidiče má následující strukturu dat:

Soubor/prvek dat	Počet záznamů	Velikost (v bajtech)		Standardní hodnoty
		Min	Max	
MF		*11411*	*24959*	
╠EF ICC		*25*	*25*	
└CardIccIdentification		*25*	*25*	
├clockStop		1	1	{00}
├cardExtendedSerialNumber		8	8	{00..00}
├cardApprovalNumber		8	8	{20..20}
├cardPersonaliserID		1	1	{00}
├embedderIcAssemblerId		5	5	{00..00}
└icIdentifier		2	2	{00 00}
╠EF IC		*8*	*8*	
└CardChipIdentification		*8*	*8*	
├icSerialNumber		4	4	{00..00}
└icManufacturingReferences		4	4	{00..00}
└DF Tachograph		*11378*	*24926*	
╠EF Application_Identification		*10*	*10*	
└DriverCardApplicationIdentification		*10*	*10*	
├typeOfTachographCardId		1	1	{00}
├cardStructureVersion		2	2	{00 00}
├noOfEventsPerType		1	1	{00}
├noOfFaultsPerType		1	1	{00}
├activityStructureLength		2	2	{00 00}
├noOfCardVehicleRecords		2	2	{00 00}
└noOfCardPlaceRecords		1	1	{00}
╠EF Card_Certificate		*194*	*194*	
└CardCertificate		194	194	{00..00}
╠EF CA_Certificate		*194*	*194*	
└MemberStateCertificate		194	194	{00..00}
╠EF Identification		*143*	*143*	
├CardIdentification		*65*	*65*	
├cardIssuingMemberState		1	1	{00}
├cardNumber		16	16	{20..20}
├cardIssuingAuthorityName		36	36	{20..20}
├cardIssueDate		4	4	{00..00}
├cardValidityBegin		4	4	{00..00}
└cardExpiryDate		4	4	{00..00}
└DriverCardHolderIdentification		*78*	*78*	
├cardHolderName		*72*	*72*	
├holderSurname		36	36	{00, 20..20}
└holderFirstNames		36	36	{00, 20..20}
├cardHolderBirthDate		4	4	{00..00}
└cardHolderPreferredLanguage		2	2	{20 20}

EF Card_Download		*4*	*4*	
LastCardDownload		4	4	
EF Driving_Licence_Info		*53*	*53*	
CardDrivingLicenceInformation		*53*	*53*	
drivingLicenceIssuingAuthority		36	36	{00, 20..20}
drivingLicenceIssuingNation		1	1	{00}
drivingLicenceNumber		16	16	{20..20}
EF Events_Data		*864*	*1728*	
CardEventData		*864*	*1728*	
cardEventRecords	6	*144*	*288*	
CardEventRecord	n_1	*24*	*24*	
eventType		1	1	{00}
eventBeginTime		4	4	{00..00}
eventEndTime		4	4	{00..00}
eventVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Faults_Data		*576*	*1152*	
CardFaultData		*576*	*1152*	
cardFaultRecords	2	*288*	*576*	
CardFaultRecord	n_2	*24*	*24*	
faultType		1	1	{00}
faultBeginTime		4	4	{00..00}
faultEndTime		4	4	{00..00}
faultVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Driver_Activity_Data		*5548*	*13780*	
CardDriverActivity		*5548*	*13780*	
activityPointerOldestDayRecord		2	2	{00 00}
activityPointerNewestRecord		2	2	{00 00}
activityDailyRecords	n_6	5544	13776	{00..00}
EF Vehicles_Used		*2606*	*6202*	
CardVehiclesUsed		*2606*	*6202*	
vehiclePointerNewestRecord		2	2	{00 00}
cardVehicleRecords		*2604*	*6200*	
CardVehicleRecord	n_3	*31*	*31*	
vehicleOdometerBegin		3	3	{00..00}
vehicleOdometerEnd		3	3	{00..00}
vehicleFirstUse		4	4	{00..00}
vehicleLastUse		4	4	{00..00}
vehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
vuDataBlockCounter		2	2	{00 00}
EF Places		*841*	*1121*	
CardPlaceDailyWorkPeriod		*841*	*1121*	
placePointerNewestRecord		1	1	{00}
placeRecords		*840*	*1120*	
PlaceRecord	n_4	*10*	*10*	
entryTime		4	4	{00..00}
entryTypeDailyWorkPeriod		1	1	{00}
dailyWorkPeriodCountry		1	1	{00}
dailyWorkPeriodRegion		1	1	{00}
vehicleOdometerValue		3	3	{00..00}
EF Current_Usage		*19*	*19*	
CardCurrentUse		*19*	*19*	
sessionOpenTime		4	4	{00..00}
sessionOpenVehicle				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Control_Activity_Data		*46*	*46*	
CardControlActivityDataRecord		*46*	*46*	
controlType		1	1	{00}
controlTime		4	4	{00..00}
controlCardNumber				
cardType		1	1	{00}
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
controlVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
controlDownloadPeriodBegin		4	4	{00..00}
controlDownloadPeriodEnd		4	4	{00..00}
EF Specific_Conditions		*280*	*280*	
SpecificConditionRecord	56	*5*	*5*	
entryTime		4	4	{00..00}
SpecificConditionType		1	1	{00}

TCS_404 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 bajtů (28 dnů * 93 změn činnosti)	13 776 bajtů (28 dnů * 240 změn činnosti)

4.2. **Struktura karty dílny**

TCS_405 Po personalizaci vykazuje karta dílny následující trvalou strukturu souborů a podmínek přístupu do souborů:

		Podmínky přístupu		
Soubor	ID souboru	Čtení	Aktualizace	Kódování
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 bezpečným zpracováním zpráv musí být možné pro všechny soubory pod DF tachograf.

TCS_408 Karta dílny má následující strukturu dat:

Soubor/prvek dat	Počet záznamů	Velikost (v bajtech) Min	Velikost (v bajtech) Max	Standardní hodnoty
MF		*11088*	*29061*	
├─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		*11055*	*29028*	
├─EF Application_Identification		*11*	*11*	
└─WorkshopCardApplicationIdentification		*11*	*11*	
├─typeOfTachographCardId		1	1	{00}
├─cardStructureVersion		2	2	{00 00}
├─noOfEventsPerType		1	1	{00}
├─noOfFaultsPerType		1	1	{00}
├─activityStructureLength		2	2	{00 00}
├─noOfCardVehicleRecords		2	2	{00 00}
├─noOfCardPlaceRecords		1	1	{00}
└─noOfCalibrationRecords		1	1	{00}

EF Card_Certificate		*194*	*194*	
CardCertificate		194	194	{00..00}
EF CA_Certificate		*194*	*194*	
MemberStateCertificate		194	194	{00..00}
EF Identification		*211*	*211*	
CardIdentification		*65*	*65*	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{00, 20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
WorkshopCardHolderIdentification		*146*	*146*	
workshopName		36	36	{00, 20..20}
workshopAddress		36	36	{00, 20..20}
cardHolderName				
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00, 20..20}
cardHolderPreferredLanguage		2	2	{20 20}
EF Card_Download		*2*	*2*	
NoOfCalibrationsSinceDownload		2	2	{00 00}
EF Calibration		*9243*	*26778*	
WorkshopCardCalibrationData		*9243*	*26778*	
calibrationTotalNumber		2	2	{00 00}
calibrationPointerNewestRecord		1	1	{00}
calibrationRecords		*9240*	*26775*	
WorkshopCardCalibrationRecord	n_5	*105*	*105*	
calibrationPurpose		1	1	{00}
vehicleIdentificationNumber		17	17	{20..20}
vehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
wVehicleCharacteristicConstant		2	2	{00 00}
kConstantOfRecordingEquipment		2	2	{00 00}
lTyreCircumference		2	2	{00 00}
tyreSize		15	15	{20..20}
authorisedSpeed		1	1	{00}
oldOdometerValue		3	3	{00..00}
newOdometerValue		3	3	{00..00}
oldTimeValue		4	4	{00..00}
newTimeValue		4	4	{00..00}
nextCalibrationDate		4	4	{00..00}
vuPartNumber		16	16	{20..20}
vuSerialNumber		8	8	{00..00}
sensorSerialNumber		8	8	{00..00}
EF Sensor_Installation_Data		*16*	*16*	
SensorInstallationSecData		16	16	{00..00}
EF Events_Data		*432*	*432*	
CardEventData		*432*	*432*	
cardEventRecords	6	*72*	*72*	
CardEventRecord	n_1	*24*	*24*	
eventType		1	1	{00}
eventBeginTime		4	4	{00..00}
eventEndTime		4	4	{00..00}
eventVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Faults_Data		*288*	*288*	
CardFaultData		*288*	*288*	
cardFaultRecords	2	*144*	*144*	
CardFaultRecord	n_2	*24*	*24*	
faultType		1	1	{00}
faultBeginTime		4	4	{00..00}
faultEndTime		4	4	{00..00}
faultVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Driver_Activity_Data		*202*	*496*	
CardDriverActivity		*202*	*496*	
activityPointerOldestDayRecord		2	2	{00 00}
activityPointerNewestRecord		2	2	{00 00}
activityDailyRecords	n_6	198	492	{00..00}
EF Vehicles_Used		*126*	*250*	
CardVehiclesUsed		*126*	*250*	
vehiclePointerNewestRecord		2	2	{00 00}
cardVehicleRecords		*124*	*248*	
CardVehicleRecord	n_3	*31*	*31*	
vehicleOdometerBegin		3	3	{00..00}

├─vehicleOdometerEnd		3	3	{00..00}
├─vehicleFirstUse		4	4	{00..00}
├─vehicleLastUse		4	4	{00..00}
├─vehicleRegistration				
│ ├─vehicleRegistrationNation		1	1	{00}
│ └─vehicleRegistrationNumber		14	14	{00, 20..20}
└─vuDataBlockCounter		2	2	{00 00}
═EF Places		*61*	*81*	
└─CardPlaceDailyWorkPeriod		*61*	*81*	
├─placePointerNewestRecord		1	1	{00}
└─placeRecords		*60*	*80*	
└─PlaceRecord	n_4	*10*	*10*	
├─entryTime		4	4	{00..00}
├─entryTypeDailyWorkPeriod		1	1	{00}
├─dailyWorkPeriodCountry		1	1	{00}
├─dailyWorkPeriodRegion		1	1	{00}
└─vehicleOdometerValue		3	3	{00..00}
═EF Current_Usage		*19*	*19*	
└─CardCurrentUse		*19*	*19*	
├─sessionOpenTime		4	4	{00..00}
└─sessionOpenVehicle				
├─vehicleRegistrationNation		1	1	{00}
└─vehicleRegistrationNumber		14	14	{00, 20..20}
═EF Control_Activity_Data		*46*	*46*	
└─CardControlActivityDataRecord		*46*	*46*	
├─controlType		1	1	{00}
├─controlTime		4	4	{00..00}
├─controlCardNumber				
│ ├─cardType		1	1	{00}
│ ├─cardIssuingMemberState		1	1	{00}
│ └─cardNumber		16	16	{20..20}
├─controlVehicleRegistration				
│ ├─vehicleRegistrationNation		1	1	{00}
│ └─vehicleRegistrationNumber		14	14	{00, 20..20}
├─controlDownloadPeriodBegin		4	4	{00..00}
└─controlDownloadPeriodEnd		4	4	{00..00}
═EF Specific_Conditions		*10*	*10*	
└─SpecificConditionRecord	2	*5*	*5*	
├─entryTime		4	4	{00..00}
└─SpecificConditionType		1	1	{00}

TCS_409 Následující, v tabulce uvedené hodnoty k údajům o rozměrech jsou nejmenší a největší počty záznamů, které musí datová struktura karty dílny 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 bajtů (1 dnů * 93 změn činnosti)	492 bajtů (1 dnů * 240 změn činnosti)

4.3 **Struktura kontrolní karty**

TCS_410 Po personalizaci vykazuje kontrolní karta následující trvalou strukturu souborů a podmínek přístupu do souborů:

		Podmínky přístupu		
Soubor	ID souboru	Čtení	Aktualizace	Kódování
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 bezpečným zpracováním zpráv musí být možné pro všechny soubory pod DF tachograf.

TCS_413 Kontrolní karta má následující strukturu dat:

Soubor/prvek dat	Počet záznamů	Velikost (v bajtech) Min	Velikost (v bajtech) Max	Standardní hodnoty
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 podniku**

TCS_415 Po personalizaci vykazuje karta podniku následující trvalou strukturu souborů a podmínek přístupu do souborů:

Soubor	ID souboru	Podmínky přístupu		
		Čtení	Aktualizace	Kódování
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 bezpečným zpracováním zpráv musí být možné pro všechny soubory pod DF tachograf.

TCS_418 Karta podniku má následující strukturu dat:

Soubor/prvek dat	Počet záznamů	Velikost (v bajtech) Min	Velikost (v bajtech) Max	Standardní hodnoty
MF		*11147*	*24487*	
├─EF ICC		*25*	*25*	
│ └─CardIccIdentification		*25*	*25*	
│ ├─clockStop		1	1	{00}
│ ├─cardExtendedSerialNumber		8	8	{00..00}
│ ├─cardApprovalNumber		8	8	{20..20}
│ ├─cardPersonaliserID		1	1	{00}
│ ├─embedderIcAssemblerId		5	5	{00..00}
│ └─icIdentifier		2	2	{00 00}
├─EF IC		*8*	*8*	
│ └─CardChipIdentification		*8*	*8*	
│ ├─icSerialNumber		4	4	{00..00}
│ └─icManufacturingReferences		4	4	{00..00}
└─DF Tachograph		*11114*	*24454*	
├─EF Application_Identification		*5*	*5*	
│ └─CompanyCardApplicationIdentification		*5*	*5*	
│ ├─typeOfTachographCardId		1	1	{00}
│ ├─cardStructureVersion		2	2	{00 00}
│ └─noOfCompanyActivityRecords		2	2	{00 00}
├─EF Card_Certificate		*194*	*194*	
│ └─CardCertificate		194	194	{00..00}
├─EF CA_Certificate		*194*	*194*	
│ └─MemberStateCertificate		194	194	{00..00}
├─EF Identification		*139*	*139*	
│ ├─CardIdentification		*65*	*65*	
│ │ ├─cardIssuingMemberState		1	1	{00}
│ │ ├─cardNumber		16	16	{20..20}
│ │ ├─cardIssuingAuthorityName		36	36	{00, 20..20}
│ │ ├─cardIssueDate		4	4	{00..00}
│ │ ├─cardValidityBegin		4	4	{00..00}
│ │ └─cardExpiryDate		4	4	{00..00}
│ └─CompanyCardHolderIdentification		*74*	*74*	
│ ├─companyName		36	36	{00, 20..20}
│ ├─companyAddress		36	36	{00, 20..20}
│ └─cardHolderPreferredLanguage		2	2	{20 20}
└─EF Company_Activity_Data		*10582*	*23922*	
└─CompanyActivityData		*10582*	*23922*	
├─companyPointerNewestRecord		2	2	{00 00}
└─companyActivityRecords		*10580*	*23920*	
└─companyActivityRecord	n_8	46	46	
├─companyActivityType		1	1	{00}
├─companyActivityTime		4	4	{00..00}
├─cardNumberInformation				
│ ├─cardType		1	1	{00}
│ ├─cardIssuingMemberState		1	1	{00}
│ └─cardNumber		16	16	{20..20}
├─vehicleRegistrationInformation				
│ ├─vehicleRegistrationNation		1	1	{00}
│ └─vehicleRegistrationNumber		14	14	{00, 20..20}

├─cardNumberInformation			
│ ├─cardType	1	1	{00}
│ ├─cardIssuingMemberState	1	1	{00}
│ └─cardNumber	16	16	{20..20}
├─downloadPeriodBegin	4	4	{00..00}
└─downloadPeriodEnd	4	4	{00..00}

TCS_419 Následující, v tabulce uvedené hodnoty k údajům o rozměrech jsou nejmenší a největší počty záznamů, které musí datová struktura karty podniku použít:

		Min	Max
n_8	NoOfCompanyActivityRecords	230	520

Dodatek 3

PIKTOGRAMY

PIC_001 Záznamové zřízení může používat tyto piktogramy a jejich kombinace:

1. ZÁKLADNÍ PIKTOGRAMY

	Osoby	**Akce**	**Mód provozu**
	podnik		podnikový mód
	kontrolor	kontrola	kontrolní mód
	řidič	řízení	provozní mód
	dílna/zkušebna	přezkoušení/kalibrace	kalibrační mód
	výrobce		

	Činnosti	**Trvání**
	pohotovost	průběžná doba pohotovosti
	řízení	nepřetržitá doba řízení
	odpočinek	nepřetržitá doba odpočinku
	práce	nepřetržité trvání práce
	přestávka	kumulovaná doba odpočinku
?	neznámá	

	Zařízení	**Funkce**
1	otvor pro kartu řidiče	
2	otvor pro kartu druhého řidiče	
	karta	
	hodiny	
	displej	zobrazení
	externí paměťové médium	stažení dat
	napájení (el. proudem)	
	tiskárna/výtisk	tisknout
	snímač	
	rozměr pneumatiky	
	vozidlo/celek ve vozidle	

	Zvláštní podmínky
OUT	kontrolní zařízení není nutné
	PŘEVOZ LODÍ / PŘEVOZ VLAKEM

	Různé		
!	události		závady
	začátek denní pracovní doby		konec denní pracovní doby
	umístění	M	ruční zadání činností řidiče
	bezpečnost	>	rychlost
	čas	Σ	celkem/souhrn

	Kvalifikace
24h	denně
| >	týdně
||	dva týdny
	od nebo do

2. KOMBINACE PIKTOGRAMŮ

	Různé		
	kontrolní místo		
	místo začátku denní pracovnídoby		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 podniku


kontrolní karta

karta dílny


žádná karta

Řízení


řízení posádkou

doba řízení během jednoho týdne

doba řízení během dvou týdnů

Tisky


denní výtisk činností řidiče z karty

denní výtisk činností řidiče z celku ve vozidle

výtisk událostí a závad z karty


výtisk událostí a závad z celku ve vozidle


výtisk technických dat


výtisk překročení povolené rychlosti

Události


vložení neplatné karty


konflikt karty

překrytí času


řízení bez vhodné karty

vložení karty během řízení


nesprávné uzavření poslední operace


překročení povolené rychlosti


přerušení napájení proudem


chyba dat dráhy a rychlosti

narušení spolehlivosti


nastavení času (dílnou)

kontrola překročení povolené rychlosti

Závady


závada karty (otvor pro kartu řidiče)

závada karty (otvor pro kartu druhého řidiče)


závada displeje


závada stahování dat

závada tiskárny


závada snímače

závada celku ve vozidle

Proces ručního zadání


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 tiskový blok nebo identifikátory záznamového zařízení jsou uvedeny v dodatku 4.

Dodatek 4

VÝTISKY

OBSAH

1. **VŠEOBECNĚ**

Každý výtisk sestává z řetězce bloků různých údajů, které je možné rozlišit identifikátorem bloku.

Údaje v bloku obsahují jeden nebo více záznamů, které je možné rozlišit identifikátorem záznamu.

PRT_001 Pokud identifikátor bloku bezprostředně předchází identifikátoru záznamu, identifikátor záznamu se netiskne.

PRT_002 Není-li určitá informace známa nebo nemůže být vytištěna z důvodů právna přístupu k ní, je místo ní vytištěna mezera.

PRT_003 Není-li obsah celé řádky nebo nemůže být vytištěn, vynechá se celá řádka.

PRT_004 Číselná data se vytisknou se zarovnáním vpravo s mezerami mezi tisíci a miliony a bez nul na začátku.

PRT_005 Alfanumerická data se vytisknou se zarovnáním vlevo doplněny mezerami pro dosažení požadované délky datového článku zkrácené z téhož důvodu (jména a adresy)

2. **SPECIFIKACE DATOVÝCH BLOKŮ**

V této kapitole je použit tento formát:

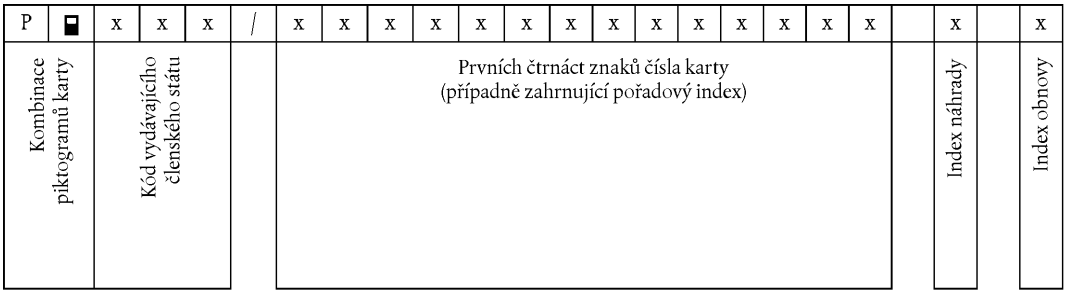
— znaky vytištěné **tučně** znamenají prostý text uvedený v tisku (výtisk je normálními znaky),

— normální znaky označují proměnné (piktogramy nebo údaje), pro vytištění jsou nahrazeny svými hodnotami,

— názvy proměnných byly podtrženy, aby se ukázala délka datového článku k dispozici pro proměnnou,

— datum je uváděno ve tvaru ‚dd/mm/yyyy' (den/měsíc/rok). Tvar ‚dd.mm.yyyy' se též smí použít.

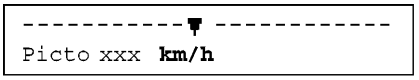
— termín ‚identifikace karty' označuje skladbu: typu karty pomocí kombinace piktogramů, kódu členského státu vydávajícího kartu, znaku lomítka, čísla karty, indexu náhrady a indexu obnovy oddělených mezerami:



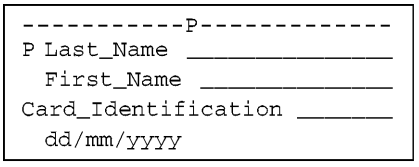
PRT_006 Výtisky musí použít následující bloky údajů nebo záznamy údajů v souladu s následujícími významy a formáty

Blok nebo záznam čísla Význam	Data Format
1. **Datum a čas, kdy byl dokument vytištěn**	dd/mm/yyyy hh:mm **(UTC)**

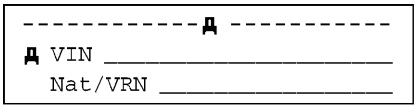
2. **Typ výtisku**
Identifikátor bloku
Vytištěná kombinace piktogramů (viz dodatek 3). Nastavení omezovače rychlosti (vytištění pouze překročení povolené rychlosti)



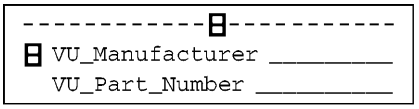
3. **Označení držitele karty**
Identifikátor bloku, P = piktogram lidí
Příjmení držitele karty
Jméno (a) držitele karty (pokud existují)
Identifikace karty
Datum konce platnosti karty
Je-li karta není osobní a neobsahuje příjmení držitele, musí být místo něj vytištěno jméno podniku nebo dílny nebo kontrolního orgánu.



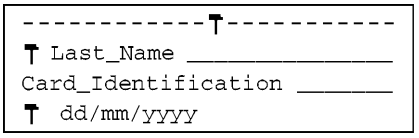
4. **Identifikace vozidla**
Identifikátor bloku
(identifikační číslo vozidla)
Členský stát registrace a registrační číslo vozidla



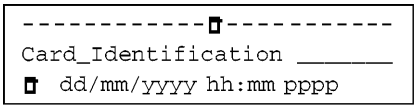
5. **Identifikace celku ve vozidle**
Identifikátor bloku
Název výrobce celku ve vozidle
číslo celku ve vozidle



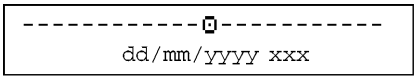
6. **Poslední kalibrace záznamového zařízení**
Identifikátor bloku
Název dílny
Identifikace karty dílny
Datum kalibrace



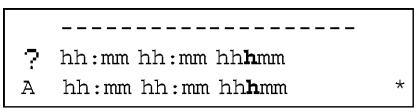
7. **Poslední kontrola (kontrolním úředníkem)**
Identifikátor bloku
Identifikace karty kontrolora
Datum, čas a typ kontroly
Typ kontroly; do čtyř piktogramů. Typ kontroly může být: vyprázdnění karty, vyprázdněním VJ, vytištěním, zobrazením na displeji (nebo jejich kombinací)
: stahování dat karty, : stahování dat, : výtisk,
: zobrazení



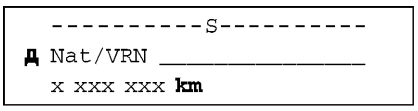
8. **Činnosti řidiče zaznamenané na kartě v pořadí událostí**
Identifikátor bloku
Datum šetření (kalendářní den výtisku) + denní karta počítadla



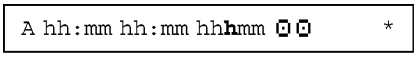
8.1 *Doba, po níž nebyla karta vložena*
8.1a Identifikátor záznamu (začátek časového úseku)
8.1b Neznámá doba. Začátek, konec a trvání
8.1c *Ručně vložené činnosti*
Piktogram činnosti, začátek, konec a trvání alespoň jednohodinové doby odpočinku jsou označeny hvězdičkou



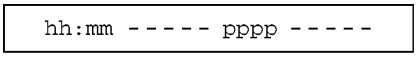
8.2 *Vložení karty do otvoru pro kartu S*
Identifikátor záznamu, Piktogram otvoru pro kartu
Členský stát, který vozidlo registruje a registrační číslo vozidla
Stav tachometru při vložení karty



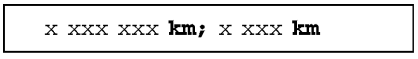
8.3 *Činnosti (po vložení karty)*
Piktogram činnosti, začátek, konec a trvání Stav posádky (piktogram posádky, pokud je, jinak prázdné místo), alespoň jednohodinové doby odpočinku jsou označeny hvězdičkou



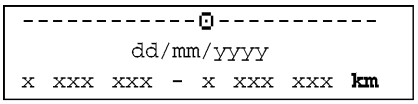
8.3a Specifické podmínky. Čas vstupu, piktogram specifické podmínky (nebo kombinace piktogramů)



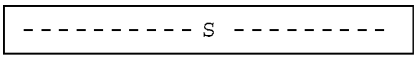
8.4 *Vyjmutí karty*
Stav tachometru vozidla a ujetá vzdálenost od posledního zasunutí, s ohledem na tehdejší stav tachometru



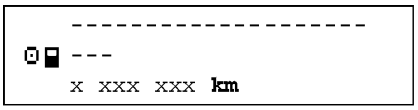
9. **Činnosti řidiče zaznamenané v celku ve vozidle za otvor pro kartu v chronologickém pořadí**
Identifikátor bloku
Datum šetření (kalendářní den výtisku)
Stav tachometru v 00:00 a 24:00



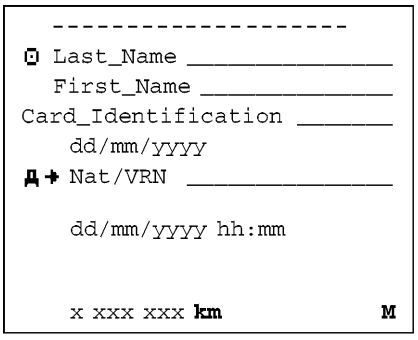
10. **Činnosti uvedené v otvoru pro kartu S**
Identifikátor bloku



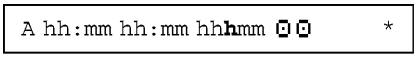
10.1 *Doba po kterou nebyla karta vložena do otvoru pro kartu S*
Identifikátor záznamu
Žádná karta nevložena
Stav tachometru na začátku doby



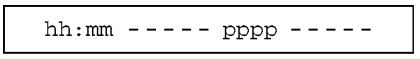
10.2 *Vložení karty*
Identifikátor záznamu vložení karty
Příjmení řidiče
Jméno(a) řidiče
Identifikační karta řidiče
Datum konce platnosti karty řidiče
Členský stát registrace a registrační číslo předtím používaného vozidla
Datum a čas vyjmutí karty z předtím používaného vozidla
Prázdná řádka
Stav tachometru při zasunutí karty, ruční zadání kolonky činnosti řidiče (M pokud je, prázdné pokud není)



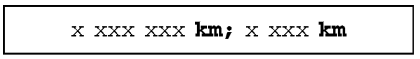
10.3 *Činnost*
Piktogram činnosti, začátek, konec a trvání Stav posádky (piktogram posádky, pokud je, jinak prázdné místo), alespoň jednohodinové doby odpočinku jsou označeny hvězdičkou



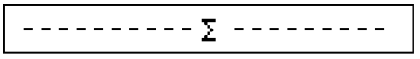
10.3a *Specifické podmínky.* Čas vstupu, piktogram specifické podmínky (nebo kombinace piktogramů)



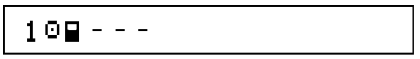
10.4 *Vyjmutí karty nebo konec doby bez použití karty*
Stav tachometru vozidla při vyjmutí karty nebo na konci doby bez použití karty a ujetá vzdálenost od posledního zasunutí nebo od začátku doby bez použití karty



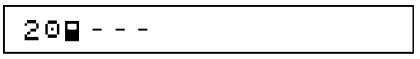
11. **Denní součet**
Identifikátor bloku



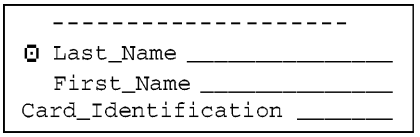
11.1 *Součet dob celku ve vozidle bez karty v otvoru pro kartu řidiče*
Identifikátor bloku



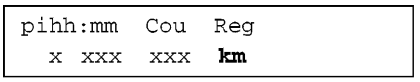
11.2 *Součet dob celku ve vozidle bez karty v otvoru pro kartu druhého řidiče*
Identifikátor bloku



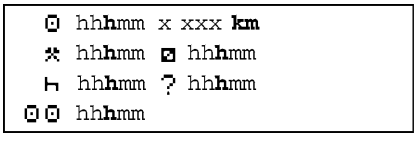
11.3 *Denní součet celku ve vozidle připadající na řidiče*
Identifikátor záznamu
Příjmení řidiče
Jméno (a) řidiče
Identifikační karta řidiče



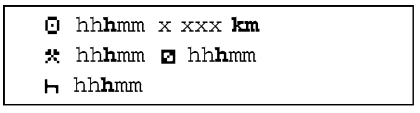
11.4 *Vstupní místo, kde denní pracovní doba začíná nebo končí*
pi = umístění piktogramu začátku/konce, čas, země, region.
Měřič ujeté vzdálenosti



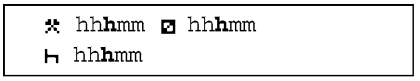
11.5 *Celkové činnosti (z karty)*
Celková doba řízení, ujetá vzdálenost
Celková doba práce a dosažitelnosti
Celková doba odpočinku a nevyužitelnosti
Celková doba činnosti posádky



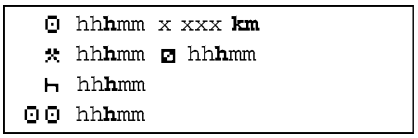
11.6. *Celkové činnosti (v době bez karty v otvoru pro kartu řidiče)*
Celková doba řízení, ujetá vzdálenost
Celková doba práce a dosažitelnosti
Celková doba odpočinku



11.7 *Celkové činnosti (v době bez karty v otvoru pro kartu druhého řidiče)*
Celková doba práce a dosažitelnosti
Celková doba odpočinku



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



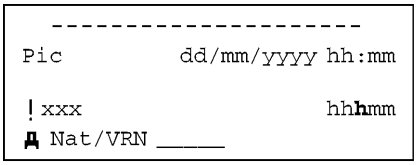
12. **Události nebo závady zaznamenané na kartě**

12.1 Identifikátor bloku posledních 5 ‚událostí a závad' na kartě

12.2 Identifikátor bloku všech ‚událostí' zaznamenaných na kartě

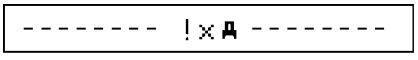
12.3 Identifikátor bloku všech ‚závad' zaznamenaných na kartě

12.4 *Záznam událostí nebo závad*
Identifikátor záznamu
Piktogram události nebo závady, účel záznamu, datum čas počátku
Případný dodatečný kód události nebo závady, trvání
Členský stát registrace a registrační číslo vozidla, v kterém k události nebo závadě došlo

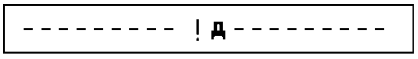


13. **Události nebo závady zaznamenané nebo probíhající v celku ve vozidle**

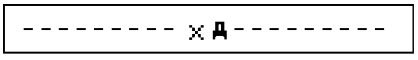
13.1 Identifikátor bloku posledních 5 ‚událostí a závad' z celku ve vozidle



13.2 Identifikátor bloku všech zaznamenaných nebo probíhajících ‚událostí' v celku ve vozidle

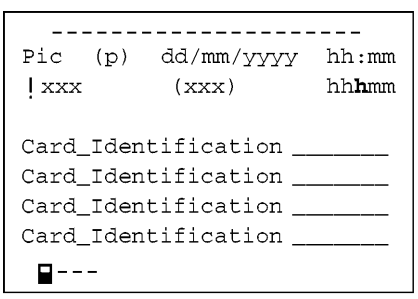


13.3 Identifikátor bloku všech zaznamenaných nebo probíhajících ‚závad' v celku ve vozidle

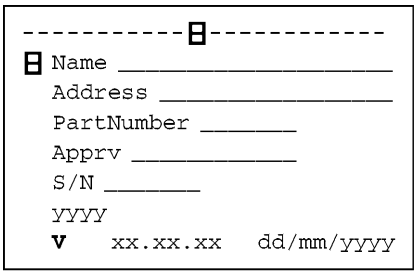


13.4 *Záznam událostí nebo závad*
Identifikátor záznamu
Piktogram události nebo závady, účel záznamu, datum a čas zařátku
Případný dodatečný kód události nebo závady, poznámka o podobných událostech téhož dne, trvání
Identifikace karet vložených na počátku nebo konci události nebo závady, až 4 řádky, bez opakování dvojice stejných čísel karty
Případ, kdy nebyla vložena žádná karta

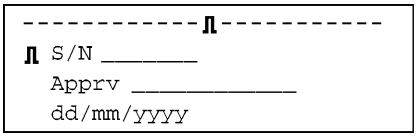
Účel záznamu (p) je numerický kód vysvětlující, proč byla událost nebo závada zaznamenána, kódování je v souladu s datovým prvkem `EventFaultRecordPurpose`



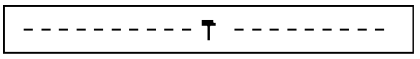
14. **Identifikace celku ve vozidle**
Identifikátor bloku
Název výrobce celku ve vozidle
Adresa výrobce celku ve vozidle
Číslo celku ve vozidle
Číslo schválení typu celku ve vozidle
Výrobní číslo celku ve vozidle
Rok výroby celku ve vozidle
Verze programového vybavení a datum instalace celku ve vozidle



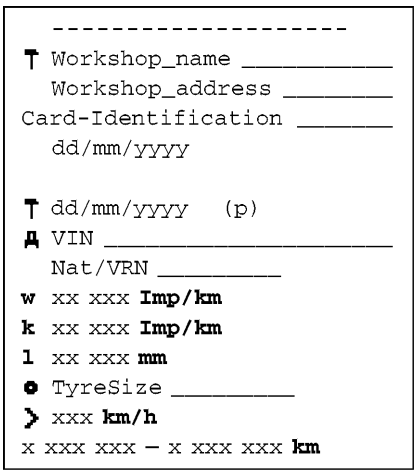
15. **Identifikace snímače**
Identifikátor bloku
Výrobní číslo snímače
Číslo schválení typu snímače
Datum první instalace snímače



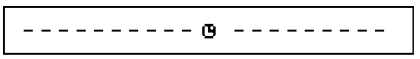
16. **Údaje o kalibraci**
Identifikátor bloku



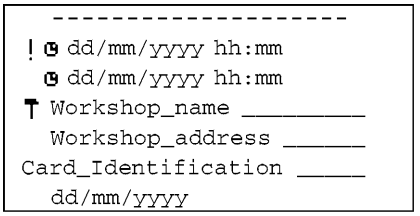
16.1 *Kalibrační záznam*
Identifikátor záznamu
Dílna, která provedla kalibraci
Adresa dílny
Identifikační karta dílny
Datum konce platnosti karty dílny
Prázdný řádek
Datum kalibrace + účel kalibrace
Identifikační číslo vozidla
Členský stát registrace a registrační číslo vozidla
Charakteristický koeficient vozidla
Konstanty záznamového zařízení
Efektivní obvod pneumatik kol
Rozměr použitých pneumatik
Staré a nové hodnoty měřiče ujeté vzdálenosti
Účel záznamu (p) je numerický kód vysvětlující, proč byly kalibrační parametry zaznamenány, kódování je v souladu s datovým prvkem `CalibrationPurpose`



17. **Časové nastavení**
Identifikátor bloku



17.1 *Záznam časového nastavení*
Identifikátor záznamu
Původní datum a čas
Nové datum a čas
Déílna, která provedla časové nastavení
Adresa dílny
Identifikační karta dílny
Datum konce platnosti karty dílny



18. **Poslední události a závady zaznamenané v celku ve vozidle**

Identifikátor bloku

Datum a čas poslední události

Datum a čas poslední závady

```
---------- !×🚙----------
!  jj/mm/aaaa  hh:mm
×  jj/mm/aaaa  hh:mm
```

19. **Informace o kontrole překročení povolené rychlosti**

Identifikátor bloku

Datum a čas poslední kontroly překročení POVOLENÉ rychlosti

Datum a čas prvního překročení povolené rychlosti a počet překročení povolené rychlosti od té doby

```
-----------►► ----------
►□ dd/mm/yyyy  hh:mm
►► dd/mm/yyyy  hh:mm (nnn)
```

20. **Záznam překročení povolené rychlosti**

20.1 Identifikátor bloku ‚První překročení povolené rychlosti po poslední kalibraci'

```
-------- ►►T --------
```

20.2 Identifikátor bloku ‚5 nejvážnějších překročení v posledních 365 dnech'

```
------- ►►(365)-------
```

20.3 Identifikátor bloku ‚Nejvážnější překročení v každém z posledních 10 dnů'

```
------- ►►(10) -------
```

20.4 Identifikátor záznamu

Datum, čas a trvání

Maximální a průměrné rychlosti, poznámka o podobných událostech téhož dne

Příjmení řidiče

Jméno (a) řidiče

Identifikační karta řidiče

```
   ------------------
►► dd/mm/yyyy hh:mm hhhmm
   xxx km/h xxx km/h (xxx)
Ⓘ  Last_Name _____________
   First_Name _____________
Card_Identification _______
```

20.5 Pokud není v bloku žádný záznam o překročení povolené rychlosti

```
►► - - -
```

21. **Informace zadané z klávesnice**

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' Vložte dostatek prázdných řádků nad položku pro psaní rukou, aby bylo skutečně možné napsat požadované informace nebo se podepsat.

```
------------------------
□●  ....................
□   ....................
◷+  ....................
+◷  ....................
Ⓘ   ....................
```

3. SPECIFIKACE VÝTISKŮ

V této kapitole je použit tento formát:

N	Tisk bloku nebo záznamu čísla N
N	Tisk bloku nebo záznamu čísla N dle potřeby opakovaný
X/Y	Tisk bloků nebo záznamů X nebo Y dle potřeby a dle nutnosti opakovaný

3.1 **Výpis denní činnosti řidiče z karty**

PRT_007 Výpis denní činnosti řidiče z karty musí mít následující formát

1	Datum a čas, kdy byl dokument vytištěn
2	Typ výtisku
3	Identifikace kontrolora (pokud je kontrolní karta vložena v celku ve vozidle)
3	Identifikace řidiče (z výtisku karty)
4	Identifikace vozidla (vozidla, z něhož byl výtisk získán)
5	Identifikace celku ve vozidle (celek ve vozidle, z nějž byl výtisk získán)
6	Poslední kalibrace tohoto celku ve vozidle
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 nebo závad (Posledních 5 událostí nebo závad zaznamenaných na kartě
13.1	Události a chyby podle vymezení celku ve vozidle
13.4	Záznamy událostí nebo závad (Posledních 5 událostí nebo závad zaznamenaných nebo probíhajících v celku ve vozidle)
21.1	Místo kontroly
21.2	Podpis kontrolora
21.5	Podpis řidiče

3.2 **Výpis denní činnosti řidiče z celku ve vozidle**

PRT_008 Výpis denní činnosti řidiče z celku ve vozidle musí mít následující formát

1	Datum a čas, kdy byl dokument vytištěn
2	Typ výtisku
3	Identifikace držitele karty (všech karet vložených do celku ve vozidle)
4	Identifikace vozidla (vozidla, z něhož byl výtisk získán)
5	Identifikace celku ve vozidle (celek ve vozidle, z nějž byl výtisk získán)
6	Poslední kalibrace tohoto celku ve vozidle
7	Poslední kontrola tohoto záznamového zařízení
9	Vymezení činností řidiče
10	Vymezení otvoru pro kartu řidiče (1)
10.1 / 10.2 / 10.3 /10.3a / 10.4	Činnosti v časovém sledu (otvor pro kartu řidiče)
10	Vymezení otvoru pro kartu druhého řidiče (2)
10.1 / 10.2 / 10.3 /10.3a / 10.4	Činnosti v časovém sledu (otvor pro kartu 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 druhého řidiče	
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 nebo závad	
13.4	Záznamy událostí nebo závad (posledních 5 událostí nebo závad zaznamenaných nebo probíhajících v celku ve vozidle)	
21.1	Místo kontroly	
21.2	Podpis kontrolora	(místo k dispozici řidiči bez karty pro uvedení období, která se ho týkají)
21.3	Počáteční čas	
21.4	Konečný čas	
21.5	Podpis řidiče	

3.3 **Výtisk událostí a závad z karty**

PRT_009 Výtisk událostí a závad z karty musí mít následující formát

1	Datum a čas, kdy byl dokument vytištěn
2	Typ výtisku
3	Identifikace kontrolora (pokud je kontrolní karta vložena v celku ve vozidle)
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 závad
12.4	Záznamy závad (všechny závady zaznamenané na kartě)
21.1	Místo kontroly
21.2	Podpis kontrolora
21.5	Podpis řidiče

3.4 **Výtisk událostí a závad z celku ve vozidle**

PRT_010 Výtisk událostí a závad z celku ve vozidle musí mít následující formát

1	Datum a čas, kdy byl dokument vytištěn
2	Typ výtisku
3	Identifikace držitele karty (všech karet vložených do celku ve vozidle)
4	Identifikace vozidla (vozidla, z něhož byl výtisk získán)
13.2	Vymezení událostí
13.4	Záznamy událostí (všechny události zaznamenané nebo probíhající v celku ve vozidle)
13.3	Vymezení závad
13.4	Záznamy závad (všechny závady zaznamenané nebo probíhající v celku ve vozidle)
21.1	Místo kontroly
21.2	Podpis kontrolora
21.5	Podpis řidiče

3.5 **Výpis technických údajů**

PRT_011 Výpis technických údajů musí mít následující formát

1	Datum a čas, kdy byl dokument vytištěn
2	Typ výtisku
3	Identifikace držitele karty (všech karet vložených do celku ve vozidle)
4	Identifikace vozidla (vozidla, z něhož byl výtisk získán)
14	Identifikace celku ve vozidle
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 v celku ve vozidle

3.6 **Výtisk překročení povolené rychlosti**

PRT_012 Výtisk překročení povolené rychlosti musí mít následující formát

1	Datum a čas, kdy byl dokument vytištěn
2	Typ výtisku
3	Identifikace držitele karty (všech karet vložených do celku ve vozidle)
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 nejvážnějších překročení povolené rychlosti v posledních 365 dnech
20.3	Identifikátor údajů o překročení povolené rychlosti
20.4 / 20.5	Nejvážnější překročení povolené rychlosti v každém z posledních 10 dnů
21.1	Místo kontroly
21.2	Podpis kontrolora
21.5	Podpis řidiče

Dodatek 5

DISPLEJ

V tomoto dodatku je použit tento formát:

— znaky vytištěné **tučně** znamenají jednoduchý text uvedený na displeji (zobrazení 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 závad
O:	piktogram provozního režimu

DIS_001 Záznamové zařízení musí zobrazovat na displeji data v následujícím formátu

Data	Format
Chybové zobrazení	
Místní čas	hh:mm
Provozní režim	O
Informace o řidiči	1 Dhh**h**mm ▮▮hh**h**mm
Informace o druhém řidiči	2 Dhh**h**mm
Mimo působnost	OUT
Varovná zobrazení	
Překročení nepřetržité doby řízení	1 0 hh**h**mm ▮▮hh**h**mm
Událost nebo závada	EF
Další zobrazení	
Datum UTC	UTC dd/mm/yyyy nebo UTC dd.mm.yyyy
Čas	hh:mm
Doba nepřetržitého řízení řidiče a souhrnná doba přestávek	1 0 hh**h**mm ▮▮hh**h**mm
Doba nepřetržitého řízení druhého řidiče a souhrnná doba přestávek	2 0 hh**h**mm ▮▮hh**h**mm
Souhrnná doba řízení řidiče v předchozím a probíhajícím týdnu	1 0 ‖ hhh**h**mm
Souhrnná doba řízení druhého řidiče v předchozím a probíhajícím týdnu	2 0 ‖ hhh**h**mm

Dodatek 6

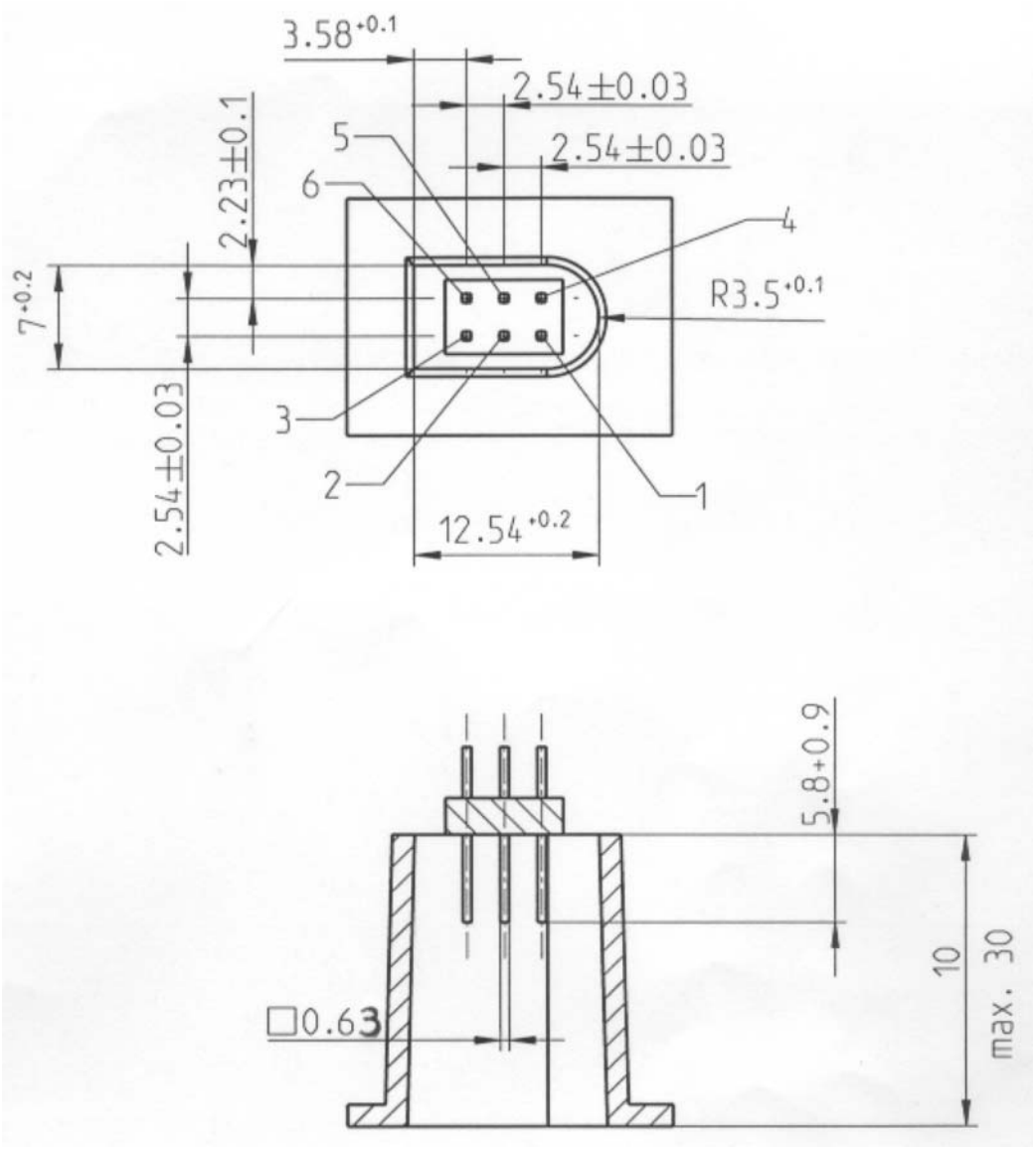
VNĚJŠÍ ROZHRANÍ

OBSAH

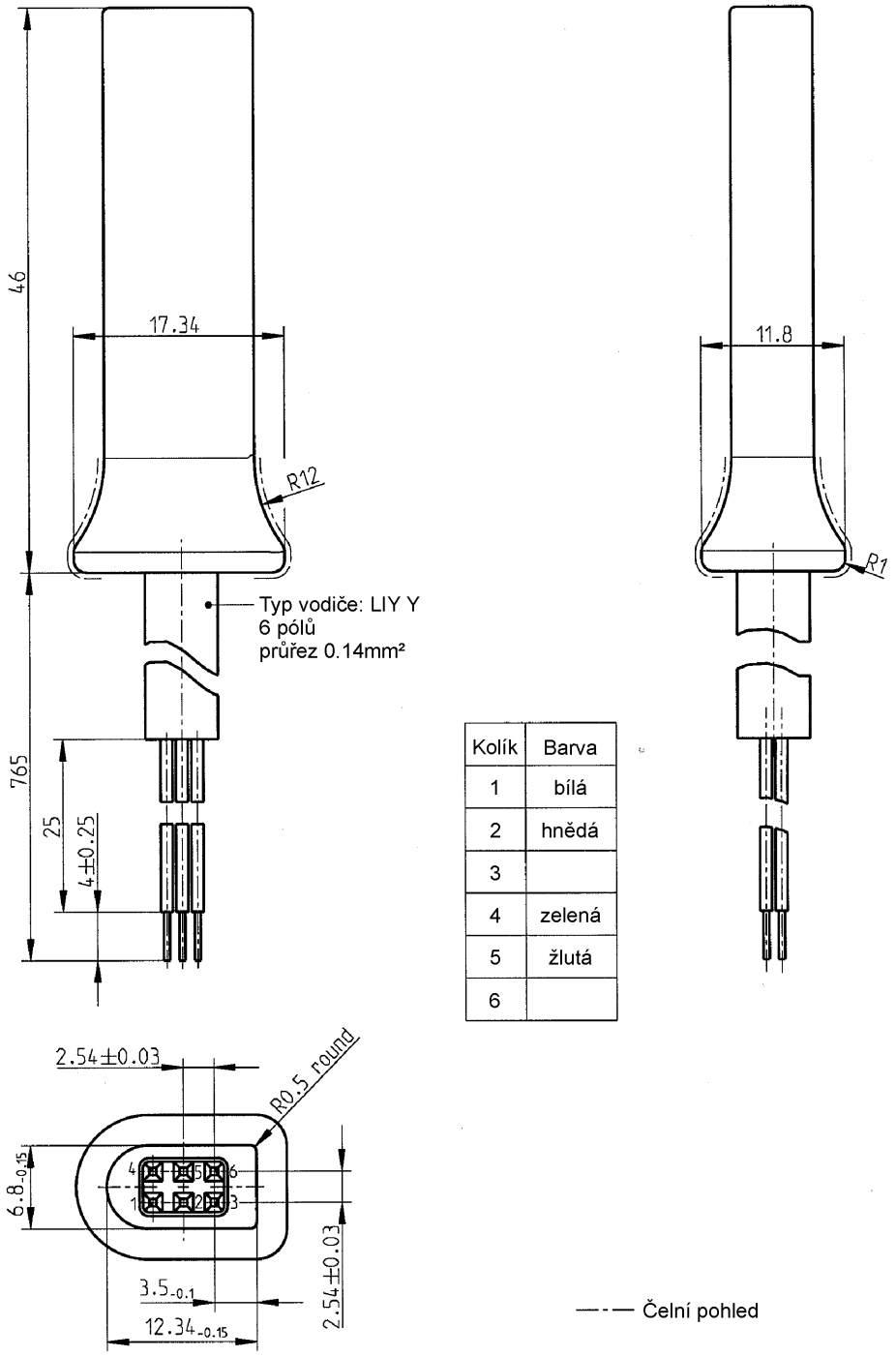
1. TECHNICKÉ VYBAVENÍ

1.1 **Konektor**

INT_001 Konektor pro stažení dat/kalibraci musí být šestikolíkový, přístupný na předním panelu bez nutnosti odpojení jakékoli části záznamového zařízení a musí odpovídat následujícímu výkresu (všechny rozměry jsou uvedeny v milimetrech):



Tento obrázek znázorňuje typickou šestikolíkovou zástrčku.



Kolík	Barva
1	bílá
2	hnědá
3	
4	zelená
5	žlutá
6	

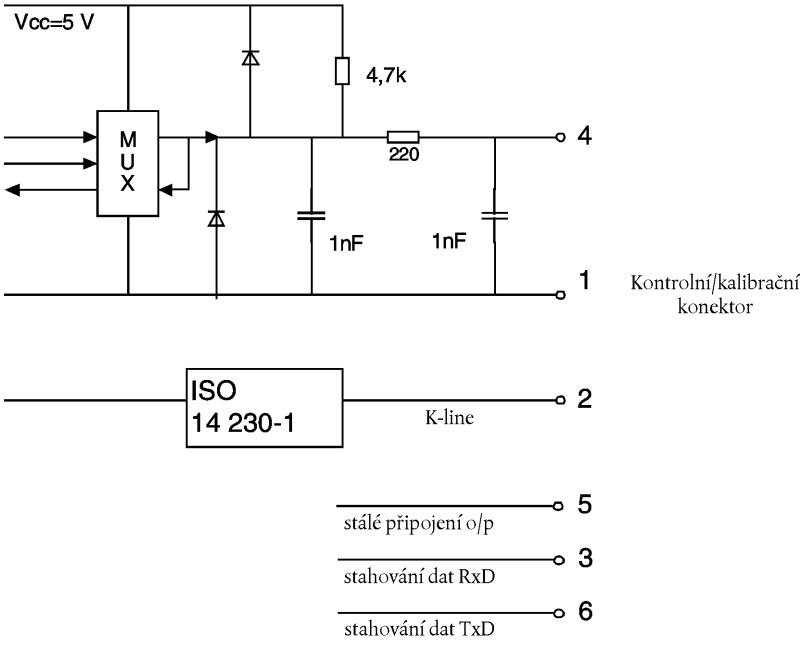
1.2 **Propojení kontaktů**

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:



2. ROZHRANÍ PRO STAŽENÍ DAT

INT_004 Rozhraní pro stažení dat musí splňovat specifikaci RS232

INT_005 Rozhraní pro stažení dat musí použít jeden spouštěcí bit (puls), 8 datových bitů LSB, jeden bit sudé parity a 1 koncový bit.

Uspořádání datových bitů

Spouštěcí bit: jeden bit s logickou hladinou 0

Datové bity: přenášené s LSB jako prvním

Paritní bit: sudá parita

Koncový bit: jeden bit s logickou úrovní 1

Když jsou přenášena numerická data tvořená více než jedním bajtem, nejvýznamnější bajt je přenesen nejdříve a následně jsou přenášeny nejméně významné bajty.

INT_006 Přenosová rychlost musí být nastavitelná od 9 600 bps do 115 200 bps. Přenos musí být uskutečnitelný při nejvýše možných přenosových rychlostech, počáteční rychlost po začátku komunikace se nastaví na 9 600 bps.

3. ROZHRANÍ PRO KALIBRACI

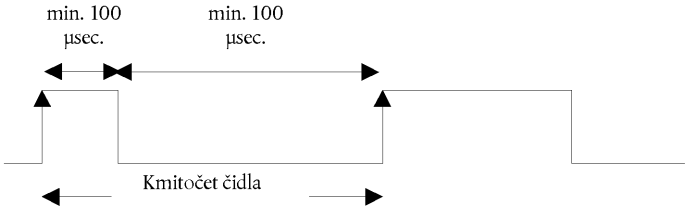
INT_007 Datová komunikace musí splňovat ISO 14230-1 Silniční vozidla — Diagnostické systémy — Protokol klíčových slov 2000 — Část 1: Fyzická vrstva, První vydání 1999

INT_008 Vstupní/výstupní signál musí splňovat následující specifikace:

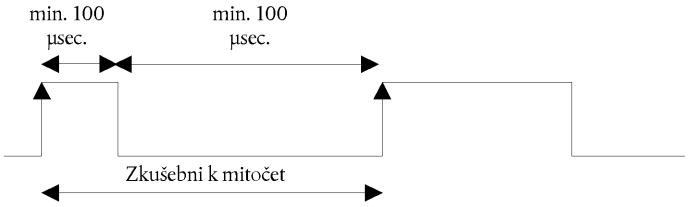
Parametr	Minimální	Typický	Maximální	Poznámka
U_N (vstupní)			1,0 V	I = 750 μA
U_V (vstupní)	4 V			I = 200 μA
Kmitočet			4 kHz	
U_N (vstupní)			1,0 V	I = 1 mA
U_V (výstupní)	4 V			I = 1 mA

INT_009 Vstupní/výstupní signál musí vyhovovat následujícím časovým diagramům:

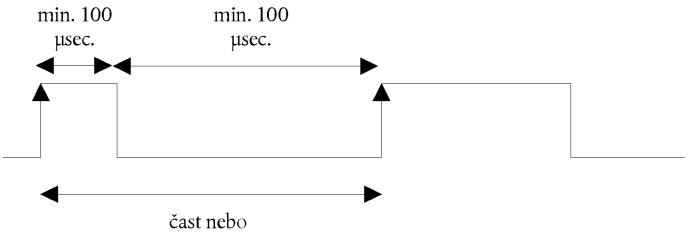
Signál z čidla (výstupní)



Zkušební signál (vstupní)



Časový signál UTC (výstupní) násobek jedné vteřiny



Dodatek 7

PROTOKOLY STAHOVÁNÍ DAT

OBSAH

1. ÚVOD

Tento dodatek určuje postup pro uložení různých typů stažených dat na externí paměťové médium společně s protokoly, které je nutno používat k zajištění správného přenosu dat a plné slučitelnosti formátu stažených dat, aby umožnilo kontrolorovi prozkoumání těchto dat a umožnilo kontrolu jejich totožnosti a úplnosti před analyzováním.

1.1 **Oblast působnosti**

Data se smí stáhnout na externí paměťové médium:

— z jednotky ve vozidle inteligentním zařízením (IDE) připojeným k jednotce ve vozidle,

— z karty tachografu přes IDE vybavené kartovým rozhraním,

— z karty tachografu přes jednotku ve vozidle a IDE připojeným k jednotce ve vozidle.

Pro možnost ověřit totožnost a úplnost stažených dat uložených na externí paměťové médium jsou data stažena s přiloženým podpisem v souladu s dodatkem 11 ‚Společné bezpečnostní mechanismy'. Identifikaci zdrojového zařízení (celek ve vozidle nebo karta) a jeho bezpečnostní osvědčení (členský stát a zařízení) se též stáhnou. Ověřovatel dat musí mít nezávisle v držení spolehlivý veřejný evropský klíč.

DDP_001 Stažená data během jednoho stahování musí být zapamatována v externím paměťovém médiu v jednom souboru.

1.2 **Zkratky a označování**

V tomto dodatku jsou použity následující zkratky:

AID	identifikátor aplikace
ATR	odpověď pro opětné spuštění
CS	bajt kontrolního součtu
DF	vyhrazený soubor
DS_	diagnostika
EF	základní soubor
ESM	externí paměťové médium
FID	identifikátor souboru
FMT	formátový bajt (první bajt hlavičky zprávy)
ICC	čipová karta
IDE	inteligentní zařízení: Zařízení používané k stažení dat do ESM (např. osobní počítač)
IFD	zařízení rozhraní
KWP	protokol klíčového slova 2000
LEN	délkový bajt (poslední bajt hlavičky zprávy)
PPS	výběr parametrů protokolu
PSO	provedení bezpečné činnosti
SID	identifikátor služby
SRC	zdrojový bajt
TGT	cílový bajt (bajt označující konec)
TLV	hodnota délky příznaku
TREP	parametr odezvy přenosu
TRTP	parametr požadavku přenosu
VU	celek ve vozidle

2. STAŽENÍ DAT CELKU VE VOZIDLE

2.1 **Postup stahování**

Aby se provedlo stažení dat VU, musí operátor provést následující činnosti:

— vsunout svou kartu tachografu do otvoru pro kartu VU ([1]),

— připojit IDE ke konektoru VU určenému pro stahování,

— zřídit 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 založena na vztahu hlavního zařízení IDE a podřízeného zařízení VU (master-slave).

Struktura zprávy, typy a tok jsou v zásadě založeny na Protokolu klíčového slova 2000(KWP) (ISO 14230-2 Silniční vozidla — Diagnostické systémy — Protokol klíčového slova 2000 — Část 2: Vrstva spojení dat).

Aplikační vrstva je v zásadě založena na projednávaném návrhu ISO 14229-1 (Silniční vozidla — Diagnostické systémy — Část 1: Diagnostické služby, verze 6 ze dne 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 formátového bajtu (FMT), cílového bajtu (TGT), zdrojového bajtu délkového bajtu (LEN).

— datové pole sestává z bajtu identifikátoru služby (SID) a různého počtu datových bajtů, které mohou obsahovat dle přání bajt diagnostiky nebo volitelný bajt přenosového parametru (TRTP nebo TREP).

— kontrolní součet sestávající z bajtu kontrolního součtu (CS).

Hlavička				Datové pole					Kontrolní součet
FMT	TGT	SRC	LEN	SID	DATA	…	…	…	CS
4 bajty				Max 255 bajtů					1 bajt

TGT a SRC bajt zastupuje fyzickou adresu příjemce a původce zprávy. Hodnoty jsou F0 Hex pro IDE a EE Hex pro VU.

Bajt LEN je délka části datového pole.

Bajt kontrolního součtu jsou osmibitové série modulo 256 ze všech bajtů zprávy vyjma samotného CS.

FMT, SID, DS, TRTP a TREP bajty jsou definovány dále v tomto dokumentu.

([1]) Vložená karta spustí příslušná přístupová práva k funkci stažení dat a k datům.

DDP_003 V případě, že dat, která mají být přenesena zprávou, je víc než dostupný prostor v části datového pole, je zpráva poslána v několika částech. Každá část nese hlavičku, stejný SID, TREP a 2 bajty počítadla zpráv ukazujícího číslo dílčí zprávy v celkové zprávě. Aby bylo umožněno ověření chyb a ztrát, potvrdí IDE každou dílčí zprávu. IDE může přijmout dílčí zprávu, požádat o to, aby byla znovu přenesena, nebo žádat VU o opětovný start nebo o zrušení přenosu.

DDP_004 Jestliže poslední část zprávy obsahuje přesně 255 bajtů z datového pole, musí se připojit koncová část s prázdným datovým polem (vyjma SID TREP a počítadla částí), aby se označil konec zprávy.

Příklad:

Hlavička	SID	TREP	Zpráva	CS
4 bajty	Delší než 255 bajtů			

Přenese se jako:

Hlavička	SID	TREP	00	01	Dílčí zpráva 1	CS
4 bajty	255 bajtů					

Hlavička	SID	TREP	00	01	Dílčí zpráva 2	CS
4 bajty	255 bajtů					

…

Hlavička	SID	TREP	xx	yy	Dílčí zpráva n	CS
4 bajty	Méně než 255 bajtů					

nebo jako

Hlavička	SID	TREP	00	01	Dílčí zpráva 1	CS
4 bajty	255 bajtů					

Hlavička	SID	TREP	00	02	Dílčí zpráva 2	CS
4 bajty	255 bajtů					

…

Hlavička	SID	TREP	xx	yy	Dílčí zpráva n	CS
4 bajty	255 bajtů					

Hlavička	SID	TREP	xx	yy+1	CS
4 bajty	4 bajty				

2.2.2 ***Typy zpráv***

Zápis z přenosu při stahování dat mezi VU a IDE požaduje výměnu osmi různých typů zpráv.

Následující tabulka uvádí přehled těchto zpráv

Struktura zprávy	Minimálně 4 bajty Hlavička				Maximálně 255 bajtů Data			1 bajt kontrolní součet
IDE -> <- VU	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		8F,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
Služba řízení spojení								
Ověření rychlosti přenosu v baudech (stav 1)								
9 600. Bd	80	EE	F0	04	87		01,01,01	EC
19 200. Bd	80	EE	F0	04	87		01,01,02	ED
38 400. Bd	80	EE	F0	04	87		01,01,03	ED
57 600. Bd	80	EE	F0	04	87		01,01,04	EF
115 200. Bd	80	EE	F0	04	87		01,01,05	F0
Kladná odezva ověření rychlosti přenosu	80	F0	EE	02	C7		01	28
Změna rychlosti přenosu (stav 2)	80	EE	F0	03	87		02,03	ED
Požadavek odeslání dat	80	EE	F0	0A	35		00,00,00, 00,00,FF,FF, FF,FF	99
Kladná odezva na požadavek odeslání dat	80	F0	EE	03	75		00,FF	D5
Požadavek na přenos dat								
Přehled	80	EE	F0	02	36	01		97
Činnosti	80	EE	F0	06	36	02	Datum	CS
Události a chyby	80	EE	F0	02	36	03		99
Rychlost podrobně	80	EE	F0	02	36	04		9A
Technická data	80	EE	F0	02	36	05		9B
Stažení karty	80	EE	F0	02	36	06		9C
Kladná odezva na přenos dat	80	F0	EE	Len	76	TREP	Data	CS
Požadavek na ukončení přenosu	80	EE	F0	01	37			96
Kladná odezva na požadavek ukončení	80	F0	EE	01	77			D6
Požadavek na ukončení spojení	80	EE	F0	01	82			E1
Kladná odezva na požadavek ukončení	80	F0	EE	01	C2			21
Potvrzení přijetí dílčí zprávy	80	EE	F0	Len	83		Data	CS
Záporné odezvy								
Úplné odmítnutí	80	F0	EE	03	7F	Sid Req	10	CS
Služba nepodporována	80	F0	EE	03	7F	Sid Req	11	CS
Dílčí funkce nepodporována	80	F0	EE	03	7F	Sid Req	12	CS
Nesprávná délka zprávy	80	F0	EE	03	7F	Sid Req	13	CS
Nesprávné podmínky nebo chybný požadavek úseku	80	F0	EE	03	7F	Sid Req	22	CS
Požadavek mimo rozsah	80	F0	EE	03	7F	Sid Req	31	CS
Odeslání neakceptováno	80	F0	EE	03	7F	Sid Req	50	CS
Nevyřízená odezva	80	F0	EE	03	7F	Sid Req	78	CS
Nedosažitelná data	80	F0	EE	03	7F	Sid Req	FA	CS

Poznámky:
— Sid Req = bajt SID souhlasného požadavku
— TREP = TRTP souhlasného požadavku
— Prázdná buňka znamená, že se nic nepřenáší
— Termín odeslání dat (z pohledu IDE) se používá z důvodu shodnosti s ISO 14229. To znamená totéž jako stažení dat (z pohledu VU).
— Možná 2bajtová počítadla dílčí zprávy nejsou v tabulce uvedena

2.2.2.1 *Požadavek na začátek spojení (SID 81)*

DDP_005 Tuto zprávu vydá zařízení IDE, aby zajistilo spojení s VU. Počáteční spojení vždy probíhají na 9 600 baudech (až do doby případné změny rychlosti přenosu vhodnou službou řízení spojení).

2.2.2.2 *Kladná odezva na začátek spojení (SID C1)*

DDP_006 Tato zpráva je vydána VU, aby kladně odpověděl na požadavek začátku spojení. Obsahuje 2 klíčové bajty ‚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 zařízení IDE, aby požádalo 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 zařízení IDE, aby vyvolalo změnu rychlosti přenosu v baudech. To probíhá ve dvou krocích. V kroku jedna navrhne IDE 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 přejde VU 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 na žádost o potvrzení se nedává žádná odezva (krok dvě).

2.2.2.7 *Požadavek na odeslání dat (SID 35)*

DDP_009 Zprávu o požadavku na odeslání dat vydává IDE, aby ukázalo VU, že je požadována činnost stahování dat. Pro splnění požadavků ISO 14229 jsou data uváděna 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 nezkomprimovaný a velikost paměti je nastavena na maximum.

2.2.2.8 *Kladná odezva na požadavek odeslání dat (SID 75)*

DDP_010 Zprávu o kladné odezvě na požadavek odeslání dat posílá VU, aby ukázal IDE, že VU je připraven 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 bajtů.

2.2.2.9 *Požadavek na přenos dat (SID 36)*

DDP_011 Zprávu o požadavku na přenos dat posílá IDE, aby ukázalo VU typ dat, která budou stahována. Jednobajtový parametr požadavku přenosu (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),

— stažení karty (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) obsahuje zpráva o požadavku stažení dat označení kalendářního dne `TimeReal` format ke stažení.

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 prvém případě (TREP 01) pošle VU data pomáhající operátoru IDE vybrat data, která chce dále stáhnout. Informace obsažené v této zprávě jsou:

— certifikace bezpečnosti,

— identifikace vozidla,

— datum a čas VU,

— minimální a maximální datum pro stažení (dat VU),

— indikace přítomnosti karet ve VU,

— předešlé stažení dat podnikem,

— zámky podniku,

— předešlé kontroly.

2.2.2.11 *Požadavek na ukončení přenosu (SID 37)*

DDP_013 Zprávu o požadavku na ukončení přenosu zasílá IDE, aby ukázalo 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 přerušilo 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 potvrdil příjem požadavku na ukončení spojení.

2.2.2.15 *Potvrzení příjmu dílčí zprávy*

DDP_017 Potvrzení příjmu dílčí zprávy zasílá IDE, aby potvrdilo stvrzenku každé části zprávy, která byla přenesena jako několik dílčích zpráv. Datové pole obsahuje SID obdržené od VU a následující dvoubajtové kódy:

— MsgC + 1 Potvrzení příjmu správné stvrzenky o počtu dílčích zpráv MsgC.

Požadavek od IDE na VU, aby poslal další dílčí zprávu.

— MsgC značí problém se stvrzenkou počtu dílčích zpráv MsgC.

Požadavek od IDE na VU, aby poslal dílčí zprávu znovu.

— FFFF požaduje ukončení zprávy.

Toto může použít IDE, aby z určitých důvodů ukončilo přenos zpráv VU.

Příjem poslední dílčí zprávy ze zprávy (bajt LEN < 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 nepodporována

Nebylo porozuměno SID požadavku.

— 12 dílčí funkce nepodporována

Nebylo porozuměno DS nebo TRTP požadavku nebo žádné další dílčí zprávy nebudou přenášeny.

— 13 nesprávná délka zprávy

Délka obdržené zprávy je chybná.

— 22 nesprávné podmínky nebo chyba úseku žádosti

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 včas a VU není připraven přijmout další požadavek.

— FA data nejsou k dispozici

Datový objekt požadavku přenosu dat není k dispozici ve VU (např. není vložená žádná karta…).

2.2.3 ***Tok zprávy***

Typický tok zprávy během normálního postupu stahování dat je následující:

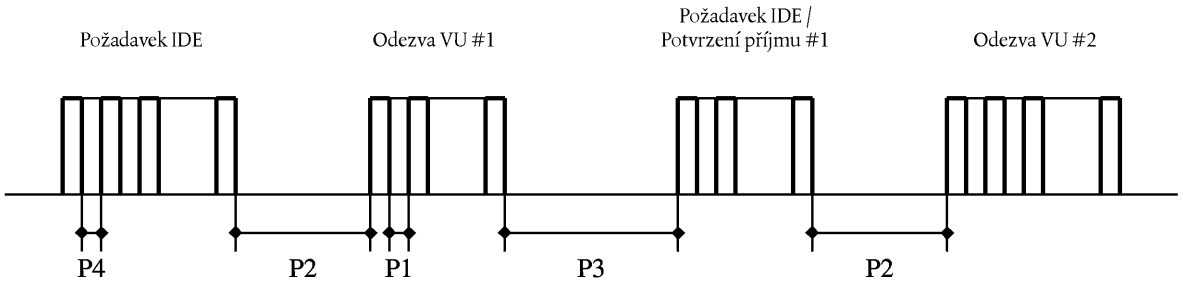
IDE		FE
Požadavek na začátek spojení	⇨	
	⇦	Kladná odezva
Požadavek na začátek diagnostiky	⇨	
	⇦	Kladná odezva
Požadavek na odeslání dat	⇨	
	⇦	Kladná odezva
Požadavek na přehled přenášených dat	⇨	
	⇦	Kladná odezva na přenos
Požadavek dat #2	⇨	
	⇦	Kladná odezva #1
Potvrzení přijetí dílčí zprávy #1	⇨	
	⇦	Kladná odezva #2
Potvrzení přijetí dílčí zprávy #2	⇨	
	⇦	Kladná odezva #m
Potvrzení přijetí dílčí zprávy #m	⇨	
	⇦	Kladná odezva (Datové pole < 255 bajtů)
Potvrzení přijetí dílčí zprávy (na přání)	⇨	
	…	
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 obrázku 1 jsou při normální činnosti důležité:

Obrázek 1

Tok zprávy, časování



Kde:

P1 = mezibajtový čas 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 nebo mezi koncem požadavku IDE a začátkem nového požadavku IDE, pokud VU nestačí odpovědět

P4 = mezibajtový čas pro požadavek IDE

P5 = rozšířená platnost P3 na stažení dat karty

Přípustné hodnoty parametrů časování jsou uvedeny v následující tabulce (rozšířený soubor parametrů časování KWP používaný v případě fyzického adresování kvůli rychlejšímu spojení).

Parametr časování	Spodní limitní hodnota (ms)	Horní limitní hodnota (ms)
P1	0	20
P2	20	1 000 (*)
P3	10	5 000
P4	5	20
P5	10	20 minut

(*) Pokud VU odpoví se zápornou odezvou obsahující kód s významem ‚požadavek správně přijat, odezva se očekává', je tato hodnota prodloužena na stejnou horní hodnotu P3

2.2.5 ***Zpracování chyb***

Pokud se objeví chyba při výměně zprávy, je schéma toku zprávy změněno v závislosti na zařízení, kterým byla chyba zjištěna, a na zprávě, jež chybu vyvolala.

Na obrázku 1 a obrázku 2 jsou uvedeny zvlášť pro VU a IDE postupy zpracování chyb.

2.2.5.1 *Fáze začátku spojení*

DDP_020 Pokud IDE zjistí chybu v průběhu začátku spojení buď časováním, nebo tokem bitů, počká po dobu P3 min před opětným vydáním požadavku.

DDP_021 Pokud VU zjistí chybu v úseku přicházejícím z IDE, neodešle žádnou odezvu a počká na následující zprávu o začátku spojení během doby P3 max.

2.2.5.2 *Fáze spojení*

Je možné definovat dvě různé oblasti zpracování chyb:

1. **VU zjistí chybu v přenosu IDE**

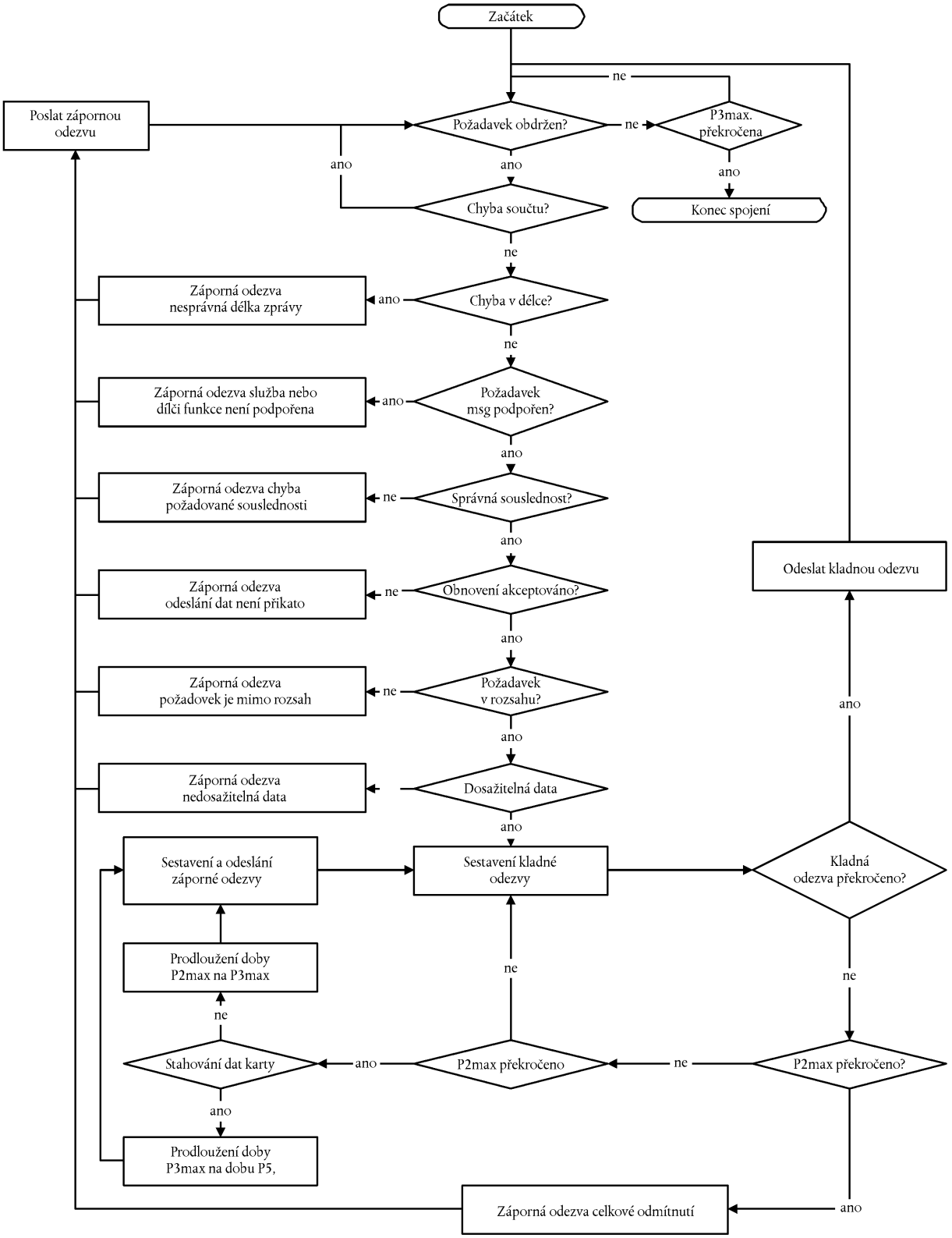
DDP_022 VU zjistí chyby v časování pro každou obdrženou zprávu, chyby ve formátu bajtů (např. porušení počátečního a koncového bitu) a rámcové chyby (chybný počet obdržených bajtů, chybný bajt kontrolního součtu).

DDP_023 Pokud VU zjistí jednu z výše uvedených chyb, 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 kontrolního součtu, a v takovém případě musí VU odpovědět IDE zprávou se zápornou odezvou určující povahu chyby.

Obrázek 2

Zpracování chyb VU



2. **IDE zjistí chybu v přenosu VU**

DDP_025 IDE zjistí chyby časování pro každou obdrženou zprávu, chyby ve formátu bajtů (např. porušení počátečního a koncového bitu) a rámcové chyby (chybný počet obdržených bajtů, chybný bajt kontrolního součtu).

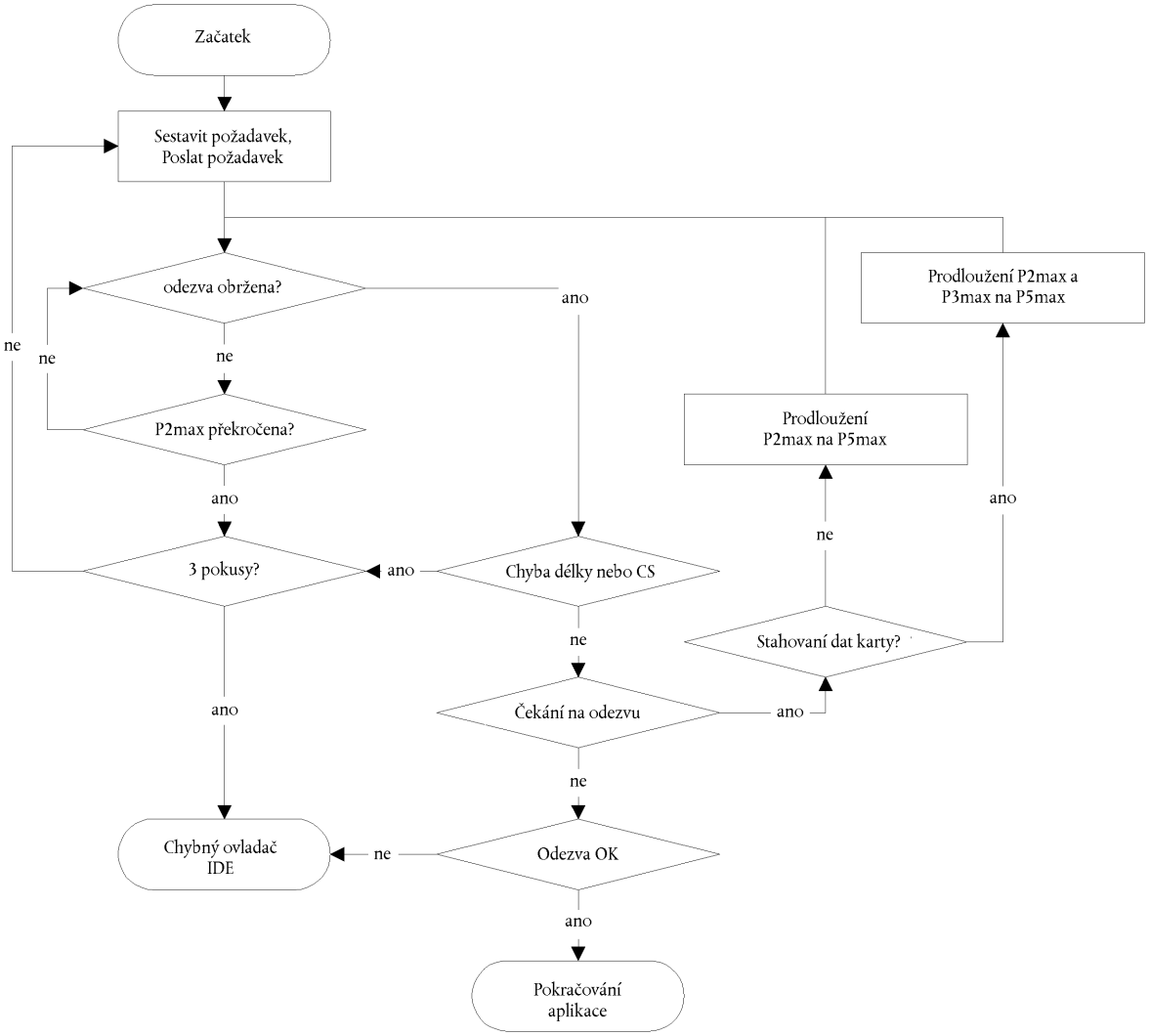
DDP_026 IDE zjistí chyby pořadí, např. nesprávná okénka dílčí zprávy v následujících obdržených zprávách.

DDP_027 Pokud IDE zjistí chybu nebo neobdrží odezvu od VU za čas P2max, pošle znova zprávu s požadavkem u celkem maximálně tří přenosů. Pro účely detekce této chyby se potvrzení příjmu dílčí zprávy považuje za požadavek na VU.

DDP_028 IDE počká alespoň po dobu P3min před začátkem každého přenosu, doba čekání se měří od posledně počítaného koncového bitu po zjištění chyby.

Obrázek 3

Zpracování chyb 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 dodatku 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 pořadí s SID 76 Hex, TREP 01 Hex a dílčí zprávou s vhodným dělením a řazením:

Datový prvek	Délka (bajty)	Komentář
MemberStateCertificate	194	Certfikát zabezpečení VU
VUCertificate	194	
VehicleIdentificationNumber	17	Identifikace vozidla
VehicleRegistrationIdentification		
vehicleRegistrationNation	1	
vehicleRegistrationNumber	14	
CurrentDateTime	4	Současné datum a čas
VuDownloadablePeriod		Perioda stažení dat VU
minDownloadableTime	4	
maxDownloadableTime	4	
CardSlotsStatus	1	Typ karet vložených do VU
VuDownloadActivityData		Předešlé stažení dat VU
downloadingTime	4	
fullCardNumber	18	
companyOrWorkshopName	36	
VuCompanyLocksData		Uložené zámky podniku. Pokud je tato sekce prázdná, odešle se jen noOfLocks = 0
noOfLocks	1	
...	(98)	
VuCompanyLocksRecord		
lockInTime	4	
lockOutTime	4	
companyName	36	
companyAddress	36	
companyCardNumber	18	
...		
VuControlActivityData		Všechny záznamy o kontrole uložené ve VU. Pokud je tato sekce prázdná, odešle se jen noOFControls = 0
noOfControls	1	
...	(31)	
VuControlActivityRecord		
controlType	1	
controlTime	4	
controlCardNumber	18	
downloadPeriodBeginTime	4	
downloadPeriodEndTime	4	
...		
Signature	128	RSA označení všech dat (vyjma certifikátů) začínají od VehicleIdentificationNumber po poslední bajt posledního záznamu VuControlActivityRecord

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 pořadí s SID 76 Hex, TREP 02 Hex a dílčí zprávou s vhodným dělením a řazením

Datový prvek	Délka (bajty)	Komentář
TimeReal	4	Datum dne stažení dat
OdometerValueMidnight	3	Stav měřiče vzdálenosti na konci dne stažení dat
VuCardIWData		Data cyklů vložení a vyjmutí karet.
noOfVuCardIWRecords	2	
...	(129)	— Pokud sekce neobsahuje dosažitelná data, odešle se jen noOfVuCardIWRecords = 0.
VuCardIWRecord: cardHolderName		— Pokud VuCardIWRecord přechází přes 00:00 (karta vsunuta předchozí den) nebo přes 24:00 (karta vyjmuta následující den), musí se objevit vše za celé dva dny
holderSurname	36	
holderFirstNames	36	
fullCardNumber	18	
cardExpiryDate	4	
cardInsertionTime	4	
vehicleOdometerValueAtInsertion	3	
cardSlotNumber	1	
cardWithdrawalTime	4	
vehicleOdometerValueAtWithdrawal	3	
previousVehicleInfo		
vehicleRegistrationIdentification		
vehicleRegistrationNation	1	
vehicleRegistrationNumber	14	
cardWithdrawalTime	4	
manualInputFlag	1	
...		
VuActivityDailyData		Stav otvorů pro kartu v 00:00 a změny činnosti zaznamenané pro stahovaný den
noOfActivityChanges	2	
...		
ActivityChangeInfo	2	
...		
VuPlaceDailyWorkPeriodData		Místa vztahující se k datům zaznamenaným pro stahovaný den. Pokud je sekce prázdná, odešle se jen noOfPlaceRecords = 0
noOfPlaceRecords	1	
...	(28)	
VuPlaceDailyWorkPeriodRecord: fullCardNumber	18	
placeRecord		
entryTime	4	
entryTypeDailyWorkPeriod	1	
dailyWorkPeriodCountry	1	
dailyWorkPeriodRegion	1	
vehicleOdometerValue	3	
...		
VuSpecificConditionData		Data specifických podmínek zaznamenaných pro stahovaný den. Pokud je sekce prázdná, odešle se jen noOfSpecificConditionRecords = 0
noOfSpecificConditionRecords	2	
...	(5)	
SpecificConditionRecord		
EntryTime	4	
specificConditionType	1	
...		
Signature	128	RSA označení všech dat začínají od TimeReal po poslední bajt posledního záznamu specifických 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 pořadí se SID 76 Hex, TREP 03 Hex a dílčí zprávou s vhodným dělením a řazením:

Datový prvek	Délka (bajty)	Komentář
VuFaultData		Všechny závady zaznamenané nebo probíhající ve VU. Pokud je sekce prázdná, odešle se jen NoOfFaults = 0
NoOfVuFaults	1	
...	(82)	
VuFaultRecord: FaultType	1	
VuFaultRecord: FaultRecordPurpose	1	
VuFaultRecord: FaultBeginTime	4	
VuFaultRecord: FaultEndTime	4	
VuFaultRecord: CardNumberDriverSlotBegin	18	
VuFaultRecord: cardNumberCodriverSlotBegin	18	
VuFaultRecord: CardNumberDriverSlotEnd	18	
VuFaultRecord: CardNumberCodriverSlotEnd	18	
...		
VuEventData		Všechny události (vyjma překročení povolené rychlosti) zaznamenané nebo probíhající ve VU. Pokud je sekce prázdná, odešle se jen NoOfVuEvents = 0
NoOfVuEvents	1	
...	(83)	
VuEventRecord: EventType	1	
VuEventRecord: EventRecordPurpose	1	
VuEventRecord: EventBeginTime	4	
VuEventRecord: EventEndTime	4	
VuEventRecord: CardNumberDriverSlotBegin	18	
VuEventRecord: cardNumberCodriverSlotBegin	18	
VuEventRecord: CardNumberDriverSlotEnd	18	
VuEventRecord: CardNumberCodriverSlotEnd	18	
VuEventRecord: SimilarEventsNumber	1	
...		
VuOverSpeedingControlData		Data vztažená k poslední kontrole překročení rychlosti (standardně bez dat)
LastOverspeedControlTime	4	
FirstOverspeedSince	4	
NumberOfOverspeedSince	1	
VuOverSpeedingEventData		Všechny události uložené ve VU. Pokud je sekce prázdná, odešle se jen NoOfVuOverSpeedingEvents = 0
NoOfVuOverSpeedingEvents	1	
...	(31)	
VuOverSpeedingEventRecord: EventType	1	
VuOverSpeedingEventRecord: EventRecordPurpose	1	
VuOverSpeedingEventRecord: EventBeginTime	4	
VuOverSpeedingEventRecord: EventEndTime	4	
VuOverSpeedingEventRecord: MaxSpeedValue	1	
VuOverSpeedingEventRecord: AverageSpeedValue	1	
VuOverSpeedingEventRecord: CardNumberDriverSlotBegin	18	
VuOverSpeedingEventRecord: SimilarEventsNumber	1	
...		
VuTimeAdjustmentData		Všechna nastavení času uložená ve VU (mimo rámec úplné kalibrace). Pokud je sekce prázdná, odešle se jen NoOfVuTimeAdjRecords = 0
NoOfVuTimeAdjRecords	1	
...	(98)	
VuTimeAdjustmentRecord: OldTimeValue	4	
VuTimeAdjustmentRecord: NewTimeValue	4	
VuTimeAdjustmentRecord: WorkshopName	36	
VuTimeAdjustmentRecord: WorkshopAddress	36	
VuTimeAdjustmentRecord: WorkshopCardNumber	18	
...		
Signature	128	RSA označení všech dat začínajících od NoOfFaults po poslední bajt posledního záznamu nastavení času.

2.2.6.4 *Kladná odezva přenosu dat detailní rychlosti*

DDP_032 Datové pole zprávy ‚kladná odezva přenosu dat detailní rychlosti' musí zajistit následující data v následujícím pořadí se SID 76 Hex, TREP 04 Hex a dílčí zprávou s vhodným dělením a řazením:

Datový prvek	Délka (bajty)	Komentář
VuDetailedSpeedData		
NoOfSpeedBlocks	2	Všechna nastavení času uložené do VU (mimo rámec úplné kalibrace). Pokud je sekce prázdná, odešle se jen NoOfSpeedBlocks = 0
...		
VuDeatailedSpeedBlock		
SpeedBlockBeginDate	4	
speedsPerSecond	60	
...		
Signature	128	RSA označení všech dat začínají od NoOfFaults po poslední bajt posledního záznamu nastavení času.

2.2.6.5 *Kladná odezva přenosu dat technických údajů*

DDP_033 Datové pole zprávy ‚kladná odezva přenosu dat technických údajů' musí zajistit následující data v následujícím pořadí se SID 76 Hex, TREP 05 Hex a dílčí zprávou s vhodným dělením a řazením:

Datový prvek	Délka (bajty)	Komentář
VuIdentification		
vuManufacturerName	36	
vuManufacturerAddress	36	
vuPartNumber	16	
vuSerialNumber	8	
vuSoftwareIdentification		
vuSoftwareVersion	4	
vuSoftInstallationDate	4	
vuManufacturingDate	4	
vuApprovalNumber	8	
SensorPaired		
sensorSerialNumber	8	
sensorApprovalNumber	8	
sensorPairingDateFirst	4	
VuCalibrationData		Všechny kalibrační záznamy uložené ve VU.
noOfVuCalibrationRecords	1	
...	(164)	
VuCalibrationRecord		
calibrationPurpose	1	
workshopName	36	
workshopAddress	36	
workshopCardNumber	18	
workshopCardExpiryDate	4	
vehicleIdentificationNumber	17	
vehicleRegistrationIdentification		
vehicleRegistrationNation	1	
vehicleRegistrationNumber	14	
wVehicleCharacteristicConstant	2	
kConstantOfRecordingEquipment	2	
lTyreCircumference	2	
tyreSize	15	
authorisedSpeed	1	
oldOdometerValue	3	
newOdometerValue	3	
oldTimeValue	4	
newTimeValue	4	
nextCalibrationDate	4	
...		
Signature	128	RSA označení všech dat začínají od vuManufacturerName po poslední bajt posledního kalibračního záznamu VU.

2.3 **Ukládání souboru na externí paměťové médium (ESM)**

DDP_034 Jestliže proces stahování zahrnuje přenos dat VU, musí IDE uložit do jednoho fyzického souboru všechna data obdržená z VU během stažení dat ze zpráv s kladnou odezvou na přenos dat. Uložená data vylučují hlavičky zprav, 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 **Oblast působnosti**

Tento odstavec popisuje přímé stahování dat z karty tachografu do IDE. IDE není součástí bezpečného prostředí, tudíž není prováděno žádné prokázání totožnosti mezi kartou a IDE.

3.2 **Definice**

Proces stahování dat: Každé stahování dat čipové karty (ICC). Proces obsahuje úplný postup od resetování ICC pomocí zařízení rozhraní (IFD) až po deaktivaci ICC (vyjmutí karty nebo dalšího resetování).

Značený datový soubor: Soubor od ICC. Soubor je převeden do IFD v jednoduchém textu. V ICC je soubor upraven a označen a označení je převedeno do IFD.

3.3 **Stažení dat karty**

DDP_035 Stažení dat karty tachografu zahrnuje následující kroky:

— Stažení dat běžných informací karty v základních souborech `ICC` a `IC`. Tyto informace jsou na přání a nejsou zabezpečeny digitálním podpisem.

— Stažení dat základních souborů `Card_Certificate` a `CA_Certificate`. Tato informace je zabezpečena digitálním podpisem.

Je povinné stáhnout data těchto souborů při každém procesu stahování dat.

— Stažení základních souborů dat další aplikace (z vyhrazeného souboru `TachogrÃf DF`) kromě základního souboru `Card_Download`. Tato informace je zabezpečena digitálním podpisem.

  — Je povinné stáhnout data alespoň základní soubor `Application_Identification` a `ID` pro každý proces stahování dat.

  — Při stahování dat karty řidiče je také povinné stáhnout data následující základní soubory:

    — `Events_Data`,

    — `Faults_Data`,

    — `Driver_Activity_Data`,

    — `Vehicles_Used`,

    — `Places`,

    — `Control_Activity_Data`,

    — `Specific_Conditions`.

— Při stahování dat karty řidiče, obnovte datum `LastCardDownload` v základním souboru `Card_Download`.

— Při stahování dat karty dílny resetujte kalibrační počítadlo v základním souboru `Card_Download`.

3.3.1 ***Inicializační sekvence***

DDP_036 IDE musí zahájit sekvenci takto:

Karta	Směr	IDE/IFD	Význam/Poznámky
	⇦	Resetování technického vybavení	
ATR	⇨		

Je možné zvolit použití PPS k přepnutí na vyšší přenosovou rychlost co nejdéle, pokud to podporuje ICC

3.3.2 ***Sekvence pro neoznačené soubory dat***

DDP_037 Sekvence pro stažení `ICC`, `IC`, `Card_Certificate` a `CA_Certificate` je následující:

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	v souladu s 3.4 (Formát uložených dat)

:Poznámka: Před vybráním EF `Card_Certificate` musí být vybrána aplikace tachografu (vybírá AID).

3.3.3 ***Sekvence pro označené soubory dat***

DDP_038 Následující sekvence má být použita pro každý z následujících souborů, které musí být staženy s podpisem:

Karta	Směr	IDE/IFD	Význam/Poznámky
	⇦	Výběr souboru	
OK	⇨		
	⇦	Transformace souboru	Určit hodnotu transformace podle obsahu dat vybraného souboru použitím předepsaného algoritmu transformace podle dodatku 11. Tento příkaz není ISO příkaz.
Vypočítat 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: a digitális aláírás kiszámítása	Určit hodnotu transformace podle obsahu dat vybraného souboru použitím předepsaného algoritmu rozsekání podle dodatku 11. Tento příkaz není ISO příkaz
Zabezpečit operaci ‚vypočítat digitální označení' dočasným uložením hodnoty transformace			
Označení OK	⇨	Přidat data k předešle uloženým do ESM	V souladu s 3.4 (formát uložených dat)

3.3.4 ***Sekvence při resetování kalibračního počítadla***

DDP_039 Souslednost při resetování počítadla `NoOfCalibrationsSinceDownload` v souboru `Card_Download` v dílně je následující:

Karta	Směr	IDE/IFD	Význam/Poznámky
OK	⇦ ⇨	Výběr souboru EF `Card_Download`	Výběr identifikátorem souboru
	⇦	Binární obnovení `NoOfCalibrationsSinceDownload` = '00 00'	
Resetovat počet stahování karty.			
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 bajtů a právě tak bitů uvnitř bajtu 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 bloků tlv.

DDP_042 Příznak pro EF musí být FID plus přípona ‚00'.

DDP_043 Příznak označení EF musí být FID souboru plus přípona ‚01'.

DDP_044 Délka je dvoubajtová hodnota. Hodnota ‚FF FF' je v délce pole rezervována pro budoucí použití.

DDP_045 Jestliže se soubor nestahuje, neukládá se pro daný soubor nic (žádný příznak a žádná nulová délka).

DDP_046 Označení se musí uložit jako příští objekt TLV hned za objekt TLV, který obsahuje data souboru.

Definice	Význam	Délka
FID (2 bajty) || ‚00'	Příznak pro EF (FID)	3 bajty
FID (2 bajty) || ‚01'	Příznak označení EF (FID)	3 bajty
xx xx	Délka pole hodnot	2 bajty

Příklad dat ve staženém souboru v ESM:

Příznak	Délka	Hodnota
00 02 00	00 11	Data `ICC` EF
C1 00 00	00 C2	Data `Card_Certificate` EF
		…
05 05 00	0A 2E	Data `Vehicles_Used` EF
05 05 01	00 80	Označení `Vehicles_Used` EF

4. STAHOVÁNÍ DAT KARTY TACHOGRAFU PŘES JEDNOTKU VE VOZIDLE

DDP_047 VU musí umožnit stažení obsahu dat karty řidiče, která je vložena do připojeného zařízení IDE.

DDP_048 IDE musí poslat zprávu ‚požadavek na přenos stažených dat karty' do VU, aby tuto činnost vyvolalo (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 určeném v odstavci 3 a směrovat 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 zpráv a kontrolních součtů) a uložit je v jednom fyzickém souboru jak předepisuje odstavec 2.3.

DDP_051 VU pak musí co nejvhodněji do současnosti obnovit `Control_Activity_Data` nebo soubor `Card_Download` karty řidiče.

Dodatek 8

KALIBRAČNÍ PROTOKOL

OBSAH

1. ÚVOD

Tento dodatek popisuje, jak se vyměňují data mezi celkem ve vozidle a zkušebním zařízením po vedení K, které 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 oblast působnosti řízení vedení K za různých podmínek. Předvoleným jednáním 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 být celek ve vozidle navíc v pracovním módu CALIBRATION (kalibrace).

Přenos dat po vedení K je popsán v části 6 ‚Služby přenosu dat'. Formáty přenášených dat jsou podrobně uvedeny v části 8 ‚Formáty záznamů dat'.

CPR_002 ‚ECUAdjustmentSession' (seřizovací jednání ECU) umožňuje volbu I/O módu (vstup/výstup) na kalibračním signálním vedení 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 dávána přednost adresám zkušebních zařízení, celek ve vozidle musí správně spolupracovat s kterýmkoliv zkušebním zařízením. Fyzická adresa celku ve vozidle 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 bajtové kódování a hexadecimální hodnoty.

Pojem ‚zkušební zařízení' se vztahuje na zařízení, užívané pro vstup programovacích nebo kalibračních dat do celku ve vozidle.

Pojmy ‚klient' a ‚server' se vztahují na zkušební zařízení a na celek ve vozidle.

Zkratka ECU znamená ‚Electronic Control Unit' (elektronický řídící celek) a vztahuje se na 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,

— 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,

— šestý sloupec stanovuje služby ‚ECUProgrammingSession' (ECUPS), které musí být zavedeny pro umožnění programování parametrů v celku ve vozidle.

Tabulka 1

Souhrnná tabulka hodnot identifikátoru služeb

			Diagnostické jednání		
Název diagnostické služby	Část č.	SID hodnota požadavku	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 serverem (servery)
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 označovacího prvku StartCommunication 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 odezvový prvek StartCommunication společně se zvolenými parametry kladné odezvy.

CPR_008 Pokud celek ve vozidle, který byl již inicializován (a který vstoupil do jakéhokoliv diagnostického jednání), obdrží nový požadavek StartCommunication (například 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 obdržením pokusu o inicializaci komunikačního spojení.

CPR_010 Požadavek zprávy StartCommunication musí být fyzicky adresován.

CPR_011 Inicializace celku ve vozidle proběhne postupem ‚rychlé inicializace‘,

— každé činnosti 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 bajtů na hodnoty definované v tabulce 4,

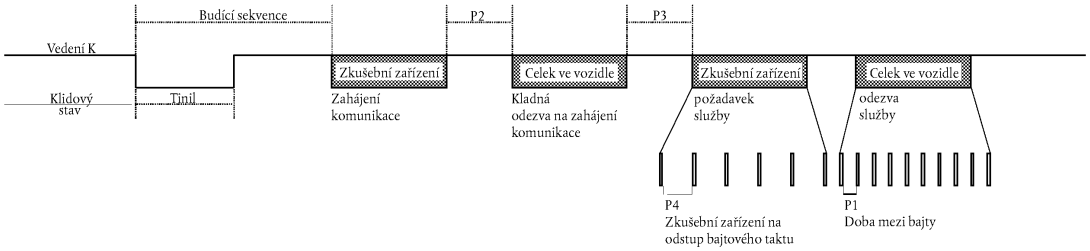
— celek ve vozidle vyčkává na první požadavek od zkušebního zařízení,

— celek ve vozidle je ve standardním diagnostickém módu, tj. StandardDiagnosticSession,

— kalibrace signálního spojení I/O je ve standardním stavu, tj. ve vyřazeném stavu.

CPR_014 Rychlost přenosu dat na vedení K musí být 10 400 baudů.

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 prvý bit ze StartCommunicationService následně po Twup taktu, který začíná po první sestupné hraně impulsu.



CPR_017 Hodnoty časování pro rychlou inicializaci a komunikaci jsou obecně rozepsány v níže uvedených tabulkách. Existují různé možnosti pro dobu klidu (idle):

— prvý přenos po zapojení napájení, T_{idle} = 300 ms,

— po dokončení služby StopCommunication, T_{idle} = P3 min,

— po zakončení komunikace v důsledku překročení doby P3max, T_{idle} = 0.

Tabulka 3

Hodnoty časování pro rychlou inicializaci

Parametr		Minimální hodnota	Maximální hodnota
Tinil	25 ± 1 ms	24 ms	26 ms
Twup	50 ± 1 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 bajty pro odezvu celku ve vozidle	0	20
P2	Doba mezi požadavkem zkušebního zařízení a odezvou celku ve vozidle nebo mezi dvěma odezvami celku ve vozidle	25	250
P3	Doba mezi konce odezvy celku ve vozidle a startem nového požadavku zkušebního zařízení	55	5 000
P4	Doba mezi bajty pro požadavek zkušebního zařízení	5	20

CPR_018 Formáty zprávy pro rychlou inicializaci jsou rozepsány v níže uvedených tabulkách:

Tabulka 5

Zpráva o požadavku StartCommunication

Bajt #	Název parametru	Hexadecimální hodnota	Symbol
#1	Formátový bajt — fyzické adresování	81	FMT
#2	Bajt cílové adresy	EE	TGT
#3	Bajt adresy zdroje	tt	SRC
#4	Služba požadavku StartCommunication	81	SCR
#5	Kontrolní součet	00-FF	CS

Tabulka 6

Zpráva o kladné odezvě StartCommunication

Bajt #	Název parametru	Hexadecimální hodnota	Symbol
#1	Formátový bajt — fyzické adresování	80	FMT
#2	Bajt cílové adresy	tt	TGT
#3	Bajt adresy zdroje	EE	SRC
#4	Bajt dodatečné délky	03	LEN
#5	Kladná odezva Id služby StartCommunication	C1	SCRPR
#6	Klíčový bajt 1	EA	KB1
#7	Klíčový bajt 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 celku ve vozidle, 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 iniciačního prvku StopCommunication musí celek ve vozidle ověřit, zda existující podmínky umožní tuto komunikaci ukončit. V tomto případě musí celek ve vozidle provést veškeré kroky potřebné k ukončení komunikace.

CPR_021 Pokud je možno komunikaci ukončit, musí celek ve vozidle, dříve než komunikace skončí, vydat odezvový prvek StopCommunication se zvolenými parametry Positive Response.

CPR_022 Pokud nemůže být komunikace z jakéhokoliv důvodu ukončena, vydá celek ve vozidle odezvový prvek StopCommunication se zvoleným parametrem Negative Response (záporná odezva).

CPR_023 Pokud celek ve vozidle zjistí překročení času P3max, komunikace se ukončí bez vydání jakékoliv odpovědi.

4.2.2 ***Formát zprávy***

CPR_024 Formáty zpráv pro prvky StopCommunication jsou rozepsány v níže uvedených tabulkách:

Tabulka 7

Zpráva požadavku StopCommunication

Bajt #	Název parametru	Hexadecimální hodnota	Symbol
#1	Formátový bajt — fyzické adresování	80	FMT
#2	Bajt cílové adresy	EE	TGT
#3	Bajt adresy zdroje	tt	SRC
#4	Bajt dodatečné délky	01	LEN
#5	Služba Id požadavku StopCommunication	82	SPR
#6	Kontrolní součet	00-FF	CS

Tabulka 8

Zpráva o kladné odezvě StopCommunication

Bajt #	Název parametru	Hexadecimální hodnota	Symbol
#1	Formátový bajt — fyzické adresování	80	FMT
#2	Bajt cílové adresy	tt	TGT
#3	Bajt adresy zdroje	EE	SRC
#4	Bajt dodatečné délky	01	LEN
#5	Služba kladné odezvy StopCommunication	C2	SPRPR
#6	Kontrolní součet	00-FF	CS

Tabulka 9

Zpráva o záporné odezvě StopCommunication

Bajt #	Název parametru	Hexadecimální hodnota	Symbol
#1	Formátový bajt — fyzické adresování	80	FMT
#2	Bajt cílové adresy	tt	TGT
#3	Bajt adresy zdroje	EE	SRC
#4	Bajt 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 označení serveru, že je stále připojeno, aby tak bylo serveru zabráněno v automatickém návratu do normální činnosti a případnému přerušení komunikace. Tato služba, která se vysílá pravidelně, udržuje diagnostické jednání nebo komunikaci aktivní tím, že vždy po obdržení požadavku této služby resetuje časovač P3.

4.3.2 ***Formát zprávy***

CPR_079 Formáty zpráv pro prvky TesterPresent jsou rozepsány v níže uvedených tabulkách:

Tabulka 10

Zpráva o požadavku TesterPresent

Bajt #	Název parametru	Hexadecimální hodnota	Symbol
#1	Formátový bajt — fyzické adresování	80	FMT
#2	Bajt cílové adresy	EE	TGT
#3	Bajt adresy zdroje	tt	SRC
#4	Bajt dodatečné délky	02	LEN
#5	Služba Id požadavku TesterPresent	3E	TP
#6	Dílčí funkce = responseRequired = [ano	01	RESPREQ_Y
	ne]	02	RESPREQ_NO
#7	Kontrolní součet	00-FF	CS

CPR_080 Je-li parametr responseRequired nastaven na ‚ano', odpoví server následující kladnou zprávou. Je-li nastaven na ‚ne', neodešle server žádnou zprávu.

Tabulka 11

Zpráva o kladné odezvě TesterPresent

Bajt #	Název parametru	Hexadecimální hodnota	Symbol
#1	Formátový bajt — fyzické adresování	80	FMT
#2	Bajt cílové adresy	tt	TGT
#3	Bajt adresy zdroje	EE	SRC
#4	Bajt 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

Bajt #	Název parametru	Hexadecimální hodnota	Symbol
#1	Formátový bajt — fyzické adresování	80	FMT
#2	Bajt cílové adresy	tt	TGT
#3	Bajt adresy zdroje	EE	SRC
#4	Bajt dodatečné délky	03	LEN
#5	Služba záporné odezvy Id	7F	NR
#6	Záporná identifikace služby TesterPresent	3E	TP
#7	ResponseCode = [SubFunctionNotSupported-InvalidFormat	12	RC_SFNS_IF
	incorrectMessageLength]	13	RC_IML
#8	Kontrolní součet	00-FF	CS

5. ŘÍDÍCÍ SLUŽBY

Dostupné služby jsou rozepsány v následující tabulce:

Tabulka 13

Řídící služby

Název služby	Popis
StartDiagnosticSession	Klient požaduje zahájení diagnostického jednání s celkem ve vozidle
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 výrobci 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, musí celek ve vozidle 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 ‚Standard-DiagnosticSession'.

5.1.2 ***Formát zprávy***

CPR_028 Formáty zpráv pro prvky StartDiagnosticSession jsou rozepsány v níže uvedených tabulkách:

Tabulka 14

Zpráva o požadavku StartDiagnosticSession

Bajt #	Název parametru	Hexadecimální hodnota	Symbol
#1	Formátový bajt — fyzické adresování	80	FMT
#2	Bajt cílové adresy	EE	TGT
#3	Bajt adresy zdroje	tt	SRC
#4	Bajt 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

Bajt #	Název parametru	Hexadecimální hodnota	Symbol
#1	Formátový bajt — fyzické adresování	80	FMT
#2	Bajt cílové adresy	tt	TGT
#3	Bajt adresy zdroje	EE	SRC
#4	Bajt 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

Bajt #	Název parametru	Hexadecimální hodnota	Symbol
#1	Formátový bajt — fyzické adresování	80	FMT
#2	Bajt cílové adresy	tt	TGT
#3	Bajt adresy zdroje	EE	SRC
#4	Bajt dodatečné délky	03	LEN
#5	Služba záporné odezvy Id	7F	NR
#6	Záporná identifikace služby StartDiagnosticService	10	STDS
#7	ResponseCode = (SubFunctionNotSupporteda ([a])	12	RC_SFNS
	incorrectMessageLength ([b])	13	RC_IML
	conditionsNotCorrect ([c]))	22	RC_CNC
#8	Kontrolní součet	00-FF	CS

([a]) Hodnota vložená do bajtu #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

Hexa-decimál	Popis	Symbol
81	StandardDiagnosticSession Toto diagnostické jednání umožňuje všechny stanovené služby podle tabulky 1, sloupci 4 ‚SD'. Tyto služby umožňují čtení dat ze serveru (celek ve vozidle). Toto diagnostické jednání je aktivní po úspěšném dokončení inicializace mezi klientem (zkušebním zařízením) a serverem (celek ve vozidle). Diagnostické jednání může být přepsáno jiným diagnostickým jednáním, stanoveným v této části.	SD
85	ECUProgrammingSession Toto diagnostické jednání umožňuje veškeré služby, stanovené v tabulce 1, sloupci 6 ‚ECUPS'. Tyto služby podporují programování paměti serveru (celek ve vozidle). 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, sloupci 6 ‚ECUAS'. Tyto služby podporují řízení vstup/výstup serveru (celek ve vozidle). 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 celek ve vozidle byl v módu KALIBRACE. Mimo vložení platné karty dílny do celku ve vozidle je nezbytné vložit do celku ve vozidle příslušný PIN dříve, než je udělen přístup k módu KALIBRACE.

Služba SecurityAccess zajišťuje prostředky pro vložení PIN a ukazuje zkušebnímu zařízení, zda je nebo není celek ve vozidle v módu KALIBRACE.

PIN může být 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 SecurityAccess PositiveResponse.

CPR_035 Pokud je celek ve vozidle připraven k přijetí PIN pro ověření kartou dílny, 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 zkušebního zařízení, buď protože vložená karta dílny není platná, nebo protože nebyla vložena žádná karta dílny, nebo protože celek ve vozidle přijímá PIN jiným postupem, odpoví celek ve vozidle 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 prokázání totožnosti karty, použije celek ve vozidle pro prodloužení času pro odezvu kód záporné odezvy requestCorrectlyReceived-ResponsePending. 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:

— SubFunctionNotSupported: 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 kartou dílny.

5.2.2 ***Formát zprávy — SecurityAccess — requestSeed***

CPR_040 Formáty zpráv pro prvky SecurityAccess ‚requestSeed' jsou rozepsány v níže uvedených tabulkách:

Tabulka 18

Požadavek SecurityAccess — zpráva requestSeed

Bajt #	Název parametru	Hexadecimální hodnota	Symbol
#1	Formátový bajt — fyzické adresování	80	FMT
#2	Bajt cílové adresy	EE	TGT
#3	Bajt adresy zdroje	tt	SRC
#4	Bajt dodatečné délky	02	LEN
#5	Služba Id požadavku SecurityAccess	27	SA
#6	accessType — requestSeed	7D	AT_RSD
#7	Kontrolní součet	00-FF	CS

Tabulka 19

Zpráva o kladné odezvě SecurityAccess — requestSeed

Bajt #	Název parametru	Hexadecimální hodnota	Symbol
#1	Formátový bajt — fyzické adresování	80	FMT
#2	Bajt cílové adresy	tt	TGT
#3	Bajt adresy zdroje	EE	SRC
#4	Bajt 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

Bajt #	Název parametru	Hexadecimální hodnota	Symbol
#1	Formátový bajt — fyzické adresování	80	FMT
#2	Bajt cílové adresy	tt	TGT
#3	Bajt adresy zdroje	EE	SRC
#4	Bajt 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 prvky SecurityAccess ‚sendKey' jsou rozepsány v níže uvedených tabulkách:

Tabulka 21

Požadavek SecurityAccess — zpráva sendKey

Bajt #	Název parametru	Hexadecimální hodnota	Symbol
#1	Formátový bajt — fyzické adresování	80	FMT
#2	Bajt cílové adresy	EE	TGT
#3	Bajt adresy zdroje	tt	SRC
#4	Bajt 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

Bajt #	Název parametru	Hexadecimální hodnota	Symbol
#1	Formátový bajt — fyzické adresování	80	FMT
#2	Bajt cílové adresy	tt	TGT
#3	Bajt adresy zdroje	EE	SRC
#4	Bajt 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

Bajt #	Název parametru	Hexadecimální hodnota	Symbol
#1	Formátový bajt — fyzické adresování	80	FMT
#2	Bajt cílové adresy	tt	TGT
#3	Bajt adresy zdroje	EE	SRC
#4	Bajt 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	RC_CNC
	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 odpovědností výrobce celku ve vozidle, aby byly při výkonu této služby splněny podmínky serveru.

6.1.2 ***Formát zprávy***

CPR_051 Formáty zprávy pro prvky ReadDataByIdentifier jsou rozepsány v níže uvedených tabulkách:

Tabulka 25

Zpráva o požadavku ReadDataByIdentifier

Bajt #	Název parametru	Hexadecimální hodnota	Symbol
#1	Formátový bajt — fyzické adresování	80	FMT
#2	Bajt cílové adresy	EE	TGT
#3	Bajt adresy zdroje	tt	SRC
#4	Bajt 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

Bajt #	Název parametru	Hexadecimální hodnota	Symbol
#1	Formátový bajt — fyzické adresování	80	FMT
#2	Bajt cílové adresy	tt	TGT
#3	Bajt adresy zdroje	EE	SRC
#4	Bajt dodatečné délky	m+3	LEN
#5	Služba Id kladné odezvy ReadDataByIdentifier	62	RDBIPR
#6 a #7	RecordDataIdentifier = (stejná hodnota, jako bajty #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

Bajt #	Název parametru	Hexadecimální hodnota	Symbol
#1	Formátový bajt — fyzické adresování	80	FMT
#2	Bajt cílové adresy	tt	TGT
#3	Bajt adresy zdroje	EE	SRC
#4	Bajt dodatečné délky	03	LEN
#5	Služba Id záporné odezvy	7F	NR
#6	Služba Id požadavku ReadDataByIdentifier	22	RDBI
#7	ResponseCode = (requestOutOfRange incorrectMessageLength conditionsNotCorrect)	31 13 22	RC_ROOR RC_IML RC_CNC
#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 recordDataqIdentifier, definované tímto dokumentem, jsou uvedeny v níže uvedené tabulce.

Tabulka recordDataIdentifier je tvořena čtyřmi sloupci a několika řádky:

— první sloupec (Hex) zahrnuje ‚hexadecimální hodnotu', určenou pro recordDataIdentifier, stanovený ve třetím sloupci,

— druhý sloupec (Datový prvek) stanovuje prvek dat z dodatku 1, na kterém je založen záznam recordDataIdentifier (někdy je potřebné překódování),

— třetí sloupec (Popis) stanovuje odpovídající název recordDataIdentifier,

— čtvrtý sloupec (Symbol) stanovuje pro tento recordDtaIdentifier příslušný symbol.

Tabulka 28

Definice hodnot recordDataIdentifier

Hex	Datový prvek	Název recordDataIdentifier (viz formát v bodě 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	`SpeedAuthorised`	SpeedAuthorised	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 byly identifikovány klientovi (zkušebnímu zařízení) pomocí recordDataIdentifier. Formáty dat jsou stanoveny v části 8. Mohou být zavedeny volitelné dataRecords dalších uživatelů včetně zvláštního vstupu celku ve vozidle, vnitřních a výstupních dat, ty však nejsou definovány v tomto dokumentu.

6.2 **Služba WriteDataByIdentifier**

6.2.1 ***Popis zprávy***

CPR_056 Službu 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 prvky WriteDataByIdentifier jsou rozepsány v níže uvedených tabulkách:

Tabulka 29

Zpráva o požadavku WriteDataByIdentifier

Bajt #	Název parametru	Hexadecimální hodnota	Symbol
#1	Formátový bajt — fyzické adresování	80	FMT
#2	Bajt cílové adresy	EE	TGT
#3	Bajt adresy zdroje	tt	SRC
#4	Bajt 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

Bajt #	Název parametru	Hexadecimální hodnota	Symbol
#1	Formátový bajt — fyzické adresování	80	FMT
#2	Bajt cílové adresy	tt	TGT
#3	Bajt adresy zdroje	EE	SRC
#4	Bajt dodatečné délky	03	LEN
#5	Služba Id kladné odezvy WriteDataByIdentifier	6E	WDBIPR
#6 a #7	RecordDataIdentifier = (stejná hodnota, jako bajty #6 a #7 v tabulce 29)	xxxx	RDI_…
#8	Kontrolní součet	00-FF	CS

Tabulka 31

Zpráva o záporné odezvě WriteDataByIdentifier

Bajt #	Název parametru	Hexadecimální hodnota	Symbol
#1	Formátový bajt — fyzické adresování	80	FMT
#2	Bajt cílové adresy	tt	TGT
#3	Bajt adresy zdroje	EE	SRC
#4	Bajt dodatečné délky	03	LEN
#5	Služba Id záporné odezvy	7F	NR
#6	Služba Id požadavku WriteDataByIdentifier	2E	WDBI
#7	ResponseCode = (requestOutOfRange	31	RC_ROOR
	incorrectMessageLength	13	RC_IML
	conditionsNotCorrect)	22	RC_CNC
#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 (celek ve vozidle), identifikovaných pomocí recordDataIdentifier. Formáty dat jsou stanoveny v části 8.

7. ŘÍZENÍ ZKUŠEBNÍCH IMPULSŮ — ŘÍDÍCÍ FUNKČNÍ CELEK VSTUP/VÝSTUP

Dostupné služby jsou rozepsány v níže uvedených tabulkách:

Tabulka 32

Řídící funkční celek vstup/výstup

Název služby	Popis
InputOutputControlByIdentifier	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 Celek ve vozidle musí zahájit 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' (výchozí).

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 Sekvence 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 prvky InputOutputControlByIdentifier jsou rozepsány v níže uvedených tabulkách:

Tabulka 33

Zpráva o požadavku InputOutputControlByIdentifier

Bajt #	Název parametru	Hexadecimální hodnota	Symbol
#1	Formátový bajt — fyzické adresování	80	FMT
#2	Bajt cílové adresy	EE	TGT
#3	Bajt adresy zdroje	tt	SRC
#4	Bajt dodatečné délky	xx	LEN
#5	Služba Id požadavku InputOutputControlByIdentifier	2F	IOCBI
#6 a #7	InputOutputIdentifier = (CalibrationInputOutput)	F960	IOI_CIO
#8 nebo #8 až #9	ControlOptionRecord = (		COR_…
	InputOutputControlParameter — jedna z hodnot v tabulce 36	xx	IOCP_…
	controlState — jedna z hodnot v tabulce 38 (viz níže)	xx	CS_…
#9 nebo #10	Kontrolní součet	00-FF	CS

Poznámka: parametr controlState je přítomný jen v některých případech (viz 7.1.3).

Tabulka 34

Zpráva o kladné odezvě InputOutputControlByIdentifier

Bajt #	Název parametru	Hexadecimální hodnota	Symbol
#1	Formátový bajt — fyzické adresování	80	FMT
#2	Bajt cílové adresy	tt	TGT
#3	Bajt adresy zdroje	EE	SRC
#4	Bajt 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 = (		CSR_
	InputOutputControlParameter — stejná hodnota jako #8 v tabulce 33	xx	IOCP_…
	controlState — stejná hodnota jako #9 v tabulce 33 (pokud lze užít)	xx	CS_…
#9 nebo #10	Kontrolní součet	00-FF	CS

Tabulka 35

Zpráva o záporné odezvě InputOutputControlByIdentifier

Bajt #	Název parametru	Hexadecimální hodnota	Symbol
#1	Formátový bajt — fyzické adresování	80	FMT
#2	Bajt cílové adresy	tt	TGT
#3	Bajt adresy zdroje	EE	SRC
#4	Bajt dodatečné délky	03	LEN
#5	Služba Id záporné odezvy	7F	NR
#6	Služba Id požadavku InputOutputControlByIdentifier	2F	IOCBI
#7	responseCode = (		
	incorrectMessageLength	13	RC_IML
	conditionsNotCorrect	22	RC_CNC
	requestOutOfRange	31	RC_ROOR
	deviceControlLimitsExceeded)	7A	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 inputOutputControlParametr

Hex	Popis	Symbol
00	ReturnControlToECU Tato hodnota musí ukazovat serveru (celku ve vozidle), že zkušební zařízení již neřídí signální spojení kalibrace I/O.	RCTECU
01	ResetToDefault Tato hodnota musí ukazovat serveru (celku ve vozidle), že se od něj požaduje nastavení signálního spojení kalibrace I/O do neaktivního stavu.	RTD
03	ShortTermAdjustment Tato hodnota musí ukazovat serveru (celku ve vozidle), že se požaduje nastavení signálního spojení kalibrace I/O na hodnotu, obsaženou v parametru controlState.	STA

CPR_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 RTCOutput

8. FORMÁTY ZÁZNAMŮ DAT

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 okamžité ukázání, 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 označení 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 bajt (hexadecimální hodnota)	2 bajty (hexadecimální hodnota)	4 bajty (hexadecimální hodnota)	ASCII
Platný signál	00 až FA	0000 až FAFF	00000000 až FAFFFFFF	1 až 254
Indikátor pro parametr	FB	FB00 až FBFF	FB000000 až FBFFFFFF	žádný
Rezervní 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 „*“ vyhrazen 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 (v bajtech)	Rozložení	Pracovní rozsah
TimeDate	8	Podrobnosti viz tabulku 40	
HighResolutionTotalVehicleDistance	4	nárůst 5 m/bit výchozí hodnota 0 m	0 až + 21 055 406 km
Kfactor	2	nárůst 0,001 imp/m/bit výchozí hodnota 0	0 až 64,255 imp/m
LfactorTyreCircumference	2	nárůst 0,123 10^{-3}/bit výchozí hodnota 0	0 až 8 031 m
WvehicleCharacteristicFactor	2	nárůst 0,001 imp/m/bit výchozí hodnota 0	0 až 64,255 imp/m
TyreSize	15	ASCII	ASCII
NextCalibrationDate	3	Podrobnosti viz tabulku 41	
SpeedAuthorised	2	nárůst 1/256 km/h/bit výchozí hodnota 0	0 až 250 996 km/h
RegisteringMemberState	3	ASCII	ASCII
VehicleRegistrationNumber	14	Podrobnosti viz tabulku 42	
VIN	17	ASCII	ASCII

CPR_075 Tabulka 40 rozepisuje formáty různých bajtů parametru TimeDate:

Tabulka 40

Rozepsaný formát TimeDate (recordDataIdentifier, hodnota # F00B)

Bájt	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
8	Místní výchozí hodnota hodiny	nárůst 1 h/bit výchozí hodnota –125	–23 až +23 h.

CPR_076 Tabulka 41 rozepisuje formáty různých bajtů parametru NextCalibrationDate:

Tabulka 41

Rozepsaný formát NextCalibrationDate (recordDataIdentifier, hodnota # F022)

Bájt	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

Poznámka týkající se užití parametru ‚den':
1. Hodnota 0 je pro datum prázdnou hodnotou. 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.
2. Tento parametr neovlivňuje nebo nemění výše uvedený parametr hodin.

Poznámka týkající se užití bajtu parametru ‚rok':
Hodnota 0 označuje rok 1985; hodnota 1 označuje rok 1986 atd.

CPR_078 Tabulka 42 rozepisuje formáty různých bajtů parametru VehicleRegistrationNumber:

Tabulka 42

Rozepsaný formát VehicleRegistrationNumber (recordDataIdentifier, hodnota # F07E)

Bájt	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 — MINIMÁLNÍ ROZSAH POŽADOVANÝCH ZKOUŠEK

OBSAH

1. ÚVOD

1.1 **Schválení typu**

EHS schválení typu pro záznamové zařízení (nebo jeho součást) nebo pro kartu tachografu se zakládá na:

— osvědčení bezpečnosti, které provádí některý z příslušných orgánů ITSEC vůči bezpečnostním cílům zcela v souladu s dodatkem 10 této přílohy;

— osvědčení funkčnosti, které provádějí příslušné orgány členských států, které potvrzují, že zkoušený prvek splňuje požadavky této přílohy z hlediska prováděných funkcí, přesnosti měření a ekologických charakteristik;

— osvědčení vzájemné operační součinnosti (interoperability), které provádí zkušebna příslušná pro osvědčování vzájemné operační součinnosti daného záznamového zařízení s nezbytnou kartou tachografu nebo dané karty tachografu s nezbytným záznamovým zařízením (viz kapitolu VIII této přílohy).

Tento dodatek stanoví formou minimálních požadavků, jaké zkoušky musí provést orgán členského státu během funkčních zkoušek a jaké příslušná zkušebna během zkoušek vzájemné operační součinnosti. Postup při zkouškách ani typy zkoušek se podrobnější neurčují.

Různé aspekty osvědčování bezpečnosti nejsou v tomto dodatku obsaženy. Pokud se některé ze zkoušek vyžadovaných pro schválení typu provedou v průběhu hodnocení a osvědčování bezpečnosti, není třeba takové zkoušky opakovat. V tom případě se mohou posuzovat jenom výsledky z těchto bezpečnostních zkoušek. Pro informaci se v tomto dodatku značkou „*“ označují požadavky, které by měly být zkoušeny (nebo blíže vázány ke zkouškám, jejichž provedení se očekává) během osvědčování bezpečnosti.

V tomto dodatku se o schválení typu snímačů pohybu pojednává odděleně od celku ve vozidle, přičemž obojí tvoří dvě 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 **Odkazy**

V tomto dodatku se odkazuje na následující normy:

IEC 68-2-1 Zkoušení vnějších vlivů — Část 2: Zkoušky — Zkoušky A: Chlad. 1990 + Změna 2: 1994.

IEC 68-2-2 Zkoušení vnějších vlivů — Část 2: Zkoušky — Zkoušky B: Suchý žár. 1974 + Změna 2: 1994.

IEC 68-2-6 Základní postupy zkoušení vnějších vlivů — Zkušební metody –Zkouška Fc a směrnice: Vibrace (sinusoidní). Šesté vydání: 1985.

IEC 68-2-14 Základní postupy zkoušení vnějších vlivů — Zkušební metody –Zkouška N: Změna teploty. Změna 1: 1986.

IEC 68-2-27 Základní postupy zkoušení vnějších vlivů — Zkušební metody –Zkouška Ea a směrnice: Náraz. Třetí vydání: 1987.

IEC 68-2-30 Základní postupy zkoušení vnějších vlivů — Zkušební metody –Zkouška Db a směrnice: Vlhký žár, cyklická (12 + 12 — hodinový cyklus). Změna 1: 1985.

IEC 68-2-35 Základní postupy zkoušení vnějších vlivů — Zkušební metody –Zkouška Fda: Náhodné vibrace v širokém pásmu — Vysoká opakovatelnost. Změna 1: 1983.

IEC 529 Stupně ochrany poskytované kryty (kód IP). Druhé vydání: 1989.

IEC 61000-4-2 Elektromagnetická kompatibilita — Zkušební a měřící metody — Zkouška odolnosti proti elektrostatickému vybití: 1995/Změna 1: 1998.

ISO 7637-1 Silniční vozidla — Elektrické rušení vedením a vazbou — Část 1: Osobní automobily a lehká obchodní vozidla se stejnosměrným napájecím napětím 12 V — Šíření elektrického přechodového jevu pouze po napájecím vedení. Vydání 2: 1990.

ISO 7637-2 Silniční vozidla — Elektrické rušení vedením a vazbou — Část 2: Obchodní vozidla se stejnosměrným napájecím napětím 24 V– Šíření elektrického přechodového jevu pouze po napájecím vedení. Vydání 2: 1990.

ISO 7637-3 Silniční vozidla — Elektrické rušení vedením a vazbou — Část 3: Vozidla se stejnosměrným napájecím napětím 12 V nebo 24 V — Elektrický přenos přechodových jevů kapacitní a induktivní vazbou vedeními jinými než napájecími vedeními. První vydání: 1995 + Oprava 1: 1995.

ISO/IEC 7816-1 Informační technika — Identifikační karty — Karty s integrovanými obvody a s kontakty — Část 1: Fyzikální vlastnosti. První vydání: 1998.

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 10373 Identifikační karty — Zkušební metody. První vydání: 1993.

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 vestavění. 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 vkládáním a vyjímáním karet		013, 014, 015*, 016*, 106
3.5.	Měření rychlosti a dráhy		017 až 026
3.6.	Měření času (zkouška při 20 °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 zámků podniku		051 až 055
3.11.	Sledování kontrolních činností		056, 057
3.12.	Zjišťování událostí nebo závad		059 až 069, 106

Bod	Zkouška	Popis	Odpovídající požadavky
3.13.	Identifikační údaje celku ve vozidle		075*, 076*, 079
3.14.	Údaje o vložení a odebrání karty řidiče		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 měřiče ujeté vzdálenosti		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 zámcích podniku		104*
3.25.	Údaje o stahování dat		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.	Stahování údajů na externí paměťová média		072, 106, 149 až 151
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

Bod	Zkouška	Popis	Odpovídající požadavky
4.	**Zkoušky vlivu prostředí**		
4.1.	Teplota	Prokázat provozuschopnost podle: — 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 °C), 1 hod v provozu, 1 hod mimo provoz, 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 °C) a s výdrží 2 hod na každé dolní i horní teplotě. 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.	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 °C do +55 °C při relativní vlhkosti od 97 % při +25 °C event. 93 % při +55 °C	160
4.3.	Vibrace	1. Sinusové vibrace: Prokázat, že celek ve vozidle vyhoví těmto parametrům sinusového kmitání: — konstantní výchylka dráhy mezi 5 a 11 Hz: max.10 mm — konstantní zrychlení mezi 11 a 300 Hz: 50g Průkaz podle IEC 68-2-6 zkouškou Fc o délce nejméně 3x12 hod (12 hod za každou nápravu) 2. Náhodné vibrace: 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 3 × 12 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	163
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 °C po 1 hod — modely pro jmenovité napětí 12 V: 17 V při +40 °C po 1 hod	161
4.6.	Ochrana proti záměně polarity	Prokázat, že celek ve vozidle vydrží přepólování napájecího napětí	161

Bod	Zkouška	Popis	Odpovídající požadavky
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**		
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	Pro modely 24 V: splnění ISO 7637-2: Impuls 1a: Vs= –100 V, Ri=10 Ohm Impuls 2: Vs= +100 V, Ri=10 Ohm Impuls 3a: Vs= –100 V, Ri=50 Ohm Impuls 3b: Vs= +100 V, Ri=50 Ohm Impuls 4: Vs= -16 V, Va= –5 V, t6= 15 ms Impuls 5: Vs= +65 V, Ri= 5 Ohm, td=100 msImpuls 5 se zkouší jen u jednotek pro instalaci v těch vozidlech, která nejsou vybavena žádnou vnější společnou ochranou pro zatížení naprázdno	162

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
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

Bod	Zkouška	Popis	Odpovídající požadavky
4.	**Zkoušky vlivu prostředí**		
4.1.	Provozní teplota	Prokázat provozuschopnost (jak stanoveno ve zkoušce 3.3) v teplotním rozsahu [–40 °C; +135 °C] podle: — IEC 68-2-1, zkouška Ad s trváním 96 hod při nejnižší teplotě Tomin — IEC 68-2-2, zkouška Bd s trváním 96 hod při nejvyšší teplotě Tomax	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 °C) k horní teplotě (+135 °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 3.3) podle IEC 68-2-30, zkouška Db, šest 24 hod cyklů, každý se změnou teploty od +25 °C do +55 °C při relativní vlhkosti od 97 % při +25 °C event. 93 % při +55 °C	160
4.4.	Vibrace	Prokázat provozuschopnost (jak stanoveno ve zkoušce 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	163
4.5.	Mechanický náraz	Prokázat provozuschopnost (jak stanoveno ve zkoušce 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 kontroluje přítomnost povinných souborů na kartě a podmínek přístupu k nim	TCS 312 TCS 400*, 401, 402, 403*, 404, 405*, 406, 407, 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)	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 osvědčování bezpečnosti)	
7.	**Zkoušky vlivu prostředí**		
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. 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
2.	Zkoušky zápisu/čtení	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 osvědčení bezpečnosti, musí výrobci konkretizovat a vyplnit nezbytné dokumenty, aniž by v nich měnili nebo vypouštěli existující specifikace možného ohrožení bezpečnosti a cílů, skutečností a funkcí zajišťujících bezpečnost.

OBSAH

Všeobecné požadavky na bezpečnost snímačů pohybu

Všeobecné požadavky na bezpečnost celku ve vozidle

Všeobecné požadavky na bezpečnost karty tachografu

VŠEOBECNÉ POŽADAVKY NA BEZPEČNOST SNÍMAČŮ POHYBU

1. **Úvod**

Tento dokument obsahuje popis snímače pohybu, možná ohrožení bezpečnosti, kterým musí být 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 možným ohrožením bezpečnosti a plněných cílů skutečnostem a specifikacím SEF přidělena jednotná označení.

2. **Zkratky, definice a odkazy**

2.1 ***Zkratky***

ROM	Trvalá paměť
SEF	Funkce zajišťující bezpečnost
TBD	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 sdílená s VU udávající rychlost a ujetou vzdálenost
Fyzicky oddělené části	Fyzické části snímače pohybu, které jsou rozložené 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)
Systém	Zařízení, osoby nebo podniky 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, zaznamenaná nebo uložená snímačem pohybu

2.3 ***Odkazy***

ITSEC Information Technology Security Evaluation Criteria 1991 (Kritéria hodnocení bezpečnosti informační technologie 1991).

3. **Princip výrobku**

3.1 ***Popis snímače pohybu a postup užití***

Snímač pohybu je určen k montáži do silničních vozidel. Jeho účelem je zajistit pro VU bezpečná data udávající rychlost a ujetou vzdálenost.

Snímač pohybu je mechanicky propojen s pohybující se částí vozidla, jejíž pohyb umožňuje odvodit rychlost vozidla nebo vozidlem ujetou vzdálenost. Snímač může být umístěn v převodové skříni vozidla nebo v kterékoliv jiné konstrukční části vozidla.

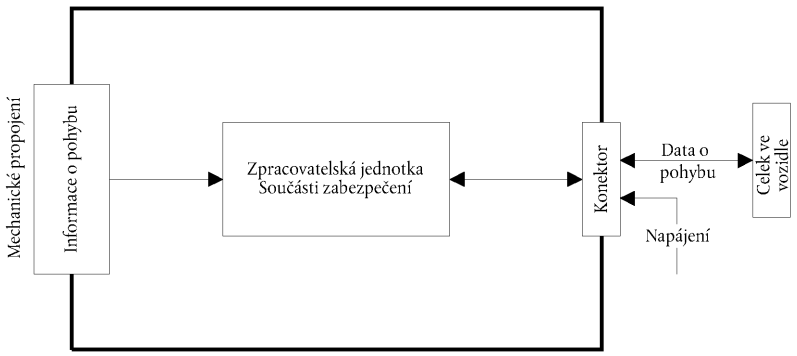
V provozním stavu je snímač pohybu propojen s VU.

Snímač pohybu může být připojen na zvláštní zařízení pro provozní účely (definuje výrobce).

Typický snímač pohybu je popsán v následujícím vyobrazení:

Obrázek 1

Typický snímač pohybu

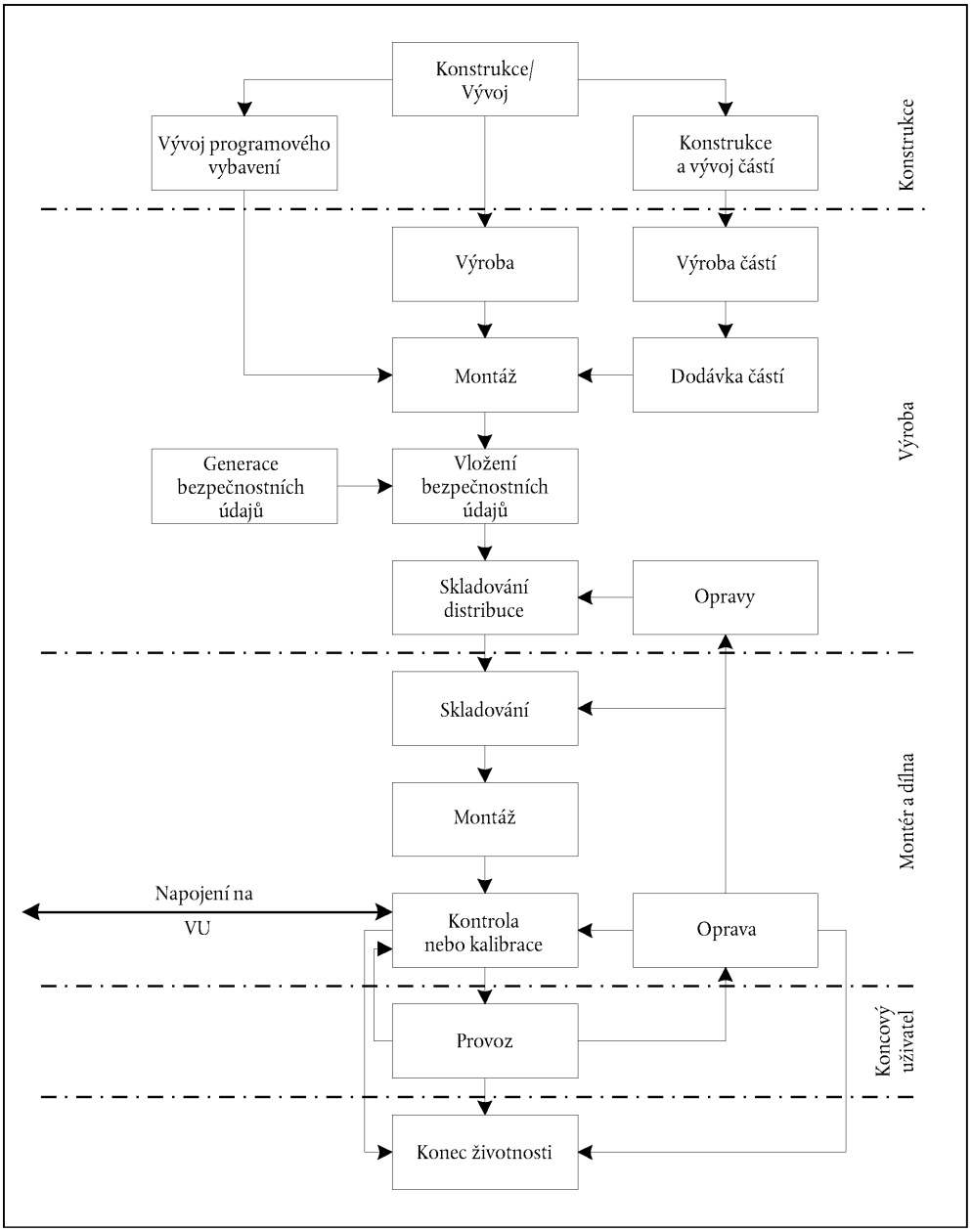


3.2 ***Životní cyklus snímače pohybu***

Typický životní cyklus snímače pohybu popisuje následující vyobrazení:

Obrázek 2

Typický životní cyklus snímače pohybu



3.3 ***Ohrožení bezpečnosti***

Tento bod 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 není povolen.

3.3.2 *Ohrožení bezpečnosti v souvislosti s konstrukcí*

T.Faults	Závady v technickém vybavení, programovém vybavení 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	Pokus uživatele o nedovolené získání znalostí o konstrukci ať již z podkladů výrobce (krádeží, uplácením 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 technické vybavení snímače pohybu.
T.Mechanical_Origin	Pokus uživatele o manipulaci se snímačem pohybu (např. demontáž z převodové skříně).
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 nedovolené získání dat při generaci bezpečnostních údajů v průběhu generace dat, při dopravě nebo při skladování zařízení.
T.Software	Pokus uživatele o změnu programového vybavení snímače pohybu.
T.Stored_Data	Pokus uživatele o změnu uložených údajů (bezpečnostní data nebo data o uživateli).

3.4 ***Cíle bezpečnosti***

Hlavním bezpečnostním cílem systému digitálního tachografu je toto:

O.Main	Kontrolním orgánům musí být ke kontrole dostupná data, jež plně a přesně udávají činnosti 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 dosažitelná 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 snímači pohybu, které přispívají k jeho celkové bezpečnosti, jsou tyto:

O.Access	Snímač pohybu musí řídit funkce a data připojených jednotek.
O.Audit	Snímač pohybu musí sledovat 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 byl postup zpracování vstupních dat, ze kterých se odvozují data o pohybu, přesný.
O.Reliability	Snímač pohybu musí pracovat spolehlivě.
O.Secured_Data_Exchange	Snímač pohybu musí zabezpečit výměnu dat s VU.

3.6 ***Prostředky fyzické, 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 bezpečnosti IT.
M.Manufacturing	Výrobci snímače pohybu musí zajistit, aby přidělování odpovědností v průběhu výroby odpovídalo bezpečnosti IT a aby byl v průběhu výroby snímač pohybu chráněn před fyzickými zásahy, které by mohly ovlivnit jeho bezpečnost IT.

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 bezpečnost IT.

3.6.3 *Generace bezpečnostních dat a jejich dodávka*

M.Sec_Data_Generation	Algoritmus generace bezpečnostních dat musí být přístupný jen oprávněným a spolehlivým osobám.
M.Sec_Data_Transport	Bezpečnostní data musí být generována, transportována a vkládána do snímače pohybu způsobem zabezpečujícím jejich příslušnou důvěrnost a úplnost (integritu).

3.6.4 *Montáž, kalibrace a kontrola záznamového zařízení*

M.Approved_Workshops	Montáž, kalibraci a opravy záznamového zařízení musí provádět jen schválení a spolehliví montéři nebo dílny.
M.Mechanical_Interface	Musí být provedena opatření detekující fyzické zásahy do mechanického propojení (např. plomby).
M.Regular_Inpections	Záznamové zařízení musí být pravidelně 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 *Modernizace programového vybavení*

M.Software_Upgrade	Než je revize programového vybavení zavedena do snímače pohybu, musí být osvědčena její bezpečnost.

4. **Funkce zajišťující bezpečnost**

4.1 ***Identifikace a prokázání totožnosti***

UIA_101 Snímač pohybu musí být pro každou interakci schopen stanovit identitu jednotky, na kterou je připojen.

UIA_102 Identitu připojené jednotky tvoří:

— skupina jednotek

— VU,

— řídící zařízení,

— ostatní

— ID jednotky (pouze u VU)

UIA_103 jednotky připojeného VU je tvořena číslem schválení typu VU a výrobním číslem VU.

UIA_104 Snímač pohybu musí být schopen prokázat totožnost kteréhokoliv VU nebo řídící jednotky, na které je napojen:

— při připojení jednotky,

— při obnově napájení.

UIA_105 Snímač pohybu musí být schopen pravidelně 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 události,

— varovat dotyčnou 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 oprávněny.

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 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 události.

AUD_102 Události ovlivňující bezpečnost snímače pohybu jsou tyto:

— pokusy o poškození bezpečnosti,

— závada v prokázání totožnosti

— závada v úplnosti (integrity) uložených dat,

— závada ve vnitřním přenosu dat,

— neoprávněné otevření pouzdra,

— manipulace s technickým vybavením.

— 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 uvést odpovídající označení závady (stanoví výrobce).

AUD_104 Snímač pohybu musí generované záznamy auditu odeslat do VU v době jejich generace a může si je také uložit ve své paměti.

AUD_105 Pokud snímač pohybu ukládá záznamy o auditu, musí snímač zajistit do vyčerpání kapacity paměti 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 bodu se použijí pouze v případě, že je snímač pohybu tvořen fyzicky oddělenými částmi.

ACR_102 Pokud jsou mezi fyzicky oddělenými částmi snímače pohybu přenášena data, musí být data chráněna před 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 ve své paměti s ohledem 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 prvém zapojení a v průběhu normálního provozu musí snímač pohybu ověřovat svou správnou funkci autotesty. Autotest snímače pohybu musí zahrnovat ověření úplnosti (integrity) 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 *Programové vybavení*

RLB_104 Nesmí existovat žádný způsob, jak při užívání analyzovat nebo ladit programové vybavení snímače pohybu.

RLB_105 Vstupy z vnějších zdrojů nesmějí 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 šest měsíců detekovat, i když k otevření dojde při odpojeném 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 určité zásahy do technického vybavení (definuje výrobce).

RLB_108 Ve výše popsaném případě musí SEF generovat záznam auditu a snímač pohybu musí: (definuje výrobce).

4.6.4 *Přerušení napájení*

RLB_109 V průběhu přerušení nebo změnách napájení musí snímač pohybu zachovat bezpečný stav.

4.6.5 *Obnovení nastavení (resetování)*

RLB_110 V případě přerušení napájení nebo zastavení transakce před jejím ukončení 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 udržována zbytečně.

4.6.7 *Vícefunkční využití*

RLB_112 Pokud snímač pohybu zajišťuje jiné využití než jen využití pro tachograf, musí být všechna další využívání fyzicky nebo logicky vzájemně oddělena. Taková využití nesmějí 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 byl schopen ověřit jejich úplnost (integritu) a totožnost.

4.8 ***Podpora šifrováním***

Požadavky tohoto odstavce se použijí pouze v případě potřeby v závislosti na použitých mechanismech bezpečnosti a na řešení výrobce.

CSP_101 Každá 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 ‚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 jiné prostředky působí proti kterému ohrožení,

— která SEF plní které cíle bezpečnosti IT.

	Ohrožení											cíle IT					
	T.Access	T.Faults	T.Test	T. Design	T.Environment	T.Hardware	T.Mechanical_Origin	T.Motion_Data	T.Power_Supply	T.Security_Data	T.Software	T.Stored_Data	O.Access	O.Audit	O.Authentication	O.Procesing	O.Reliability	O.Secured_Data_Exchange
Prostředky fyzické, personální a procedurální																		
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 zákona					x	x	x		x	x	x							
Modernizace programového vybavení											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 totožnosti 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					

	Ohrožení												cíle IT					
	T.Access	T.Faults	T.Test	T. Design	T.Environment	T.Hardware	T.Mechanical_Origin	T.Motion_Data	T.Power_Supply	T.Security_Data	T.Software	T.Stored_Data	O.Access	O.Audit	O.Authentication	O.Procesing	O.Reliability	O.Secured_Data_Exchange
ACC_103 Data uživatele												x	x					
ACC_104 Bezpečnostní data										x		x	x					
ACC_105 Struktura souborů a podmínky přístupu	x									x		x	x					
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_103 Vnitřní 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 programového vybavení				x							x						x	
RLB_105 Vstup programového vybavení											x					x	x	
RLB_106 Otevření pouzdra				x	x	x				x	x	x					x	
RLB_107 Poškození technického vybavení						x											x	
RLB_108 Poškození technického vybavení						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	x
CSP_102 Generace klíče																	x	x
CSP_103 Distribuce klíče																	x	x
CSP_104 Přístup ke klíči																	x	x
CSP_105 Poškození klíče																	x	x

VŠEOBECNÉ POŽADAVKY NA BEZPEČNOST CELKU VE VOZIDLE

1. **Úvod**

Tento dokument obsahuje popis celku ve vozidle, možná ohrožení bezpečnosti, kterým musí být 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 možným ohrožením bezpečnosti a plněných cílů, skutečnostem a specifikacím SEF přidělena jednotná označení.

2. **Zkratky, definice a odkazy**

2.1 ***Zkratky***

PIN	Osobní identifikační číslo
ROM	Trvalá paměť
SEF	Funkce zajišťující bezpečnost
TBD	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 udávající rychlost a ujetou vzdálenost
Fyzicky oddělené části	Fyzické části VU, které jsou rozložené 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 podniky jakkoliv související se záznamovým zařízením
Uživatel	Osoba užívající zařízení. Normálními uživateli VU se rozumí řidiči, kontroloři, dílny a podniky.
Data uživatele	Jakákoliv data jiná než údaje o pohybu nebo bezpečnosti, zaznamenaná nebo uložená ve VU a požadovaná kapitolou III bodem 12.

2.3 ***Odkazy***

ITSEC Information Technology Security Evaluation Criteria 1991 (Kritéria hodnocení bezpečnosti informační 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 činnostmi řidiče. VU je napojen na snímač pohybu, se kterým sdílí data o pohybu vozidla.

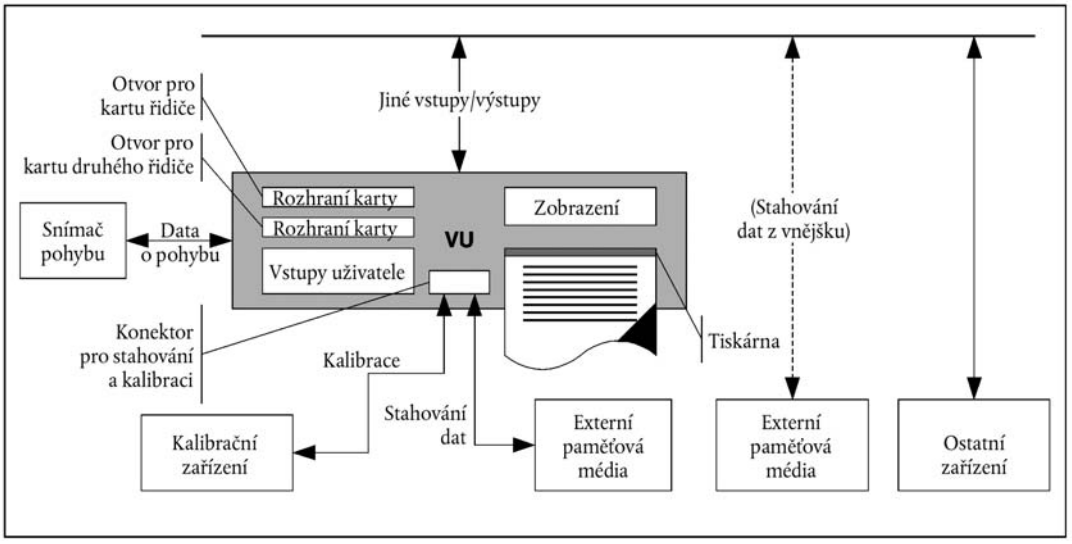
Uživatelé se VU identifikují užitím svých karet tachografu.

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:

Obrázek 1

Pracovní prostředí VU



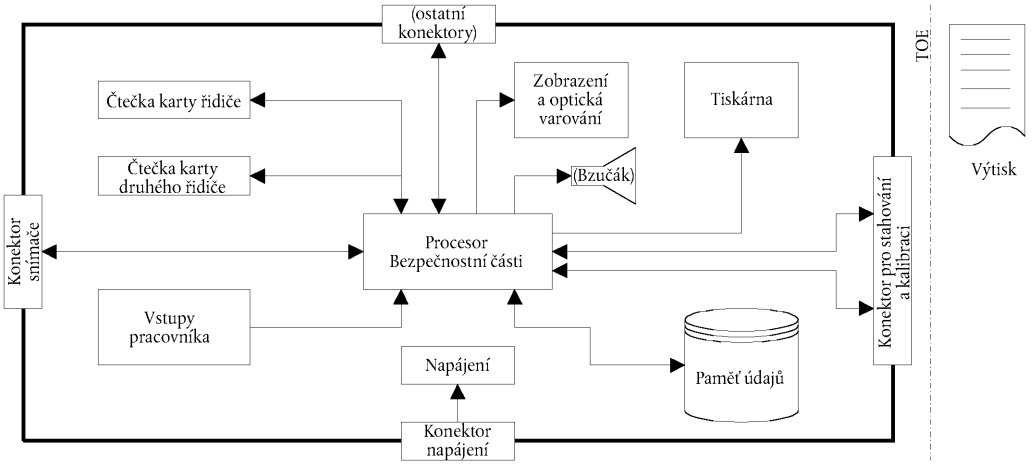
Všeobecné vlastnosti VU, jeho funkce a více o činnosti popisuje kapitola II přílohy I B.

Funkční požadavky VU stanovuje kapitola III přílohy I B.

Typický VU je popsán v následujícím vyobrazení:

Obrázek 2

Typický celek ve vozidle (VU) (…) volitelný



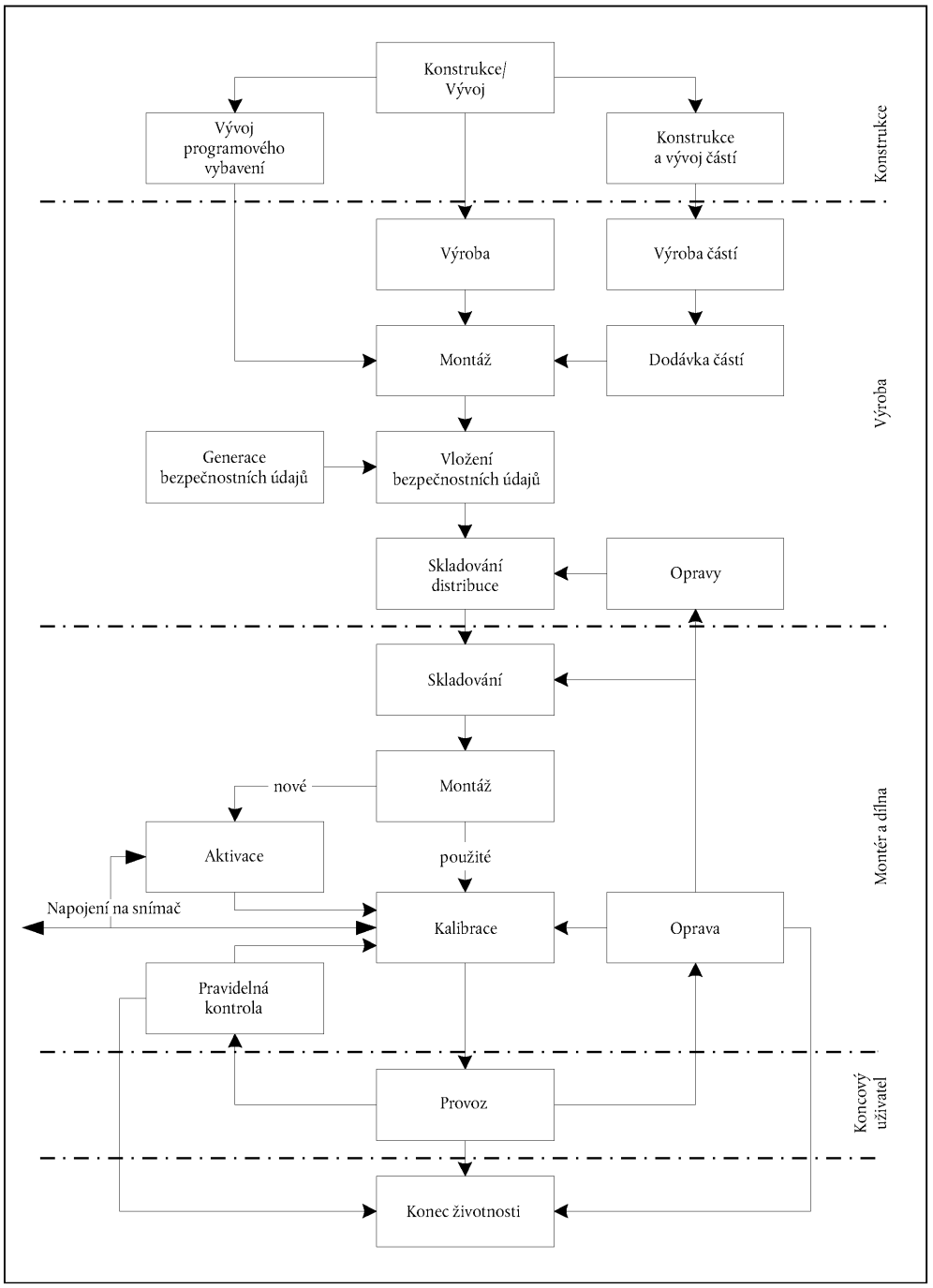
Je třeba připomenout, že i mechanismus tiskárny je součástí TOE, jednou vytištěný papírový dokument ale nikoliv.

3.2 ***Životní cyklus celku do vozidla***

Typický životní cyklus VU popisuje následující vyobrazení:

Obrázek 3

Typický životní cyklus VU



3.3 ***Ohrožení bezpečnosti***

Tento bod popisuje ohrožení bezpečnosti, kterým může být VU vystaven.

3.3.1 *Ohrožení identifikace a postupu kontroly přístupu*

T.Access	Uživatel se pokusil o přístup k funkcím, ke kterým mu není povolen (např. řidič získal přístup ke kalibračním funkcím).
T.Identification	Uživatel se pokusil užít více identifikací nebo žádné identifikace

3.3.2 *Ohrožení bezpečnosti v souvislosti s konstrukcí*

T.Faults	Závady v technickém vybavení, programovém vybavení nebo v komunikačních postupech, které mohou VU uvést do nepředpokládaných podmínek ohrožujících bezpečnost.
T.Test	Užití neplatných zkušebních módů nebo existující možnost ‚vstupu zadními dveřmi', které mohou ovlivnit bezpečnost VU.
T.Design	Pokus uživatele o nedovolené získání znalostí o konstrukci ať již z podkladů výrobce (krádeží, uplácením 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 stahování 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, čipové karty).
T.Hardware	Pokus uživatele měnit technické vybavení 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 stahování).
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 nedovolené získání dat při generaci bezpečnostních údajů v průběhu generace dat, při dopravě nebo při skladování zařízení.
T.Software	Pokus uživatele o změnu programového vybavení VU.
T.Stored_Data	Pokus uživatele o změnu uložených údajů (bezpečnostní data nebo data o uživateli).

3.4 ***Cíle bezpečnosti***

Hlavním bezpečnostním cílem systému digitálního tachografu je toto:

O.Main	Kontrolním orgánům musí být ke kontrole dostupná data, jež plně a přesně udávají činnosti 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, která mají být následně ověřována kontrolními orgány, musí být dosažitelná a přesně odpovídat činnostem 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 paměťového média tak, aby bylo možno ověřit jejich úplnost (integritu) a totožnost.

3.5 ***Cíle bezpečnosti informační technologie***

Specifické cíle bezpečnosti informační technologie VU, které přispívají k jeho celkové bezpečnosti, jsou tyto:

O.Access	VU musí řídit přístup uživatele k funkcím a datům.
O.Accountability	VU musí snímat přesná data o přiřazení.
O.Audit	VU musí sledovat pokusy o obcházení jeho bezpečnostních opatření a musí o nich předávat informace postiženým uživatelům.
O.Authentication	VU musí 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 fyzické, 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 bezpečnosti IT.
M.Manufacturing	Výrobci VU musí zajistit, aby přidělování odpovědností v průběhu výroby odpovídalo bezpečnosti IT a aby byl VU v průběhu výroby chráněn před fyzickými zásahy, které by mohly ovlivnit jeho bezpečnost IT.

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 IT.
M.Activation	Výrobci vozidla a montéři nebo dílny musí VU aktivovat po jeho montáži dříve, než vozidla opustí dílny, 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 oprávněným a spolehlivým osobám.
M.Sec_Data_Transport	Bezpečnostní data musí být generována, transportována a vkládána do VU způsobem, zabezpečujícím jejich příslušnou důvěrnost a úplnost (integritu).

3.6.4 *Dodávka karet*

M.Card_Availability	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.Card_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 schválení a spolehliví montéři nebo dílny.
M.Regular_Inpections	Záznamové zařízení musí být pravidelně kontrolováno a kalibrováno.
M.Faithful_Calibration	V průběhu kalibrace musí schválení montéři nebo schválené dílny vložit do záznamového zařízení odpovídající 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 ručně vybranou činnost atd.).

3.6.7 *Kontrola dodržování předpisů*

M.Controls	Dodržování právních předpisů je třeba pravidelně a nahodile kontrolovat a kontrola musí zahrnovat bezpečnostní audit.

3.6.8 *Modernizace programového vybavení*

M.Software_Upgrade	Než je revize programového vybavení zavedena do VU, musí být osvědčena její 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 Identitu snímače pohybu tvoří číslo schválení typu snímače a výrobní číslo snímače.

UIA_203 VU musí prokázat totožnost snímače pohybu, na který je připojen:

— při připojení snímače pohybu,

— při každé kalibraci záznamového zařízení,

— při obnově napájení.

Prokázání totožnosti musí být vzájemné a musí jej spouštět VU.

UIA_204 VU musí pravidelně (periodu stanoví výrobce, musí ale být kratší než 1 hod) opětovně identifikovat a prokázat totožnost snímače pohybu, ke kterému je napojen, a musí se ujistit, 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) 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 sledováním karet tachografu vložených v zařízení do otvoru pro kartu řidiče a do otvoru pro kartu druhého řidiče.

UIA_208 Identita uživatele musí sestávat z:

— uživatelské skupiny:

— ŘIDIČ (karta řidiče),

— KONTROLOR (kontrolní karta),

— DÍLNA (karta dílny),

— PODNIK (karta podniku),

— 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 svých uživatelů.

UIA_210 VU musí znovu zjistit totožnost svých uživatelů:

— při obnoveném napájení,

— pravidelně nebo po určitých událostech (stanoví výrobce, musí ale být vícekrát 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 vložením PIN. PIN musí mít nejméně 4 znaky.

Poznámka:Je-li 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 ukládaných dat o prokázání totožnosti.

UIA_214 Po zjištění pěti 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).

4.1.3 *Identifikace a prokázání totožnosti dálkově připojeného podniku*

Zabudování zařízení pro dálkové připojení je nepovinné. Následující odstavec se proto použije, pouze pokud je tato funkce zavedena.

UIA_215 Při každé interakci s dálkově připojeným podnikem musí být VU schopen stanovit identitu tohoto podniku.

UIA_216 Identitu dálkově připojeného podniku tvoří tyto prvky: kód členského státu vydávajícího kartu a číslo karty podniku.

UIA_217 VU provede úspěšné stanovení totožnosti dálkově připojeného podniku před povolením přenosu dat tomuto podniku.

UIA_218 Postup stanovování totožnosti spočívá v prokázání, že daný podnik má platnou kartu podniku, na které jsou zaznamenány bezpečnostní údaje, které povinně vyplývají z daného systému.

UIA_219 VU musí zajistit a ochránit využití kopírovaných a znovu uložených údajů o prokázání totožnosti.

UIA_220 Po pěti neúspěšných po sobě jdoucích pokusech o prokázání totožnosti musí SEF:

— varovat dálkově připojený podnik.

4.1.4 *Identifikace a prokázání totožnosti řídicí jednotky*

Výrobci VU mohou předvídat vývoj a výrobu zvláštních zařízení umožňujících výkon dodatčných řídicích funkcí VU (např. aktualizace programového vybavení, nové zadání bezpečnostních údajů). Následující odstavec se proto použije, pouze pokud je tato funkce zavedena.

UIA_221 Při každé interakci s řídicí jednotkou musí být VU schopen stanovit identitu této jednotky.

UIA_222 VU provede úspěšné stanovení totožnosti řídicí jednotky před povolením jakékoli další integrace s ní.

UIA_223 VU musí zajistit a ochránit využití kopírovaných a znovu uložených údajů o prokázání totožnosti.

4.2 ***Kontrola přístupu***

Kontrola přístupu zabezpečuje, že informace jsou odečítány, vytvářeny nebo modifikovány v TOE pouze osobami, které jsou k tomu oprávněny.

Je třeba podotknout, že data uživatele zaznamenaná VU, která také obsahují soukromá nebo obchodně citlivá hlediska, zde nejsou důvěrná. 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 funkcím*

ACC_202 VU musí uplatnit mód pravidel volby operací (požadavky 006 až 009).

ACC_203 VU musí využívat mód operací k zajištění funkci 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 paměti údajů 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 paměti údajů 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 ***Možnosti přiřazení***

ACT_201 VU musí zajistit, aby řidiči byli přiřazování ke svým činnostem (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 ke svým činnostem (požadavky 098, 101 a 109).

ACT_204 VU musí zajistit, aby kontroloři byli přiřazováni ke svým činnostem (požadavky 102, 103 a 109).

ACT_205 VU musí zaznamenávat data měřiče ujeté vzdálenosti (požadavek 090) a podrobná 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 nebyla měněna, s výjimkou, kdy jsou starší zaznamenaná data nahrazována daty novými.

ACT_207 VU musí zajistit, že nebude měnit data již uložená na kartě tachografu (požadavky 109 a 109a), s výjimkou, kdy jsou starší zaznamenaná data nahrazována daty novými (požadavek 110) nebo v případě popsaném v poznámce v dodatku 1 bodě 2.1.

4.4 ***Audit***

Schopnosti auditu jsou požadovány pouze u událostí, které mohou označovat manipulaci nebo narušení bezpečnosti. Audit není požadován při obvyklém výkonu práv, i pokud se týkají bezpečnosti.

AUD_201 VU musí v případech zhoršení vlastní bezpečnosti VU generovat záznamy auditu o události (požadavky 094, 096 a 109).

AUD_202 Události ovlivňující bezpečnost VU jsou tyto:

— pokusy o poškození bezpečnosti:

  — závada v prokázání totožnosti snímače pohybu,

  — závada v prokázání totožnosti karty tachografu,

  — neoprávněná výměna snímače rychlosti,

  — závada v úplnosti (integritě) dat z karty,

  — závada v úplnosti (integritě) uložených dat uživatele,

  — závada ve vnitřním přenosu dat,

  — neoprávněné otevření pouzdra,

  — poškození technického vybavení,

— 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 stahovat.

4.5 ***Opětovné použití***

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,

— řídící hodiny VU,

— kalibrační parametry záznamového zařízení,

— karta tachografu,

— vstupy uživatele.

ACR_201a 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 bodu se použijí pouze v případě, že je VU tvořen fyzicky oddělenými částmi.

ACR_202 Pokud jsou mezi fyzicky oddělenými částmi VU přenášena data, musí být data chráněna před 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 ve své paměti s ohledem 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 prvém zapojení a v průběhu normálního provozu musí VU ověřovat svou správnou funkci autotesty. Autotest VU musí zahrnovat ověření úplnosti (integrity) 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) (vnitřní závada VU),

— zachovával úplnost (integritu) uložených dat.

4.7.2 *Programové vybavení*

RLB_204 Nesmí existovat žádný způsob, jak po aktivaci VU při užívání analyzovat nebo ladit jeho programové vybavení.

RLB_205 Vstupy z vnějších zdrojů nesmějí 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 šest měsíců detekovat, i když k otevření dojde při odpojeném 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 určité zásahy do technického vybavení (definuje výrobce).

RLB_208 Ve výše popsaném případě musí SEF generovat záznam auditu a VU musí: (definuje výrobce): …

4.7.4 *Přerušení napájení*

RLB_209 VU musí detekovat odchylky od stanovených hodnot napájení, včetně jeho přerušení.

RLB_210 Ve výše popsaném případu 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 *Podmínky obnovené nastavení (resetování)*

RLB_211 V případě přerušení napájení nebo zastavení transakce před jejím ukončení 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 udržována 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 fyzicky nebo logicky vzájemně oddělena. Taková využití nesmějí 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 musí SEF:

— 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_204 Po zjištění závady v úplnosti (integritě) dat nebo v totožnosti musí SEF:

— vygenerovat záznam o auditu,

— data neužívat.

DEX_205 VU musí exportovat data do čipové karty tachografu spolu s bezpečnostními znaky tak, aby byla karta schopna ověřit jejich úplnost (integritu) 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 paměťových 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 (integritu) a totožnost.

4.9 ***Podpora šifrováním***

Požadavky tohoto odstavce se použijí pouze v případě potřeby v závislosti na použitých mechanismech bezpečnosti a na řešení výrobce.

CSP_201 Každá 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 úrovní 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 jiné prostředky působí proti kterému ohrožení,

— která SEF plní které cíle bezpečnosti IT.

	Ohrožení																		cíle IT								
	T.Access	T.Identification	T.Faults	T.Test	T.Design	T.Calibration_Parameters	T.Card_Data_Exchange	T.Clock	T.Environment	T.Fake_Device	T.Hardware	T.Motion_Data	T.Non_Activated	T.Output_Data	T.Power_Supply		T.Security_Data	T.Software	T.Stored_Data	O.Access	O.Accountability	O.Audit	O.Authentication	O.Integrity	O.Output	O.Procesing	O.Reliability	O.Secured_Data_Exchange
Prostředky fyzické, personální a procedurální																											
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 zákona		x				x		x	x		x		x		x			x	x								
Modernizace programového vybavení																			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				
UIA_213 Nepadělatelné prokázání totožnosti	x	x								x										x			x				

	Ohrožení																			cíle IT								
	T.Access	T.Identification	T.Faults	T.Test	T.Design	T.Calibration_Parameters	T.Card_Data_Exchange	T.Clock	T.Environment	T.Fake_Device	T.Hardware	T.Motion_Data	T.Non_Activated	T.Output_Data	T.Power_Supply		T.Security_Data	T.Software	T.Stored_Data	O.Access	O.Accountability	O.Audit	O.Authentication	O.Integrity	O.Output	O.Procesing	O.Reliability	O.Secured_Data_Exchange
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					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								
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	

	Ohrožení																		cíle IT							
	T.Access	T.Identification	T.Faults	T.Test	T.Design	T.Calibration_Parameters	T.Card_Data_Exchange	T.Clock	T.Environment	T.Fake_Device	T.Hardware	T.Motion_Data	T.Non_Activated	T.Output_Data	T.Power_Supply		T.Security_Data	T.Software	T.Stored_Data	O.Access	O.Accountability	O.Audit	O.Authentication	O.Integrity	O.Output	O.Procesing	O.Reliability	O.Secured_Data_Exchange
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 programového vybavení					x													x									x	
RLB_205 Vstup programového vybavení																		x							x	x	x	
RLB_206 Otevření pouzdra					x				x		x			x			x	x	x						x		x	
RLB_207 Poškození technického vybavení											x																x	
RLB_208 Poškození technického vybavení											x											x						
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

	Ohrožení																			cíle IT								
	T.Access	T.Identification	T.Faults	T.Test	T.Design	T.Calibration_Parameters	T.Card_Data_Exchange	T.Clock	T.Environment	T.Fake_Device	T.Hardware	T.Motion_Data	T.Non_Activated	T.Output_Data	T.Power_Supply		T.Security_Data	T.Software	T.Stored_Data	O.Access	O.Accountability	O.Audit	O.Authentication	O.Integrity	O.Output	O.Procesing	O.Reliability	O.Secured_Data_Exchange
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 externích 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, možná ohrožení bezpečnosti, kterým musí být 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.

Karta tachografu je standardní čipová karta s určeným použitím v tachografu a musí vyhovovat současným požadavkům na funkci a zajištění bezpečnosti čipových 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 možným ohrožením bezpečnosti a plněných cílů, skutečnostem a specifikacím SEF přidělena jednotná označení.

2. **Zkratky, definice a odkazy**

2.1 ***Zkratky***

IC	Integrovaný obvod (elektronická součást konstruovaná k zpracovávání dat nebo k funkci paměti).
OS	Operační systém
PIN	Osobní identifikační číslo
ROM	Trvalá paměť
SFP	Politika bezpečnostních funkcí
TBD	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 ochráněna z hlediska úplnosti (integrity), neoprávněných změn a důvěrnosti (pokud je použitelné pro bezpečnostní data). Citlivá data zahrnují bezpečnostní data a data uživatele.
Bezpečnostní data	Specifická data potřebná pro podporu funkcí zajišťujících bezpečnost (např. šifrovací klíče)
Systém	Zařízení, osoby nebo podniky, jakkoliv související se záznamovým zařízením
Uživatel	Jakákoliv jednotka (osoba nebo externí jednotka IT) mimo TOE, která spolupracuje s TOE (pokud není užit ve smyslu ‚data uživatele')

Data uživatele	Citlivá data uložená na kartě tachografu jiná než bezpečnostní data. Data uživatele zahrnují identifikační data a data o činnosti.
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 činností	Data činností zahrnují data činností, událostí, závad a kontrol činnosti držitele karty.
Data činnosti držitele karty	Data uživatele, která se vztahují k činnostem držitele 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 činností	Data uživatele, která se vztahují ke kontrolám uplatňování zákona podle definice požadavků 210 a 225.

2.3 *Odkazy*

ITSEC Information Technology Security Evaluation Criteria 1991 (Kritéria hodnocení bezpečnosti informační technologie 1991).

IC PP Smartcard Integrated Circuit Protection Profile (integrovaný obvod ochrany čipové karty).

ES PP Smart Card Integrated Circuit with Embedded Software Protection Profile (integrovaný obvod čipové karty s vloženou ochranou programového vybavení).

3. **Princip výrobku**

3.1 *Popis karty tachografu a postup užití*

Karta tachografu je čipová 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 činnostem;

— ukládání dat o činnostech držitele karty, událostech a závadách a kontrole činností 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 životní 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 čipové karty, který je popsán v ES PP.

3.3 ***Ohrožení bezpečnosti***

Mimo obecného ohrožení bezpečnosti čipové 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 konce 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 činnostech uložených na TOE by byla bezpečnostním ohrožením TOE.
T.Data_Exchange	Úspěšná změna dat o činnostech (doplnění, vypuštění, změna) v průběhu importu nebo exportu by byla bezpečnostním ohrožením TOE.

3.3.2 *Cesty napadení*

Prvky TOE mohou být napadeny takto:

— pokusem o nedovolené získání znalosti konstrukce technického a programového vybavení TOE, a zvláště jejich bezpečnostních funkcí nebo bezpečnostních dat. Nedovoleně lze znalost získat vstupem do materiálů konstruktéra nebo výrobce (krádež, uplácení atd.) nebo přímým prověřením TOE (fyzické pokusy, analýza výsledků atd.),

— získáním výhod z nedostatků v konstrukci nebo v realizaci TOE (využití závad technického vybavení, závady programového vybavení, chyby v přenosu, závady TOE vyvolané napadením prostředí, využití nedostatků v bezpečnostních funkcích, jako je postup prokazování totožnosti, data řízení přístupu, šifrovací operace...).

— změna TOE nebo jeho bezpečnostních funkcí fyzickým, elektrickým nebo logickým napadením nebo jejich kombinací.

3.4 ***Cíle bezpečnosti***

Hlavním bezpečnostním cílem systému digitálního tachografu je toto:

O.Main	Kontrolním orgánům musí být ke kontrole dostupná data, jež plně a přesně udávají činnosti 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 čipové karty popsaného 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 životním 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 fyzické, personální a procedurální***

Fyzické, 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**

Tento odstavec upřesňuje některé povolené operace, jako je přiřazení nebo volba ES PP, a stanovuje doplňující funkční požadavky SEF.

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 ověřit, zda se jedná o ověřený celek ve vozidle nebo nikoliv. Karta 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 ověřil, 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 akcí zprostředkovaných TSF*: žádný.

Přiřazení (FIA_ATD.1.1) *Soupis bezpečnostních vlastností*::

USER_GROUP VEHICLE_UNIT, NON_VEHICLE_UNIT,

USER_ID Registrační číslo vozidla a kód členského státu registrace (USER_ID je znám pouze pro USER_GROUP = VEHICLE_UNIT)

4.2.2 *Prokázání totožnosti uživatele*

Přiřazení (FIA_UAU.1.1) *Soupis bezpečnostních akcí TSF*.

— Karta řidiče a karta dílny: Export dat uživatele s bezpečnostními vlastnostmi (funkce stahování 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 zjištění, 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 (mechanismy) k prokázání totožnosti*: jakýkoliv mechanismus k prokázání totožnosti.

UIA_302 Karta dílny 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 karty dílny).

4.2.3 *Selhání v prokázání totožnosti*

Následující přiřazení popisují kreakci 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 (karta dílny).

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.1.1) *Jmenovitá skupina bezpečnostních atributů*: USER_GROUP.

Přiřazení (FDP_ACF.1.2) *Pravidla řídící 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 životního cyklu karty.
ACTIVITY_WRITE:	Data o činnostech mohou být zapisována do TOE pouze celkem ve vozidle.
SOFT_UPGRADE:	Žádný z uživatelů nemůže modernizovat programové vybavení TOEe.
FILE_STRUCTURE:	Struktura souborů a podmínky přístupu musí být vytvořeny před koncem fáze 6 životního 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 zajištěno uvedení času a data personalizace TOE. Údaje musí být nezaměnitelné.

4.5 ***Audit***

TOE musí sledovat události, které označují možná poškozování jeho bezpečnost.

Přiřazení (FAU_SAA.1.2) *Dílčí sada definovaných událostí podléhajících auditu*.

— selhání v prokázání totožnosti držitele karty (5 po sobě jsoucích neúspěšných ověření PIN),

— závada v autotestech,

— závada úplnosti (integrity) uložených dat,

— závada úplnosti (integrity) vstupních dat o činnostech.

4.6 ***Přesnost***

4.6.1 *Úplnost (integrita) 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 činnostech.

Přiřazení (FDP_DAU.1.2) *Soupis témat*: jakékoliv.

Požadavky tohoto bodu se použijí, pouze je-li VU tvořen fyzicky oddělenými částmi.

4.7 ***Spolehlivost funkce***

4.7.1 *Zkoušky*

Výběr (FPT_TST.1.1): v průběhu počátečního nastartování, pravidelně 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 programového vybavení, který není uložen na ROM.

RLB_302 Po zjištění závady v autotesty musí TSF varovat připojenou jednotku.

RLB_303 Po dokončení zkoušky OS 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 životního cyklu nesmějí být nikdy přístupné v průběhu jiného stavu.

4.7.2 *Programové vybavení*

RLB_304 Nesmí existovat žádný způsob, jak při užívání TOE analyzovat, ladit nebo měnit programové vybavení.

RLB_305 Vstupy z vnějších zdrojů nesmějí 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.

4.7.4 *Podmínky obnovení nastavení (resetování)*

RLB_307 V případě přerušení napájení (nebo kolísání napájecího napětí) dotýkajícího se TOE, zastavení transakce před jejím ukončením nebo při jiných podmínkách resetování musí být TOE zcela resetován.

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 musí TOE:

— 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 totožnost získaných dat.

4.8.2 *Export dat do celků mimo vozidlo (funkce stahování)*

DEX_304 TOE musí být schopno generovat důkaz o původu dat stahovaných do externích médií.

DEX_305 TOE musí být schopno zajistit příjemci možnost ověření důkazu o původu stahovaných dat.

DEX_306 TOE musí být schopen stahovat data do externích paměťových médií společně s bezpečnostními vlastnostmi tak, aby mohla být úplnost (integrita) stahovaných 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											cíle IT								
	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*	O.DIS_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 programového vybavení												x		x						
RLB_302 Autotest												x		x						
RLB_303 Zkoušky při výrobě					x	x						x		x						
RLB_304 Analyza programového vybavení					x		x	x				x		x						
RLB_305 Vstup programového vybavení					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 paměťových medií											x									x
CSP_301 Generace klíče												x								x
CSP_302 Distribuce klíče												x								x

Dodatek 11

SPOLEČNÉ BEZPEČNOSTNÍ MECHANISMY

OBSAH

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, FIPS Publication 180-1: Secure Hash Standard, duben 1995
PKCS1	RSA Laboratories. PKCS # 1: RSA Encryption Standard. Version 2.9. October 1998.
TDES	National Institute of Standards and Technology, FIPS Publication 46-3: Data encryption Standard, Draft 1999.
TDES-OP	ANSI X9.52, Triple Data Encryption Algorithm Modes of Operation. 1998.
ISO/IEC 7816-4	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 veřejného 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	veřejný klíč RSA, veřejný zmocněnec,
E()	šifrování pomocí DES,
EQT	zařízení,
Hash()	hodnota transformace, výstup transformace,
Hash	transformační funkce,
KID	identifikátor klíče,
Km	klíč TDES. Hlavní klíč podle definice ISO 16844-3,
Km_{vu}	klíč TDES, vložený do celku ve vozidle,
Km_{wc}	klíč TDES, vložený do karty dílny,
m	celé číslo mezi 0 a n-1 reprezentující zprávu,
n	klíče RSA, modul,
PB	doplňkové bajty,
PI	indikační doplňkový bajt (užití v šifře pro důvěrnost DO),
PV	jednoduchá hodnota,
s	představitel podpisu, celé číslo mezi 0 a n-1,
SSC	čítač odeslané 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 certifikační orgánem,
X.CA	certifikační orgán uživatele X,
$X.CA.PK_oX.C$	operace rozbalení certifikátu pro vyjmutí veřejného klíče. Je to zaváděcí operátor, jehož levý operand je veřejným klíčem certifikačního orgánu a jehož pravý operand je certifikátem vydaným certifikačním orgánem. Výstupem je veřejný klíč uživatele X, jeho certifikát je pravým operandem,

X.PK	veřejný klíč uživatele X,
X.PK[I]	RSA zašifrování některých informací I při užití veřejného 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.

2. ŠIFROVACÍ SYSTÉMY A ALGORITMY ŠIFROVÁNÍ

2.1 **Šifrovací systémy**

CSM_001 VU a karty tachografu musí užívat klasický šifrovací systém RSA veřejného klíče k tomu, aby vytvořily následující bezpečnostní mechanismy:

— prokazování totožnosti mezi VU a kartami,

— převod trojitých DES klíčů jednání mezi VU a karet tachografů,

— digitální podpis dat převedených z VU nebo karet tachografu do externích médií.

CSM_002 VU a karty tachografu musí užívat trojitý DES symetrický šifrovací systém k tomu, aby v průběhu výměny dat uživatele mezi VU a kartami tachografu vytvořily mechanismus pro udržení úplnosti dat a aby popřípadě zajistily důvěrnost výměny dat mezi VU a kartami tachografu.

2.2 **Algoritmy šifrování**

2.2.1 ***Algoritmus RSA***

CSM_003 Algoritmus RSA je plně definován následujícími rovnicemi:

$$X.SK[m] = s = m^d \bmod n$$

$$X.PK[s] = m = s^e \bmod n$$

Obsažnější popis funkce RSA lze nalézt v odkazu (PKCS1).

Veřejný 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 **Generování a distribuce klíčů**

3.1.1 ***Generování a distribuce klíčů RSA***

CSM_006 Klíče RSA musí být generovány prostřednictvím tří funkčních úrovní:

— evropská úroveň,

— úroveň členského státu,

— úroveň zařízení.

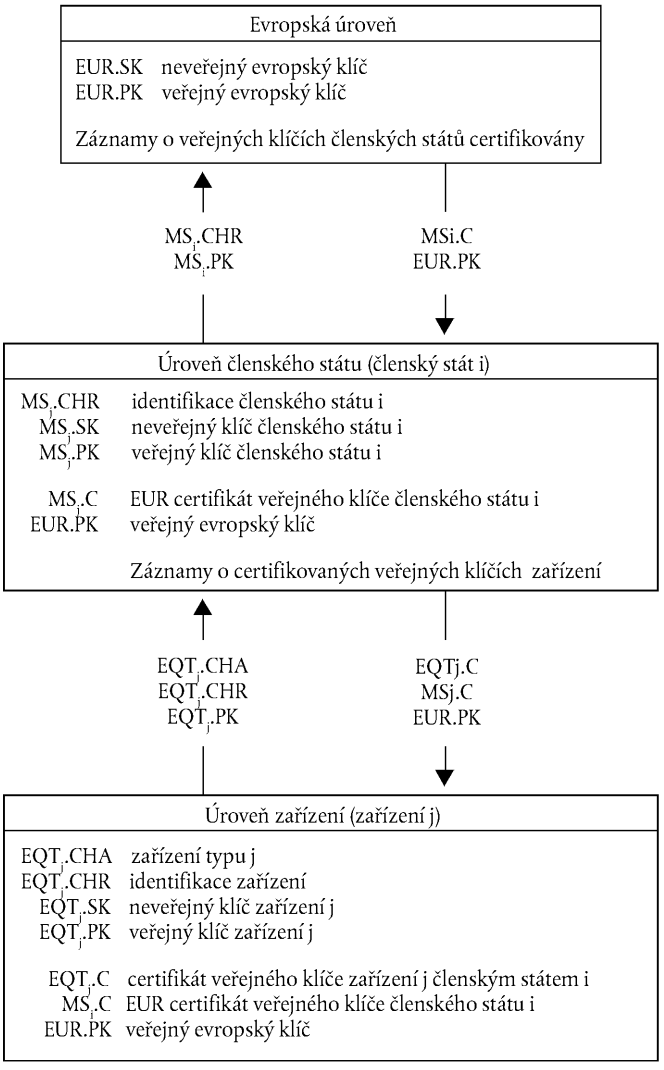
CSM_007 Na evropské úrovni musí být generován jediný pár evropských klíčů (EUR.SK a EUR.PK). Evropský neveřejný klíč musí být užíván k certifikaci veřejných klíčů členských států. Musí být udržovány záznamy o všech certifikovaných klíčích. Tento cíl musí zajišťovat Evropský certifikační úřad pod pravomocí 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 Evropským certifikačním úřadem. Neveřejný klíč členského státu se musí užívat k certifikaci veřejných klíčů, které se mají vkládat do zařízení (VU nebo karta tachografu). Musí být udržovány záznamy o všech certifikovaných veřejných klíčích spolu s identifikací zařízení, pro která jsou určeny. Tento cíl musí zajišťovat certifikační orgán 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. Veřejné klíče zařízení musí být certifikovány certifikačním orgánem členského státu. Tyto povinnosti mají být zajištěny výrobci zařízení, adresáty zařízení nebo organizacemi členského státu. Tento pár klíčů se užívá pro prokazování totožnosti, digitální podpis a šifrovací služby.

CSM_010 Během generování, dopravy (popřípadě) a skladování musí být zachována důvěrnost neveřejných klíčů.

Toto vyobrazení shrnuje tok dat v tomto procesu:



3.1.2 ***Zkušební klíče RSA***

CSM_011 Pro zkoušení zařízení (včetně zkoušek vzájemné operační součinnosti) musí Evropský certifikační úřad generovat odlišný jediný evropský pár zkušebních klíčů a nejméně dva páry zkušebních klíčů členských států, z nich veřejné klíče musí být certifikovány neveřejným evropským zkušebním 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 generování, dopravy (popřípadě) a skladování.

Pro podporu vyhovění záznamového zařízení normě ISO 16844 musí Evropský certifikační úřad a dále certifikační orgány členských států zajistit následující:

CSM_036 Evropský certifikační úřad musí generovat Km_{VU} a Km_{WC}, dva nezávislé a jedinečné klíče Triple DES, a generovat Km jako:

$$Km = Km_{VU} \text{ XOR } Km_{WC}$$

Evropský certifikační úřad musí tyto klíče za příslušných bezpečných postupů předat na vyžádání členských států jejich certifikačním orgánům.

CSM_037 Certifikační orgány členských států musí:

— užít Km k šifrování dat snímače pohybu podle požadavku výrobce snímače pohybu (fata, která mají být šifrována pomocí Km, definuje ISO 16844-3),

— předat Km_{VU} výrobcům VU pro vložení do VU za náležitě zabezpečených postupů,

— zajistit, aby Km_{WC} bylo v průběhu personalizace karty vloženo do všech karet dílny (*SensorInstallationSecData* do základního souboru *Sensor_Installation_Data*).

3.1.4 ***Klíče snímače pohybu***

CSM_012 VU 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) 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, veřejný 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 veřejných klíčů musí být certifikáty ‚non self-descriptive' (nepopisné) ‚card verifiable' (ověřující kartu) (viz ISO/IEC 7816-8).

3.3.1 ***Obsah certifikátu***

CSM_017 Certifikáty veřejných klíčů RSA jsou tvořeny těmito daty a následujícím pořadím:

Data	Formát	Bajtů	Předmět
CPI	INTEGER	1	Identifikátor profilu certifikátu (pro tuto verzi (‚01‘)
CAR	OCTET STRING	8	Odkaz na certifikační orgán
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	Veřejný klíč (modul)
e	OCTET STRING	8	Veřejný klíč (veřejný 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 veřejného klíče (sestrojit)	Délka následujících DO	Jmenovka modulu	Délka modulu	Jmenovka veřejného exponentu	Délka veřejného exponentu

2. ‚Odkaz na certifikační orgán‘ (CAR) má za účel identifikovat orgán vydávající certifikát (CA) tak, aby prvek dat mohl být užit současně jako identifikátor klíče organizace pro odkaz na veřejný klíč certifikačního orgánu (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 prvek dat současně jako identifikátor předmětu klíče a jako odkaz na veřejný klíč držitele certifikátu.

5. Identifikátory klíčů jednoznačně identifikují držitele certifikátu nebo certifikační orgány. Ty jsou kódovány takto:

   5.1 Zařízení (VU nebo karta)

Data	Výrobní číslo zařízení	Datum	Typ	Výrobce
Délka	4 bajty	2 bajty	1 bajt	1 bajt
Hodnota	Celé číslo	kódování mm yy BCD	Specifické podle výrobce	Kód výrobce

Při požadování certifikátu pro VU může nebo nemusí výrobce znát identifikaci zařízení, do kterého bude klíč vložen.

V prvém případě zašle výrobce identifikaci zařízení s veřejným klíčem certifikačního orgánu svého členského státu. Certifikát bude v takovém případě zahrnovat identifikaci zařízení a výrobce musí zajistit, že klíče a certifikáty budou vloženy do uvažovaného zařízení. 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 veřejným klíčem certifikačnímu orgánu 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 bajty	2 bajty	1 bajt	1 bajt
Hodnota	BCD kódování	kódování mm jj BCD	'FF'	Kód výrobce

5.2 Certifikační orgán

Data	Identifikace orgánu	Pořadové číslo klíče	Přídavné informace	Identifikátor
Délka	4 bajty	1 bajt	2 bajty	1 bajt
Hodnota	1 bajt vnitrostátní číselný kód 3 bajty 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.

6. Ověřovatel certifikátu musí bezpodmínečně znát, že veřejný certifikovaný klíč je RSA klíč platný pro ověřování totožnost, ověření digitálního podpisu a šifrovaný pro důvěrnost služeb (certifikát nezahrnuje žádný 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 ‚Odkazem na certifikační orgán'.

$$X.C = X.CA.SK['6A' \,||\, C_r \,||\, Hash(Cc) \,||\, 'BC'] \,||\, C_n \,||\, X.CAR$$

Kde je obsah certifikátu $= Cc = \underset{106\text{ bajtů}}{C_r} \,||\, \underset{58\text{ bajtů}}{C_n}$

Poznámky:

1. Tento certifikát je dlouhý 194 bajtů.

2. K podpisu je dále připojen podpisem překrytý odkaz na certifikační orgán (CAR) tak, že veřejný klíč certifikačního orgánu může být vybrán pro ověření certifikátu.

3. Ověřovatel certifikátu musí bezpodmínečně znát algoritmus užívaný certifikačním orgánem k podpisování certifikátu.

4. Návěští spojené s obsahem certifikátu je následující:

´7F 21´	´09´	´5F 37´	´81 80´	´5F 38´	´3A´	´42´	´08´
Jmenovkacertifikátu CV(sestrojena)	Délka následujících DO	Jmenovka podpisu	Délka podpisu	Ostaní 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 veřejného klíče, který zahrnuje: X.PK = X.CA.PK$_o$X.C, a ověření platnosti certifikátu.

CSM_019 Zahrnuje následující kroky:

Ověřte podpis a vyvolejte obsah:

— z X.C vyvolejte Sign, C_n′aCAR′: X.C = Sign (128 bajtů) || C_n´ (58 bajtů) || CAR (8 bajtů)

— z CAR′ vyberte příslušný veřejný klíč certifikačního orgánu (pokud nebylo již vybráno jinými prostředky),

— otevřete Sign pomocí veřejného klíče CA: Sr′ = X.CA.PK [Sign],

— ověření Sŕzačíná na ′6A′ a končí na ′BC′,

— Vypočítejte Cr′ a H′ ze vztahu: Sr´ = ´6A´ || Cr´ (106 bajtů) || H´ (20 bajtů) || ´BC´

— obnovte obsah certifikátu C′ = C_r′ || C_n′,

— ověřte *Hash*(C′) = H′

Pokud jsou ověření v pořádku, je certifikát pravý a jeho obsahem je C′.

Ověřte platnost. z C′:

— pokud je použitelné, ověřte datum ukončení platnosti.

Z C′ vyvolejte a uložte veřejný klíč, identifikátor klíče, autorizaci držitele certifikátu a platnost:

— X.PK = *n* || *e*,

— X.KID = CHR

— X.CHA = CHA,

— X.EOV = EOV.

4. VZÁJEMNÉ PROKÁZÁNÍ TOTOŽNOSTI

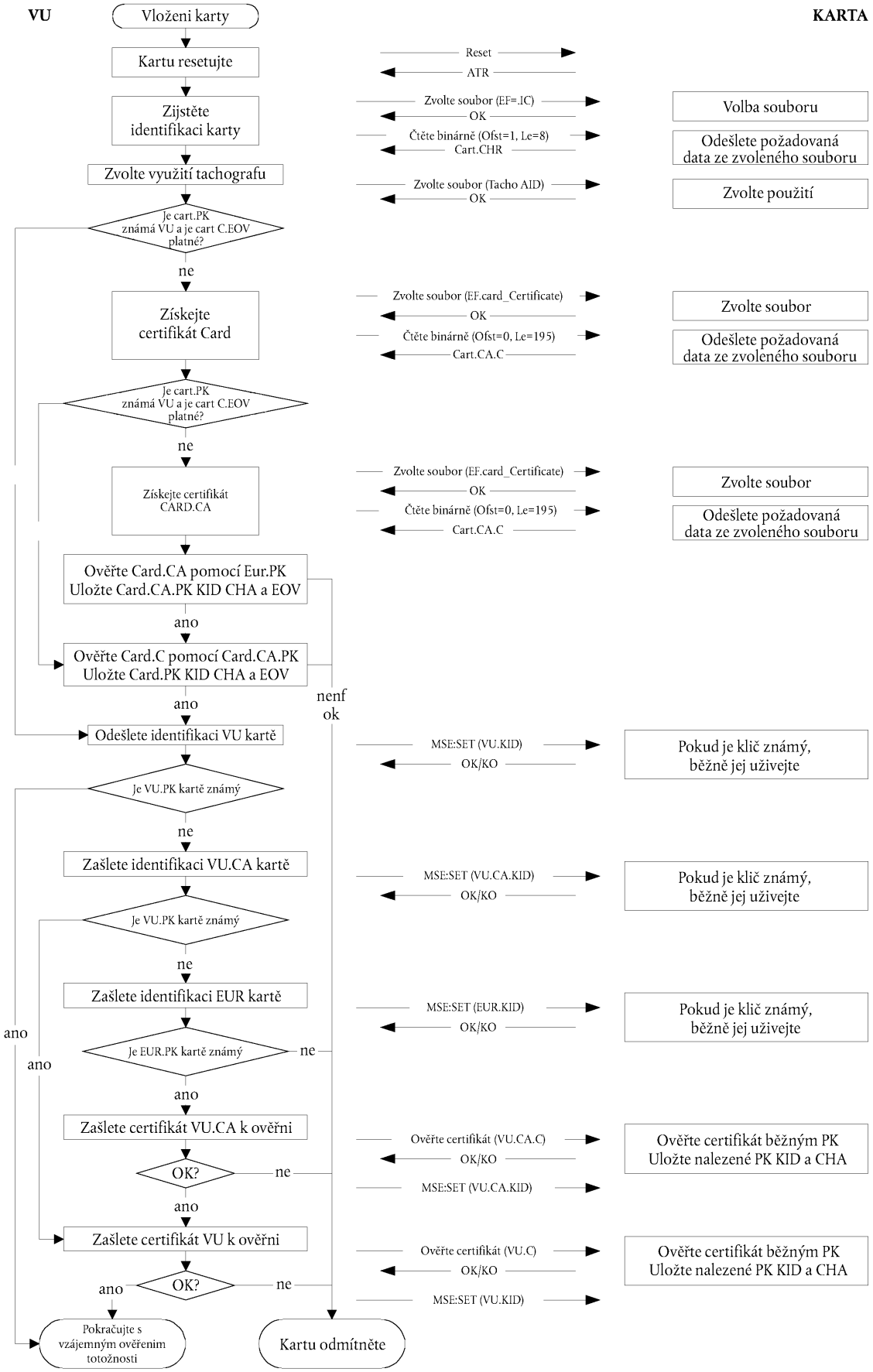
Vzájemné prokázání totožnosti mezi kartami a VU je založeno na následujícím principu:

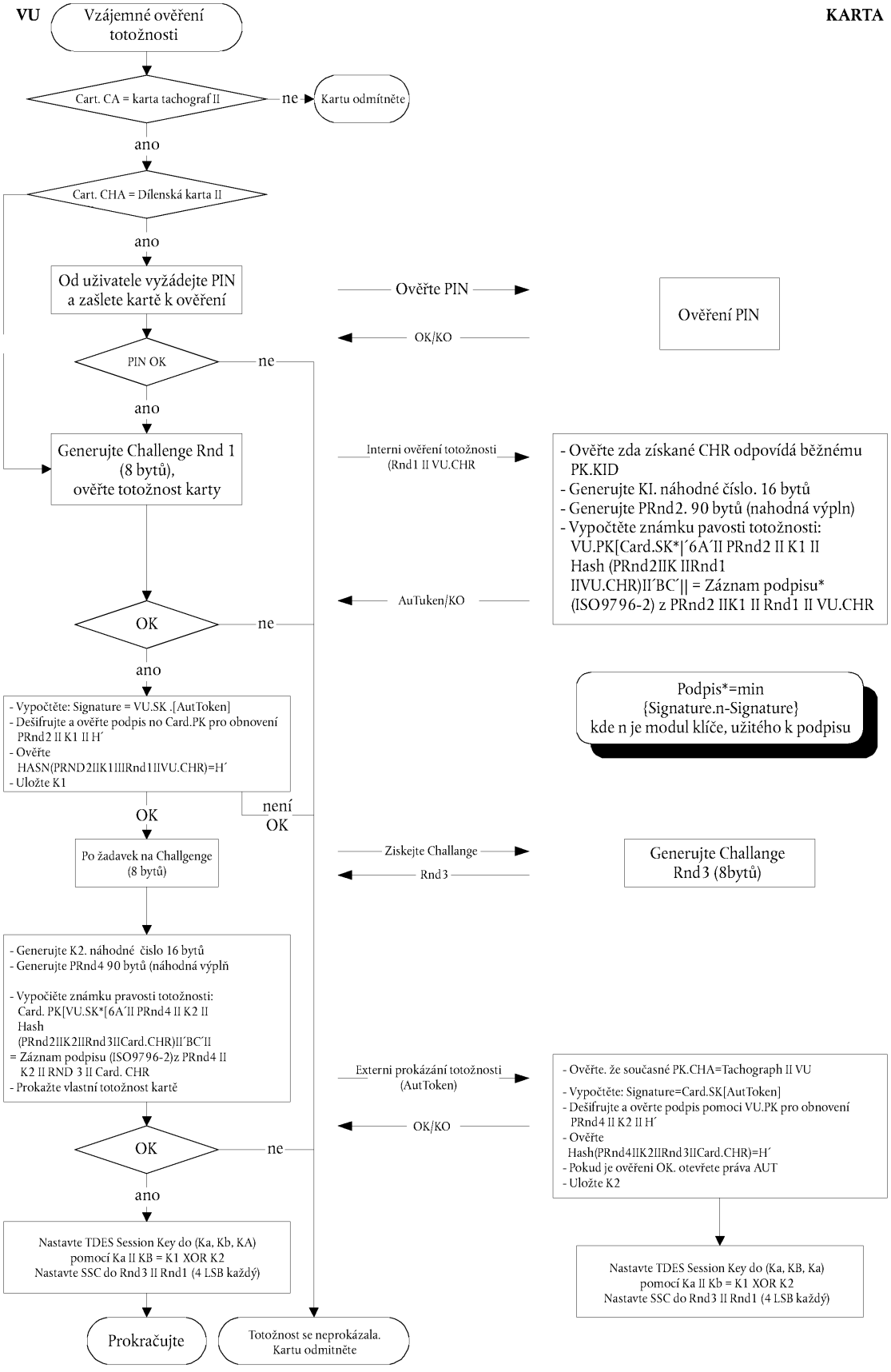
Každá strana dokládá druhé straně, že vlastní platný pár klíčů, ze kterých byl veřejný klíč certifikován certifikačním orgánem členského státu, a že sama byla certifikována Evropským certifikačním úřadem.

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 vložením karty do VU. Mechanismus začíná výměnou a rozvinutím veřejného klíče a končí nastavením klíče relace.

CSM_020 Použit musí být dále uvedený protokol (šipky označují povely a výměnu dat (viz dodatek 2)):




VU
KARTA
Vzájemné ověření totožnosti
Cart. CA = karta tachograf II
ne
Kartu odmítněte
ano
Cart. CHA = Dílenská karta II
ano
Od uživatele vyžádejte PIN a zašlete kartě k ověření
Ověřte PIN
Ověření PIN
OK/KO
PIN OK
ne
ano
Generujte Challenge Rnd 1 (8 bytů), ověřte totožnost karty
Interni ověření totožnosti (Rnd1 II VU.CHR
- Ověřte zda získané CHR odpovídá běžnému PK.KID
- Generujte KI. náhodné číslo. 16 bytů
- Generujte PRnd2. 90 bytů (nahodná výpln)
- Vypočtěte známku pavosti totožnosti: VU.PK[Card.SK*|´6A´II PRnd2 II K1 II Hash (PRnd2IIK IIRnd1 IIVU.CHR)II´BC´|| = Záznam podpisu* (ISO9796-2) z PRnd2 IIK1 II Rnd1 II VU.CHR
AuTuken/KO
OK
ne
ano
Podpis*=min {Signature.n-Signature} kde n je modul klíče, užitého k podpisu
- Vypočtěte: Signature = VU.SK .[AutToken]
- Dešifrujte a ověřte podpis no Card.PK pro obnovení PRnd2 II K1 II H´
- Ověřte HASN(PRND2IIK1IIIRnd1IIVU.CHR)=H´
- Uložte K1
není OK
OK
Po žadavek na Challgenge (8 bytů)
Ziskejte Challange
Rnd3
Generujte Challange Rnd3 (8bytů)
- Generujte K2. náhodné čislo 16 bytů
- Generujte PRnd4 90 bytů (náhodná výplň
- Vypočtěte známku pravosti totožnosti: Card. PK[VU.SK*[6A´II PRnd4 II K2 II Hash (PRnd2IIK2IIRnd3IICard.CHR)II´BC´II = Záznam podpisu (ISO9796-2)z PRnd4 II K2 II RND 3 II Card. CHR
- Prokažte vlastní totožnost kartě
Externi prokázání totožnosti (AutToken)
- Ověřte. že současné PK.CHA=Tachograph II VU
- Vypočtěte: Signature=Card.SK[AutToken]
- Dešifrujte a ověrte podpis pomoci VU.PK pro obnovení PRnd4 II K2 II H´
- Ověřte Hash(PRnd4IIK2IIRnd3IICard.CHR)=H´
- Pokud je ověřeni OK. otevřete práva AUT
- Uložte K2
OK/KO
OK
ne
ano
Nastavte TDES Session Key do (Ka, Kb, KA) pomocí Ka II KB = K1 XOR K2 Nastavte SSC do Rnd3 II Rnd1 (4 LSB každý)
Nastavte TDES Session Key do (Ka, KB, Ka) pomocí Ka II Kb = K1 XOR K2 Nastavte SSC do Rnd3 II Rnd1 (4 LSB každý)
Prokračujte
Totožnost se neprokázala. Kartu odmitněte

5. DŮVĚRNOST PŘENOSU DAT KARET VU, ÚPLNOST A MECHANISMUS PROKAZOVÁNÍ TOTOŽNOSTI

5.1 **Bezpečné zpracování zpráv**

CSM_021 Úplnost přenosu dat VU karet musí být chráněna prostřednictvím bezpečného zpracování zpráv podle odkazových norem 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 ‚kontrolní součet šifrovaných dat'.

CSM_023 Kontrolní součet šifrovaných dat zaslaný v rámci příkazu musí zahrnovat záhlaví povelu a veškeré odeslané datové objekty (= > CLA = ′0C′ a veškeré datové objekty musí být uzavřeny jmenovkou, ve které je B1 = 1).

CSM_024 Pokud odezva neobsahuje datové pole, musí být stavové informační bajty ochráněny kontrolním součtem šifrovaných dat.

CSM_025 Kontrolní součet šifrovaných dat musí být dlouhý čtyři bajty.

Struktura povelů a odezev při užití bezpečného zpracování dat je proto následující:

Užité DO jsou částečné soubory DO bezpečného zpracování zpráv podle popisu v ISO/IEC 7816-4:

Příznak	Symbol	Význam
′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′	$T_{PI\ CG}$	Bajtový indikátor naplnění || 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 bajty	L bajty, označené jako B_1 až B_L

Těleso odezvy	Znak odezvy
(pole dat)	SW1 SW2
L_r datové bajty	dva bajty

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 bajty (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 bajty.

Data zahrnutá do kontrolního součtu = $T_{PI\ CG}$ || $L_{PI\ CG}$ || PI CG || PB

3. Případ, 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 bezpečném zpracování zpráv**

CSM_026 Pokud karta tachografu při převodu příkazu zjistí závadu SM, musí být stavové bajty vráceny bez SM. Podle ISO/IEC 7816-4 jsou pro závadu na SM definovány následující bajty:

'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 bajty bez SM DO nebo se závadným SM DO, musí VU 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(Ka, SSC),

— následující krok: užitím Ka se vypočtou zkušební bloky y1, …. yn,

— konečný krok: šifrovací kontrolní součet se vypočte z posledního zkušebního bloku yn takto: E(Ka, D(Kb, yn)),

kde E() znamená šifrování s DES a D() znamená rozšifrování s DES.

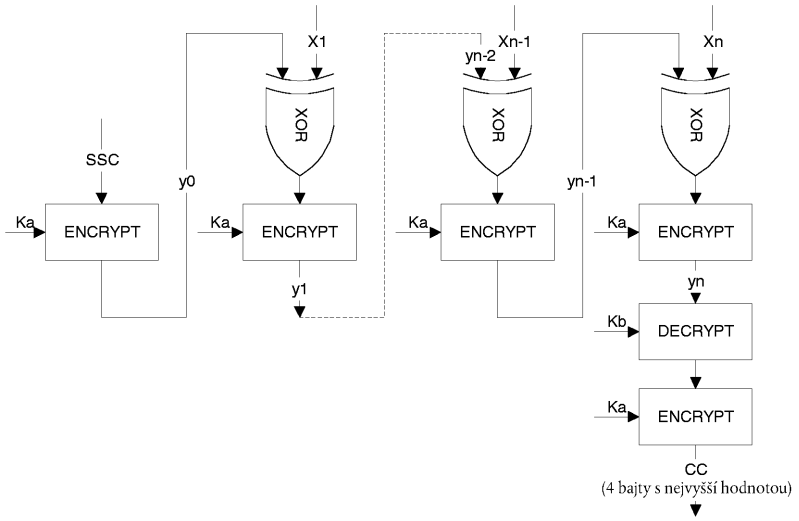
Přenášejí se čtyři bajty s nejvyšší hodnotou šifrovacího kontrolního součtu.

CSM_029 V průběhu odsouhlasení klíče se ‚čítač odeslané posloupnosti' (SSC) inicializuje takto:

výchozí SSC: Rnd3 (4 bajty s nejnižší hodnotou) ď£¬ď£¬ Rnd 1 (4 bajty 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).

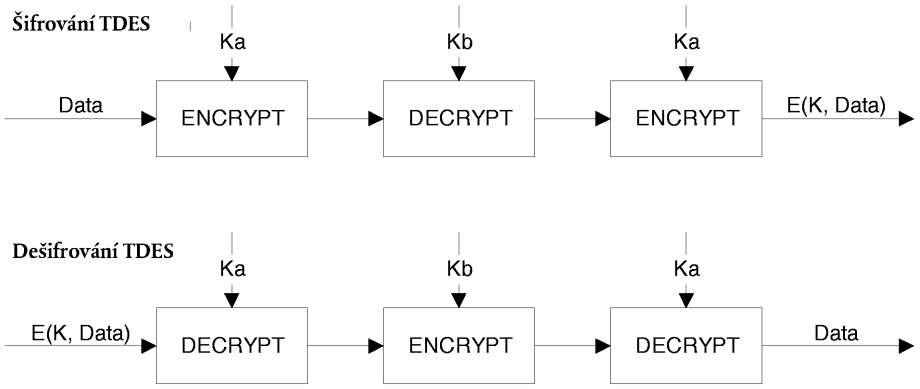
Následující vyobrazení uvádí výpočet MAC:



5.4 **Algoritmus výpočtu šifer pro důvěrnost DOs**

CSM_031 šifry se vypočtou užitím TDEA v módu TCBC podle odkazu (TDES) a (TDES-OP) spolu s nulovým vektorem jako výchozí bloku hodnot.

Toto vyobrazení uvádí využití klíčů v TDES:



6. MECHANISMY DIGITÁLNÍCH PODPISŮ PŘI STAHOVÁNÍ DAT

CSM_032 Přiřazené inteligentní zařízení (IDE) ukládá data ze zařízení (VU nebo karta) v průběhu relace stahování do jednoho fyzického souboru dat. Tento soubor musí zahrnovat certifikáty MS_i.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 **Generování podpisu**

CSM_034 Generování dat podpisu zařízením probíhá podle schématu podpisu definovaném v odkazu PKCS1 s dodatkem a s transformační funkcí SHA-1:

Podpis = EQT.SK['00' || '01' || *PS* || '00' || DER(SHA-1(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.

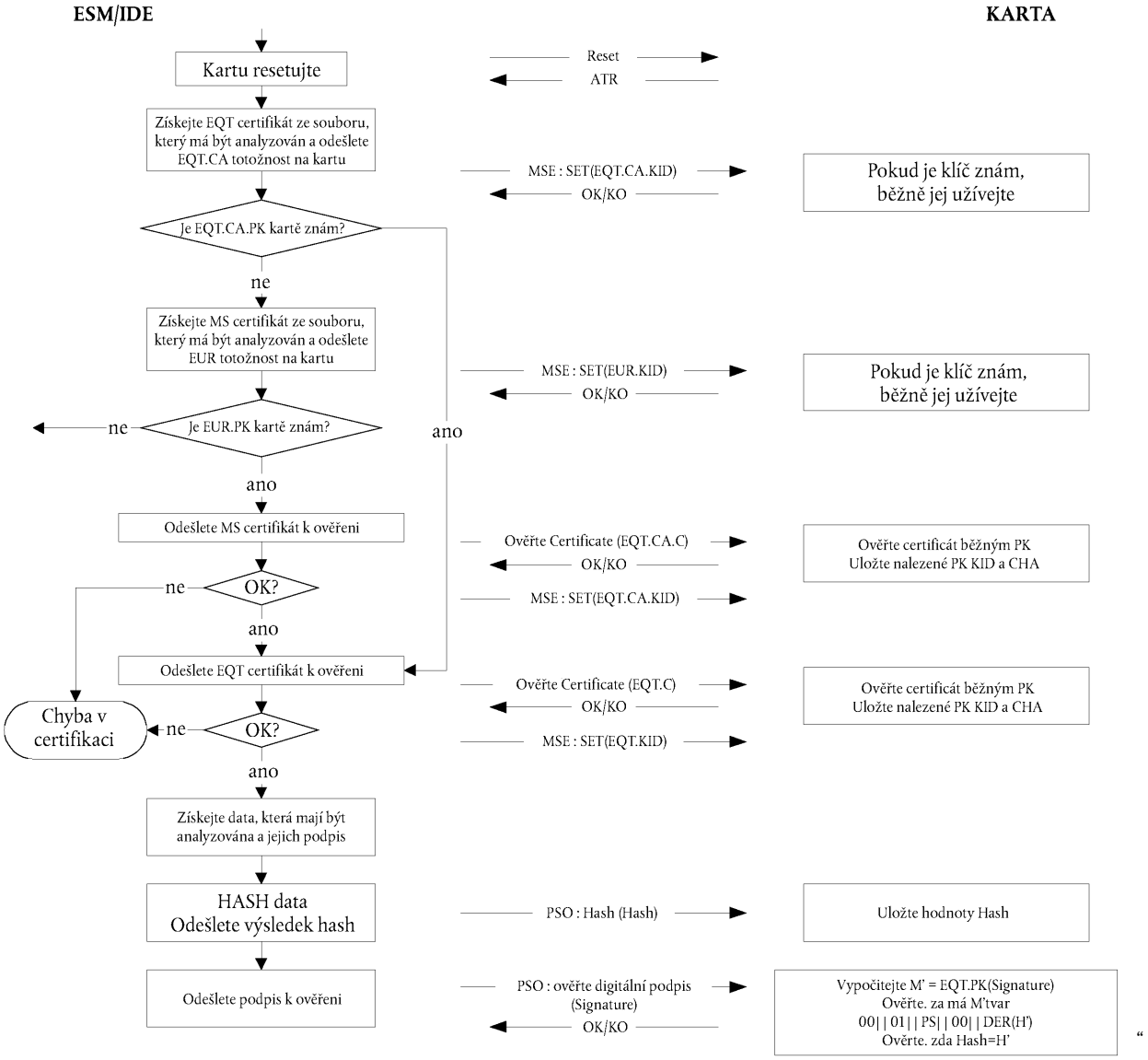
6.2 **Ověření podpisu**

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 externí paměťové médium (ESM). 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.


ESM/IDE
KARTA
Kartu resetujte
Reset
ATR
Získejte EQT certifikát ze souboru, který má být analyzován a odešlete EQT.CA totožnost na kartu
MSE : SET(EQT.CA.KID)
OK/KO
Pokud je klíč znám, běžně jej užívejte
Je EQT.CA.PK kartě znám?
ne
Získejte MS certifikát ze souboru, který má být analyzován a odešlete EUR totožnost na kartu
MSE : SET(EUR.KID)
OK/KO
Pokud je klíč znám, běžně jej užívejte
ne
Je EUR.PK kartě znám?
ano
ano
Odešlete MS certifikát k ověření
Ověřte Certificate (EQT.CA.C)
OK/KO
Ověřte certifikát běžným PK
Uložte nalezené PK KID a CHA
ne
OK?
MSE : SET(EQT.CA.KID)
ano
Odešlete EQT certifikát k ověření
Ověřte Certificate (EQT.C)
OK/KO
Ověřte certifikát běžným PK
Uložte nalezené PK KID a CHA
Chyba v certifikaci
ne
OK?
MSE : SET(EQT.KID)
ano
Získejte data, která mají být analyzována a jejich podpis
HASH data
Odešlete výsledek hash
PSO : Hash (Hash)
Uložte hodnoty Hash
Odešlete podpis k ověření
PSO : ověřte digitální podpis (Signature)
OK/KO
Vypočítejte M' = EQT.PK(Signature)
Ověřte. za má M'tvar
00| | 01| | PS| | 00| | DER(H')
Ověrte. zda Hash=H'

“