NARIADENIE RADY (EHS) č. 3821/85

z 20. decembra 1985

o záznamovom zariadení v cestnej doprave

RADA EURÓPSKYCH SPOLOČENSTIEV,

so zreteľom na Zmluvu o založení Európskeho hospodárskeho spoločenstva a najmä na jej článok 75,

so zreteľom na návrh Komisie[1];

so zreteľom na stanovisko Európskeho parlamentu[2];

so zreteľom na stanovisko Hospodárskeho a sociálneho výboru[3];

keďže nariadenie (EHS) č. 1463/70[4] naposledy zmenené a doplnené nariadením (EHS) č. 2828/77[5] zaviedlo záznamové zariadenie v cestnej doprave;

keďže berúc do úvahy úpravy uvedené ďalej, za účelom objasnenia problémov by všetky relevantné opatrenia mali byť zhrnuté v jednom texte a v dôsledku toho nariadenie (EHS) č. 1463/70 rady by malo byť zrušené; keďže oslobodenia stanovené v článku 3(1) pre určité osobné prepravy by mali zostať v platnosti určitý čas;

keďže používanie záznamového zariadenia, ktoré môže určiť časové úseky uvedené v Nariadení (EHS) č. 3820/85 o harmonizácii určitých sociálnych právnych predpisov týkajúcej sa cestnej dopravy[6], je zamerané na zabezpečenie účinnej kontroly týchto sociálnych právnych predpisov;

keďže povinnosť používať takéto záznamové zariadenie môže byť uložená len pre vozidlá registrované v členských štátoch; keďže okrem toho niektoré takéto vozidlá môžu, bez toho, aby vznikli ťažkosti, byť vylúčené z rámca platnosti tohto nariadenia;

keďže členské štáty by mali byť zmocnené na základe oprávnenia Komisie, udeľovať určitým vozidlám výnimky z ustanovení nariadenia za výnimočných okolností; keďže v naliehavých prípadoch by malo byť možné udeľovať tieto výnimky na obmedzený čas bez predchádzajúceho schválenia Komisie;

keďže pre zabezpečenie účinnej kontroly musí byť zariadenie pri práci spoľahlivé, ľahko používateľné a musí byť konštruované takým spôsobom, aby sa minimalizovala možnosť podvádzania pri jeho používaní; keďže záznamové zariadenie by malo konkrétne mať schopnosť poskytovať na zvláštnych listoch pre každého vodiča a v dostatočne presnej a ľahko čitateľnej forme, zaznamenané podrobnosti o rôznych časových úsekoch;

keďže automatické zaznamenávanie iných podrobnosti o jazde vozidla, ako je rýchlosť a vzdialenosť, podstatne prispeje k bezpečnosti na ceste a podporí citlivú jazdu vozidla; pretože v dôsledku toho sa zdá byť vhodné zabezpečiť, aby zariadenie zapisovalo aj tieto údaje;

keďže je potrebné stanoviť normy spoločenstva pre konštrukciu a inštaláciu záznamového zariadenia a zabezpečiť schvaľovací postup EHS, aby sa vylúčili akékoľvek prekážky pri registrácii vozidiel vybavených takýmto záznamovým zariadením na území členských štátov, pri ich uvedení do prevádzky alebo používaní, alebo pri používaní takéhoto zariadenia;

keďže v prípade rozdielnych názorov medzi členskými štátmi, pokiaľ ide o EHS typové schvaľovania, by mala byť Komisia zmocnená rozhodovať v spore do šiestich mesiacov, ak príslušné štáty nemôžu dospieť k riešeniu;

keďže by pomohlo pri zavádzaní tohto nariadenia a prevencii voči zneužitiu, vydávanie kópie záznamových listov vodičom, ktorí o to požiadajú;

---

[1] Ú.v. ES C 100 12.4.1984 s. 3 a OJ č. C 223 3.9.1985 s. 5
[2] Ú.v. ES C 122 20.5.1985 s. 168
[3] Ú. v. ES C 104 25.4.1985 s. 4, a Ú.v. ES C 303 25.11.1985 s.29
[4] Ú.v. ES L 164 27.7.1970 s. 1
[5] Ú.v. ES L 334 24.12.1977 s. 11
[6] Pozri stranu 1 tohto Úradného vestníka

keďže v záujme dosiahnutia vyššie uvedených cieľov pri dodržiavaní času práce a odpočinku je potrebné, aby zamestnávatelia a vodiči boli zodpovední za správne fungovanie zariadenia a aby s náležitou starostlivosťou vykonávali predpísané operácie;

keďže opatrenia riadiace počet záznamových listov, ktoré vodič musí mať so sebou, musia byť upravené v dôsledku zmeny flexibilného týždňa na pevný týždeň;

keďže technický pokrok vyžaduje rýchlu adaptáciu technických špecifikácií stanovených v prílohách k tomuto nariadeniu; keďže v záujme uľahčenia implementácie opatrení potrebných pre tento účel, mali by byť stanovené postupy zakladajúce úzku spoluprácu medzi členskými štátmi a Komisiou v rámci poradného výboru;

keďže si členské štáty mali vymieňať dostupné informácie o zistených porušeniach;

keďže v záujme zabezpečenia spoľahlivého a správneho fungovania záznamového zariadenia, je vhodné stanoviť jednotné požiadavky na periodické kontroly a prehliadky, ktorým podlieha zariadenie po inštalácii,

PRIJALA TOTO NARIADENIE :

KAPITOLA I.

Princípy a rozsah pôsobnosti

Článok 1

Záznamové zariadenie v zmysle tohto nariadenia musí, pokiaľ ide o konštrukciu, inštaláciu, použitie a testovanie, spĺňať požiadavky tohto nariadenia a jeho príloha I alebo IB a II, ktoré tvoria neoddeliteľnú súčasť tohto nariadenia.

Článok 2

Na účely tohto nariadenia sa použijú vymedzenia pojmov ustanovené v článku 4 nariadenia Európskeho parlamentu a Rady (ES) č. 561/2006 z 15. marca 2006 o harmonizácii niektorých právnych predpisov v sociálnej oblasti, ktoré sa týkajú cestnej dopravy a ktorým sa menia a dopĺňajú nariadenia Rady (EHS) č. 3821/85 a (ES) č. 2135/98[1].

Článok 3

1. Záznamové zariadenie sa inštaluje a použije vo vozidlách evidovaných v členskom štáte, ktoré sa používajú na cestnú osobnú a nákladnú dopravu, okrem vozidiel uvedených v článku 3 nariadenia (ES) č. 561/ 2006. Vozidlá uvedené v článku 16 ods. 1 nariadenia (ES) č. 561/2006 a vozidlá vyňaté z rozsahu uplatňovania nariadenia (EHS) č. 3820/85, ktoré však už nie sú vyňaté podľa nariadenia (ES) č. 561/2006, musia túto požiadavku splniť do 31. decembra 2007.

2. Členské štáty môžu vyňať vozidlá uvedené v článku 13 ods. 1 a ods. 3 nariadenia (ES) č. 561/ 2006 z rozsahu uplatňovania tohto nariadenia.

3. Členské štáty môžu po povolení Komisie vyňať z rozsahu uplatňovania tohto nariadenia vozidlá používané na dopravné činnosti uvedené v článku 14 nariadenia (ES) č. 561/2006.

4. V prípade vnútroštátnej dopravy členské štáty môžu žiadať inštaláciu a používanie záznamových zariadení v súlade s týmto nariadením v akomkoľvek vozidle, pre ktoré sa inštalácia a používanie tohto zariadenia nevyžaduje podľa odseku 1.

KAPITOLA II

Typové schválenie

[1] Ú. v. EÚ L 102, 11.4.2006, s. 1

Článok 4

Pre účely tejto kapitoly, slová" záznamové zariadenie" znamenajú "záznamové zariadenie a jeho komponenty.

Žiadosti o EHS typové schválenie záznamového zariadenia alebo záznamového listu alebo pamäťovej karty, spolu s vhodnými špecifikáciami predloží výrobca alebo jeho zástupca členskému štátu. Žiadna žiadosť týkajúca sa jedného typu záznamového zariadenia alebo jedného záznamového listu alebo pamäťovej karty nemôže byť predložené viac než jednému členskému štátu.

Článok 5

Členský štát udelí ES typové schválenie komponentu každému typu záznamového zariadenia, modelového záznamového listu alebo pamäťovej karty, ktorý zodpovedá požiadavkám stanoveným v prílohe I alebo IB k tomuto nariadeniu za predpokladu, že členský štát je schopný kontrolovať zhodnosť výrobných modelov so schváleným typom.

Zabezpečenie systému musí spĺňať požiadavky stanovené v Prílohe IB. Komisia konajúc v súlade s postupom stanoveným v článku 18 zabezpečí, aby uvedená príloha určila, že záznamovému zariadeniu nesmie byť udelené ES typové schválenie komponentu, kým celý systém (samotné záznamové zariadenie, karta vodiča a elektrické spojenie s prevodovkou) nepreukázal svoju schopnosť odolávať pokusom o manipuláciu alebo falšovanie údajov týkajúcich sa doby jazdy. Testy potrebné pre tento účel vykonajú odborníci oboznámení s najnovšími technikami manipulácie alebo falšovania.

Akékoľvek zmeny alebo dodatky k schválenému modelu musia mať dodatočné EHS typové schválenia od členského štátu, ktorý udelil pôvodné EHS typové schválenia.

Článok 6

Členské štáty vydajú žiadateľovi značku typového schválenia EHS, ktorá má zodpovedať vzoru znázornenému v prílohe II, pre každý typ záznamového zariadenia alebo záznamového listu alebo pamäťovej karty, ktorý schválili podľa článku 5.

Článok 7

Príslušné orgány členského štátu, ktorým bola predložená žiadosť o typové schválenie, vzhľadom na každý typ záznamového zariadenia alebo záznamového listu alebo pamäťovej karty, ktorý schválili alebo odmietli schváliť, buď pošlú v priebehu 1 mesiaca orgánom iného členského štátu kópiu schvaľovacieho osvedčenia spolu s kópiami relevantných špecifikácií alebo, ak je to možné prípadne oznámia týmto orgánom, že schválenie zamietli; v prípade zamietnutia oznámia dôvody svojho rozhodnutia.

Článok 8

1. Ak členský štát, ktorý udelil EHS typové schválenia, uvedené v článku 5 zistí, že určité záznamové zariadenie alebo záznamový list alebo pamäťová karta, ktoré majú značku typového schválenia EHS ktorú vydal nevyhovujú prototypu, ktorý bol schválený, urobí opatrenia potrebné na zabezpečenie zhody so schváleným prototypom. Prijaté opatrenia sa môžu, ak je to nutné, rozšíriť až na zrušenie EHS typového schválenia.

2. Členský štát, ktorý udelil EHS typové schválenie, odoberie toto schválenie, ak záznamové zariadenie alebo záznamový list alebo pamäťovú kartu ktoré schválil, nie sú v súlade s týmto nariadením alebo jeho prílohami alebo vykazuje pri používaní nejakú všeobecnú chybu, ktorá ho robí nepoužiteľným pre účel, na ktorý bol určený.

3. Ak členský štát, ktorý udelil EHS typové schválenie je iným členským štátom upozornený na jeden z prípadov uvedených v odsekoch 1 a 2, po porade s druhým členským štát urobí opatrenia stanovené v týchto odsekoch, podľa odseku 5.

4. Členský štát, ktorý zistí, že nastal jeden z prípadov uvedených v odseku 2, môže až do ďalšieho oznámenia zakázať uviesť na trh a prevádzkovať záznamové zariadenia alebo záznamové listy alebo pamäťové karty. To isté sa použije v prípadoch uvedených v odseku 1 v súvislosti so záznamovým zariadením alebo so záznamovými listami alebo so záznamovými kartami, ktoré boli oslobodené od úvodného overovania EHS, ak výrobca po náležitom upozornení, neuvedie zariadenie do súladu so schváleným modelom alebo s požiadavkami tohto nariadenia.

V každom prípade sa informujú príslušné orgány členských štátov navzájom a Komisiu do 1 mesiaca o odobratí EHS typového schválenia, alebo o akýchkoľvek iných opatreniach prijatých podľa odsekov 1, 2 a 3 a špecifikujú dôvody svojho konania.

5. Ak členský štát, ktorý udelil EHS typové schválenie, pochybuje o existencii niektorých prípadov špecifikovaných v odseku 1 alebo 2 o ktorých bol informovaný, usilujú sa dotknuté členské štáty vyriešiť spor a informovať o tom Komisiu.

Ak rozhovory medzi členskými štátmi nedospeli k dohode do štyroch mesiacov od termínu oznámenia spomínaného v odseku 3 vyššie, Komisia po porade s expertmi zo všetkých členských štátov a po zvážení všetkých relevantných faktorov, napr. ekonomických a technických faktorov, do šiestich mesiacov prijme rozhodnutie, ktoré oznámi zainteresovaným členským štátom a súčasne aj ostatným členským štátom. Komisia v každom prípade stanoví časový limit pre vykonanie svojho rozhodnutia.

Článok 9

1. Žiadateľ o EHS typové schválenie na modelový záznamový list uvedie vo svojej žiadosti typ alebo typy záznamového zariadenia, pre ktoré je tento záznam navrhovaný na používanie a poskytne vhodné zariadenie takého typu alebo typov, za účelom testovania tohto záznamu.

2. Príslušné orgány každého členského štátu označia na schvaľovacom osvedčení pre modelový záznamový list typ alebo typy záznamového zariadenia, na ktorých sa tento modelový záznamový list môže používať.

Článok 10

Žiadny členský štát nesmie odmietnuť registráciu akéhokoľvek vozidla vybaveného záznamovým zariadením alebo zakázať uviesť do prevádzky alebo používať také vozidlá z dôvodu, že toto vozidlo je vybavené takýmto zariadením, ak toto zariadenie má značku typového schválenia EHS uvedenú v článku 6 a inštalačnú dosku uvedenú v článku 12.

Článok 11

Všetky rozhodnutia podľa tohto nariadenia odmietajúce alebo odoberajúce schválenie typu záznamového zariadenia alebo modelového záznamového listu musia podrobne špecifikovať dôvody, na ktorých sú založené. Rozhodnutie sa oznámi dotknutej strane, ktorá bude súčasne informovaná o opravných prostriedkoch pre ňu použiteľných podľa právnych predpisov členských štátov a lehôt na uplatnenie týchto opravných prostriedkov.

KAPITOLA III

Inštalovanie a kontrola

Článok 12

1. Záznamové zariadenie môže inštalovať alebo opraviť len montér alebo dielne schválené príslušnými orgánmi členských štátov na tento účel po tom, čo tieto, ak to vyžadovali, vypočuli názory príslušných výrobcov.

Doba platnosti kariet vydaných schválenej dielni alebo montérovi, nesmie presiahnuť jeden rok.

Ak karta, ktorá sa má obnoviť, vydaná schválenej dielni alebo montérovi je poškodená, nefunkčná, stratená alebo odcudzená, orgán vydá náhradnú kartu do piatich pracovných dní od obdržania podrobne zdôvodnenej žiadosti.

Keď je vydaná nová karta ako náhrada za starú, má rovnaké informačné číslo dielne, ale index sa zvýši o jedna. Orgán vydávajúci karty vedie zoznam stratených, odcudzených alebo chybných kariet.

Členské štáty prijmú opatrenia potrebné na zabránenie falšovania kariet distribuovaných schváleným montérom a dielňam.

2. Schválený montér alebo dielňa dá na plomby, ktoré pripevňuje špeciálnu značku a okrem toho v prípade záznamového zariadenia zhodného s požiadavkami prílohy IB, vloží elektronické bezpečnostné dáta, na základe ktorých sa môžu vykonávať najmä overovacie kontroly. Príslušné orgány každého členského štátu vedú register značiek a použitých elektronických bezpečnostných dát a kariet vydaných schváleným dielňam a montérom.

3. Príslušné orgány členských štátov pošlú Komisii zoznamy schválených montérov a dielní a im vydaných kariet, ako aj kópie značiek a potrebných informácií týkajúcich sa použitých elektronických bezpečnostných dát.

4. Za účelom potvrdenia, že inštalovanie záznamového zariadenia prebehlo v súlade s požiadavkami tohto nariadenia, bude použitá pripojená inštalačná doska, ako je stanovené v prílohe I a IB.

5. Plomba môže byť odstránená montérmi alebo dielňami schválenými príslušnými orgánmi podľa odseku 1 tohto článku alebo za okolností uvedených v prílohe I, kapitola V, bodu 4 alebo v prílohe IB časť VI(c) tohto nariadenia.

KAPITOLA IV

Používanie zariadenia

Článok 13

Zamestnávateľ a vodiči zabezpečia správnu činnosť a vhodné používanie záznamového zariadenia na jednej strane a na strane druhej karty vodiča, keď vodič riadi vozidlo vybavené záznamovým zariadením zhodným s požiadavkami prílohy IB.

Článok 14

1. Zamestnávateľ vydá dostatočný počet záznamových listov vodičom vozidiel vybavených záznamovým zariadením zhodným s požiadavkami prílohy I., pričom musí mať na zreteli tú skutočnosť, že tieto listy majú osobný charakter, dobu prevádzky a možnú povinnosť nahradiť listy, ktoré sú poškodené, alebo ktoré zabavil oprávnený inšpektor. Zamestnávateľ vydá vodičom iba listy zodpovedajúce schválenému modelu, ktoré sú vhodné na používanie v zariadení inštalovanom vo vozidle.

Keď je vozidlo vybavené záznamovým zariadením zhodným s požiadavkami prílohy IB, zamestnávateľ a vodič, berúc do úvahy dĺžku doby služby, zabezpečia, aby sa mohla na žiadosť kontrolného orgánu podľa prílohy IB vykonať tlač.

2. Podnik uchováva záznamové listy a výtlačky, ak sú výtlačky urobené na účely dosiahnutia súladu s článkom 15 ods. 1, v chronologickom poradí a v čitateľnej forme najmenej jeden rok po ich použití a poskytne kópie dotknutým vodičom, ktorí o ne požiadajú. Podnik tiež poskytne kópie údajov stiahnutých z kariet vodičov dotknutým vodičom, ktorí o ne požiadajú, a výtlačky týchto kópií. Záznamové listy, výtlačky a stiahnuté údaje sa predložia alebo odovzdajú na požiadanie ktoréhokoľvek oprávneného inšpekčného úradníka.

3. Karta vodiča definovaná v prílohe IB vydá na žiadosť vodiča príslušný orgán členského štátu, v ktorom má vodič svoje zvyčajné bydlisko.

Členský štát môže od každého vodiča, ktorý podlieha ustanoveniam nariadenia (EHS) č. 3820/85 a má zvyčajné bydlisko na jeho území, vyžadovať, aby vlastnil kartu vodiča.

a) Pre účely tohto nariadenia "zvyčajné bydlisko" znamená miesto, kde osoba zvyčajne žije minimálne 185 dní v kalendárnom roku, pretože je k tomuto miestu osobne a pracovne viazaná alebo v prípade, že nie je pracovne viazaná, má k tomuto miestu kde žije, úzke osobné väzby.

Avšak za zvyčajné bydlisko osoby, ktorá je pracovne viazaná na inom mieste než je miesto ku ktorému je viazaná osobne, a ktorá v dôsledku toho býva postupne na rôznych miestach situovaných v dvoch alebo viacerých členských štátoch, sa považuje miesto ku ktorému je osobne viazaná za predpokladu, že sa na takéto miesto pravidelne vracia. Táto posledná podmienka sa nevyžaduje vtedy, keď osoba žije v členskom štáte preto, že vykonáva svoje úlohy, ktorých doba trvania je pevne určená.

b) Vodiči podajú akýmkoľvek vhodným prostriedkom ako je osobný preukaz alebo iný platný doklad, dôkaz o mieste svojho zvyčajného bydliska.

c) Príslušný orgán členského štátu vydávajúceho kartu vodiča môže požadovať akékoľvek ďalšie informácie alebo dôkazy, keď má pochybnosti o platnosti dôkazov uvedených pod písm. b) a týkajúcich sa zvyčajného bydliska, alebo ak je to potrebné pre účely určitých špecifických kontrol.

d) Príslušné orgány členského štátu vydávajúceho kartu vodiča sa v rámci svojich možností ubezpečia, či žiadateľ už nevlastní platnú kartu vodiča.

4. a) Príslušné orgány členského štátu opatria každú kartu vodiča osobnými údajmi vodiča podľa ustanovení prílohy IB.

Pre správne účely nesmie byť platnosť karty vodiča dlhšia než päť rokov.

Vodič môže vlastniť len jednu platnú kartu vodiča. Vodič smie používať len svoju vlastnú osobnú kartu vodiča. Vodič nesmie používať kartu vodiča, ktorá je chybná alebo ktorej doba platnosti už uplynula.

Keď je vydaná nová karta vodiča ako náhrada za starú, musí byť označená rovnakým číslom vydania, jej index sa však zvýši o jeden. Vydávajúci orgán vedie zoznam vydaných, odcudzených, stratených alebo chybných kariet vodiča po dobu minimálne rovnajúcu sa dobe ich platnosti.

Ak je karta vodiča poškodená, nefunkčná, stratená alebo odcudzená, orgán vydá náhradnú kartu do piatich pracovných dní od obdržania podrobne zdôvodnenej žiadosti.

V prípade žiadosti o obnovenie karty, ktorej doba platnosti uplynula, vydá orgán pred uplynutím doby novú kartu za predpokladu, že žiadosť obdržal v časovom limite stanovenom v druhom pododseku článku 15(1).

b) Karty vodiča sa vydajú len žiadateľom, ktorí podliehajú ustanoveniam nariadenia (EHS) č. 3820/85.

c) Karta vodiča je osobná. Nesmie byť počas doby jej platnosti odobratá alebo jej platnosť pozastavená z akýchkoľvek dôvodov pokiaľ príslušný orgán nezistí, že karta bola sfalšovaná alebo kartu používa vodič, ktorý nie je jej vlastníkom alebo, že karta bola vystavená na základe falošného vyhlásenia a/alebo falošných dokumentov. Ak také opatrenia týkajúce sa pozastavenia platnosti alebo odobratia karty prijme členský štát iný než je štát, v ktorom bola karta vydaná, vráti kartu členskému štátu, ktorý ju vydal a zdôvodní svoj postup.

d) Karty vodiča vydané členskými štátmi sa vzájomne uznávajú.

Keď si držiteľ platnej karty vodiča vydanej členským štátom zriadil svoje zvyčajné bydlisko v inom členskom štáte, môže požiadať aby jeho karta bola vymenená za ekvivalentnú kartu vodiča; členský štát, ktorý kartu vymieňa je zodpovedný za overenie platnosti predloženej karty.

Členské štáty vykonávajúce výmenu vrátia starú kartu orgánom členského štátu, ktorý kartu vydal a zdôvodnia svoj postup.

e) Keď členské štáty nahradia alebo vymenia kartu vodiča, náhrada alebo výmena a akákoľvek následná náhrada alebo obnova sa v tomto členskom štáte zaeviduje.

f) Členské štáty prijmú všetky potrebné opatrenia na zabránenie akejkoľvek možnosti falšovania kariet vodiča.

5. Členské štáty zabezpečia, aby údaje potrebné na monitorovanie súladu s nariadením (EHS) č. 3820/85 a smernice Rady 92/6/EHS z 10. februára o inštalovaní a používaní zariadení obmedzujúcich rýchlosť pre

niektoré kategórie motorových vozidiel v spoločenstve[*)], ktoré zaznamenáva a uchováva záznamové zariadenie v súlade s prílohou IB k tomuto nariadeniu, boli k dispozícii po dobu aspoň 365 dní po dátume ich zaznamenania a aby bola zaručená ich bezpečnosť a správnosť.

Členské štáty prijmú všetky opatrenia potrebné na to, aby opätovný predaj alebo odstavenie záznamového zariadenia, nemali vplyv na riadne uplatňovanie tohto odseku.

Článok 15

1. Vodiči nesmú používať špinavé alebo poškodené záznamové listy alebo karty vodiča. Záznamy budú za týmto účelom vhodne chránené.

Vodič, ktorý si chce obnoviť svoju kartu vodiča, musí o to požiadať príslušné orgány členského štátu, v ktorom má zvyčajné bydlisko najneskôr 15 pracovných dní pred uplynutím doby platnosti karty.

V prípade poškodenia listu alebo karty vodiča so záznamami vodiča pripojí vodič poškodený list alebo kartu vodiča k náhradnému listu.

Ak je karta vodiča poškodená, znefunkčnená, stratená alebo odcudzená, vodič požiada príslušné orgány členského štátu, v ktorom má zvyčajné bydlisko, do siedmich kalendárnych dní o náhradu.

Ak sa karta vodiča poškodila, bola nesprávne použitá alebo ju vodič nemá, vodič:

a) na začiatku svojej cesty vytlačí všetky údaje o vozidle, ktoré riadi, a do tohto výtlačku uvedie:

   i) údaje, ktoré umožňujú identifikáciu vodiča (meno, číslo karty vodiča alebo vodičského preukazu vodiča) vrátane jeho podpisu;

   ii) doby uvedené v odseku 3 druhej zarážke písm. b), c) a d);

b) po ukončení svojej cesty vytlačí informácie týkajúce sa dôb zaznamenaných záznamovým zariadením, zaznamená všetky doby inej práce, pohotovosti a čerpaného odpočinku od doby vyhotovenia výtlačku na začiatku cesty, keď neboli zaznamenané tachografom, a na tomto dokumente vyznačí údaje, ktoré umožnia identifikáciu vodiča (meno, číslo karty vodiča alebo vodičského preukazu vodiča) vrátane podpisu vodiča.

2. Vodiči sú povinní používať záznamové listy a karty vodiča každý deň, keď jazdia od chvíle, keď prevzali vozidlo. Záznamový list alebo karta vodiča nebude odobratý pred ukončením dennej pracovnej doby, ak jeho odobratie nie je inak schválené. Nijaký záznamový list alebo karta vodiča nesmie byť použitý na dlhšie obdobie než na ktoré bol určený.

Keď sa vodič nachádza mimo vozidla a v dôsledku toho nemôže používať zariadenie namontované vo vozidle, časové úseky uvedené v odseku 3 druhej zarážke písm. b), c) a d):

a) v prípade vybavenia vozidla záznamovým zariadením podľa prílohy I sa zapíšu na záznamový list buď ručne, automatickým záznamom, alebo inými prostriedkami, čitateľne a bez znečistenia listu, alebo

b) v prípade vybavenia vozidla záznamovým zariadením podľa prílohy IB sa zapíšu na kartu vodiča pomocou ovládača na manuálne zapi sovanie, nachádzajúceho sa na záznamovom zariadení.

Ak je vo vozidle vybavenom záznamovým zariadením podľa prílohy IB viac než jeden vodič, každý vodič zabezpečí, aby bola jeho karta vodiča vložená do správneho slotu tachografu.

Vodiči upravia v prípade potreby záznamové listy, ak je vo vozidle viac ako jeden vodič, aby informácie uvedené v kapitole II. (1) až (3) prílohy I. boli zaznamenané na záznamový list vodiča, ktorý práve jazdí.

3. Vodiči:

- zabezpečia, aby čas zaznamenaný na liste súhlasil s oficiálnym časom v štáte registrácie vozidla,
- uvedú do činnosti prepínací mechanizmus umožňujúci, aby nasledujúce časové úseky boli zaznamenané oddelene a zreteľne:

  (a) pod znakom  : doba jazdy,

[*] OJ L 57, 02. 03. 1992, str. 27.

(b) ‚iná práca' je akákoľvek iná činnosť ako vedenie vozidla, ako je vymedzená v článku 3 písm. a) smernice Európskeho parlamentu a Rady 2002/15/ES z 11. marca 2002 o organizácii pracovnej doby osôb vykonávajúcich mobilné činnosti v cestnej doprave[2], ako aj každá práca vykonávaná pre rovnakého alebo iného zamestnávateľa v odvetví dopravy alebo mimo neho, a musí sa zaznamenávať pod symbolom  ;

(c) pohotovosť, vymedzená v článku 3 písm. b) smernice 2002/15/ES sa musí zaznamenávať pod symbolom  ;

(d) pod znakom  : prestávky v práci a doby denného odpočinku.

5. Každý člen posádky zapíše na svoj záznamový list nasledujúcu informáciu:

(a) na začiatok používania listu - svoje priezvisko a krstné meno;

(b) dátum a miesto, kde používanie listu začína a dátum a miesto, kde toto používanie končí;

(c) registračné číslo každého vozidla, ku ktorému je pridelený, aj na začiatku prvej jazdy zaznamenanej na liste a potom v prípade zmeny vozidla počas používania listu;

(d) údaje počítadla kilometrov:

- na začiatku prvej cesty zaznamenanej na liste,
- na konci poslednej cesty zaznamenanej na liste,
- v prípade zmeny vozidla počas pracovného dňa / údaj na vozidle, ku ktorému bol pridelený a údaj na vozidle, ku ktorému má byť pridelený

(e) čas akejkoľvek zmeny vozidla.

5a. Vodič vloží do záznamového zariadenia podľa prílohy IB, symboly štátov, v ktorých začal a skončil svoju dennú pracovnú dobu. Členský štát však môže od vodičov vozidiel vykonávajúcich dopravné činnosti na jeho území požadovať, aby doplnili symbol štátu o podrobnejšie geografické špecifikácie za predpokladu, že členský štát ich oznámil Komisii pred 1. aprílom 1998, a že ich počet nie je väčší než 20.

Vyššie uvedené vložené údaje aktivuje vodič a môžu byť plne manuálne alebo keď je záznamové zariadenie spojené so satelitným systémom určovania polohy, môžu byť automatizované.

6. Záznamové zariadenie definované v prílohe I bude konštruované tak, aby bolo v prípade potreby pre oprávneného inšpektora možné po otvorení zariadenia, prečítať záznamy týkajúce sa 9 hodín predchádzajúcich času kontroly bez trvalého deformovania, poškodenia alebo znečistenia listu.

Okrem toho bude zariadenie konštruované tak, aby bolo možné bez otvorenia skrine overiť, že sa záznamy vykonávajú.

7. a) Ak vodič vedie vozidlo vybavené záznamovým zariadením podľa prílohy I, musí, kedykoľvek o to inšpekčný úradník požiada, predložiť:

i) záznamové listy za bežný týždeň a listy použité vodičom v predchádzajúcich 15 dňoch;

ii) kartu vodiča, pokiaľ ju má, a

iii) každý ručný záznam a výtlačok vytvorený počas bežného týždňa a predchádzajúcich 15 dní, ako to vyžaduje toto nariadenie a nariadenie (ES) č. 561/2006.

Od 1. januára 2008 sa však budú doby uvedené v bodoch i) a iii) vzťahovať na bežný deň a predchádzajúcich 28 dní.

b) Ak vodič vedie vozidlo vybavené záznamovým zariadením podľa prílohy IB, musí, kedykoľvek o to inšpekčný úradník požiada, predložiť:

i) kartu vodiča, ktorej je držiteľom;

[2] Ú. v. ES L 80, 23.3.2002, s. 35.

ii) každý ručný záznam a výtlačok vytvorený počas bežného týždňa a predchádzajúcich 15 dní, ako to vyžaduje toto nariadenie a nariadenie (ES) č. 561/2006, a

iii) záznamové listy zodpovedajúce rovnakému obdobiu, ako je uvedené v predchádzajúcom pododseku, počas ktorého viedol vozidlo vybavené záznamovým zariadením v súlade s prílohou I.

Od 1. januára 2008 sa však budú doby uvedené v bode ii) vzťahovať na bežný deň a predchádzajúcich 28 dní.

c) Oprávnený inšpekčný úradník môže skontrolovať dodržiavanie nariadenia (ES) č. 561/2006 analýzou záznamových listov, zobrazených alebo vytlačených údajov, ktoré zaznamenalo záznamové zariadenie alebo karta vodiča, alebo ak to nebude možné, tak analýzou akéhokoľvek podporného dokumentu, ktorý dokazuje nedodržanie ustanovení, ako sa stanovujú v článku 16 ods. 2 a 3.

8. Zakazuje sa falšovanie, zatajovanie alebo zničenie dát zaznamenaných na záznamovom liste, uchovávaných v záznamovom zariadení alebo na karte vodiča, alebo výtlačkov záznamového zariadenia ako je definované v prílohe IB. To isté platí pre každú manipuláciu so záznamovým zariadením, záznamovým listom alebo kartou vodiča, ktorých výsledkom môže byť falšovanie, zatajovanie alebo ničenie dát a/alebo informácií. Vo vozidle nesmie byť žiadne zariadenie, ktoré by sa mohlo použiť na tieto účely.

Článok 16

1. V prípade poruchy alebo chybnej činnosti zariadenia, dá ho zamestnávateľ opraviť schváleným montérom alebo dielňou, hneď ako to okolnosti dovolia.

Ak sa vozidlo nemôže vrátiť do prevádzkárne v priebehu jedného týždňa odo dňa poruchy alebo od objavenia chybnej činnosti, vykoná sa oprava cestou.

Opatrenia prijímané členskými štátmi podľa článku 19 môžu dať príslušným orgánom právomoc zakázať používanie vozidla v prípadoch, keď porucha alebo chybná činnosť nebola odstránená, ako je stanovené v predchádzajúcich pododsekoch.

2. Pokiaľ je zariadenie neschopné prevádzky alebo pracuje chybne, vodiči na záznamový list, listy alebo na dočasný záznam pripojený k záznamovému listu, na ktorom zaznamená dáta umožňujúce jeho identifikáciu (číslo karty vodiča a/alebo číslo vodičského preukazu), vrátane jeho podpisu, zaznačia všetky informácie o rôznych časových úsekoch, ktoré už nie sú správne zaznamenané alebo vytlačené záznamovým zariadením.

Ak je karta vodiča poškodená, znefunkčnená, stratená alebo odcudzená, vodič na konci svojej jazdy vytlačí informáciu týkajúcu sa časového obdobia zaznamenaného záznamovým zariadením, uvedie na tento dokument údaje, ktoré umožňujú jeho identifikáciu (číslo karty vodiča a/alebo meno a/alebo číslo vodičského preukazu) a tento dokument podpíše.

3. Ak je karta vodiča poškodená alebo ak je znefunkčnená, vodič ju vráti príslušnému orgánu členského štátu, v ktorom má svoje zvyčajné bydlisko. Krádež karty vodiča oznámi príslušným členského štátu, v ktorom ku krádeži došlo.

Stratu karty vodiča musí oznámiť príslušným orgánom členského štátu, ktorý ju vydal a príslušným orgánom členského štátu, v ktorom má svoje zvyčajné bydlisko, ak ide o dva rôzne štáty.

Vodič môže pokračovať v jazde bez karty vodiča maximálne 15 kalendárnych dní alebo dlhšiu dobu, ak je to potrebné na návrat vozidla do prevádzkových priestorov jeho podniku za predpokladu, že preukáže nemožnosť predloženia alebo používania karty počas tohto obdobia.

Keď orgány členského štátu, v ktorom má vodič svoje zvyčajné bydlisko nie sú tie, ktoré jeho kartu vydali a keď sa od nich žiada obnovenie, náhrada alebo výmena karty vodiča, musia informovať orgány, ktoré vydali starú kartu o presných dôvodoch jej obnovenia, náhrady alebo výmeny.

KAPITOLA V.

Záverečné ustanovenia

Článok 17

1. Zmeny potrebné na prispôsobenie príloh technickému pokroku sa prijmú v súlade s postupom stanoveným v článku 18.

2. Technické špecifikácie týkajúce sa nasledovných častí prílohy IB sa rovnakým postupom prijmú čo možno najskôr a podľa možnosti do 1. júla 1998:

a) Kapitola II
   - (d) 17:
     zobrazenie a tlač porúch záznamového zariadenia,
   - (d) 18:
     zobrazenie a tlač porúch karty vodiča,
   - (d) 21:
     zobrazenie a tlač súhrnných správ;

b) Kapitola III
   - (a) 6.3:
     normy na ochranu elektroniky vozidla proti elektrickému rušeniu a magnetickým poliam,
   - (a) 6.5:
     ochrana (bezpečnosť) celého systému,
   - (c) 1:
     výstražné signály oznamujúce vnútornú poruchu záznamového zariadenia,
   - (c) 5:
     charakter výstražných signálov,
   - (f):
     maximálne tolerancie;

c) Kapitola IV, A:
   - 4:
     normy,
   - 5:
     bezpečnosť, vrátane ochrany dát,
   - 6:
     rozsah teplôt,
   - 8:
     elektrické charakteristiky,
   - 9:
     logická štruktúra karty vodiča,
   - 10:
     funkcie a povely,
   - 11:
     základné súbory informácií;

   a kapitola IV, B:;

d) kapitola V:
   tlačiareň a štandardné výtlačky.

Článok 18

1. Komisii pomáha výbor.

2. V prípade odkazu na tento článok sa uplatňujú články 5 a 7 rozhodnutia 1999/468/ES[3], so zreteľom na ustanovenia jeho článku 8.

3. Výbor schvaľuje svoj rokovací poriadok.

[3] Rozhodnutie Rady 1999/468/ES z 28. júna 1999, ktorým sa ustanovujú postupy pre výkon vykonávacích právomocí zverených Komisii (Ú. v. ES L 184, 17.7.1999, s. 23).

Článok 19

1. Členské štáty včas a po porade s Komisiou prijmú také zákony, právne predpisy alebo správne opatrenia, potrebné na vykonávanie tohto nariadenia.

Takéto opatrenia majú medzi iným zahŕňať reorganizáciu postupu a prostriedkov vykonávania kontrol dodržiavania zhody s nariadením a pokuty uložené v prípade porušenia.

2. Členské štáty si navzájom pomáhajú pri uplatňovaní tohto nariadenia a pri kontrole jeho dodržiavania.

3. V rámci tejto vzájomnej pomoci si príslušné orgány členských štátov pravidelne posielajú všetky dostupné informácie týkajúce sa:

- porušení tohto nariadenia, ktorých sa dopustili iné osoby, ako sú obyvatelia štátu a akékoľvek pokuty uložené za tieto porušenia,
- pokút uložených členským štátom svojim obyvateľom za takéto porušenie vykonané v iných členských štátoch.

Článok 20

Nariadenie (EHS) č. 1463/70 sa zrušuje.

Článok 3(1) uvedeného nariadenia sa však do 31. decembra 1989 bude naďalej uplatňovať pre vozidlá a vodičov zamestnaných v pravidelnej medzinárodnej osobnej doprave, pokiaľ vozidlá používané pre takéto služby nie sú vybavené záznamovým zariadením používaným podľa tohto nariadenia.

Článok 20a

Toto nariadenie sa nebude uplatňovať pred 1. januárom 1991 na tie vozidlá, ktoré boli registrované na území bývalej NDR pred týmto dátumom.

Toto nariadenie sa nebude uplatňovať pred 1. januárom 1993 na tie vozidlá, ktoré sú používané iba pri operáciách vnútroštátnej dopravy na území Nemeckej spolkovej republiky. Toto nariadenie sa však bude po nadobudnutí účinnosti uplatňovať na vozidlá prepravujúce nebezpečný tovar.

Článok 21

Toto nariadenie nadobudne účinnosť 29. septembra 1986.

Toto nariadenie je záväzné vo svojej celistvosti a je priamo uplatniteľné vo všetkých členských štátoch.

V Bruseli 20. decembra 1985

Za Radu

predseda

R. KRIEPS

PRÍLOHA I

Požiadavky na konštrukciu, testovanie, montáž a kontrolu

I. DEFINÍCIE

V tejto prílohe:

a) Záznamové zariadenie znamená:

zariadenie určené na inštaláciu do cestných vozidiel na automatické alebo poloautomatické ukázanie a zaznamenanie podrobností o pohybe týchto vozidiel a určitých pracovných dobách ich vodičov,

b) Záznamový list znamená:

list určený na zachytenie a zapamätanie si zaznamenaných údajov, je umiestnený v záznamovom zariadení a jeho značkové zariadenie vypíše súvislý záznam informácií, ktoré majú byť zaznamenané,

c) Konštanta záznamového zariadenia znamená:

numerickú charakteristiku udávajúcu hodnotu vstupnému signálu požadovanému na ukázanie a zaznamenanie ubehnutej vzdialenosti 1 km, táto konštanta musí byť vyjadrená alebo v otáčkach na kilometer (k =...ot/km) alebo v impulzoch na km (k =...imp/km),

d) Charakteristický koeficient vozidla znamená:

numerickú charakteristiku udávajúcu hodnotu výstupnému signálu emitovanému časťou vozidla spájajúcou ju so záznamovým zariadením (vývodný hriadeľ alebo náprava prevodovky), zatiaľ čo vozidlo prejde vzdialenosť jedného nameraného kilometra za normálnych testovacích podmienok (pozri kapitolu VI, bod 4. tejto prílohy). Charakteristický koeficient vozidla je vyjadrený alebo v otáčka na km (w =...ot/km alebo v impulzoch na km (w =...imp/km),

e) Skutočný obvod pneumatík kolies znamená:

priemer vzdialenosti ubehnutých niekoľkými kolesami pohybujúceho sa vozidla (hnacie kolesá) v priebehu jednej úplnej rotácie. Meranie týchto vzdialeností musí byť urobené za normálnych testovacích podmienok (pozri kapitolu VI, bod 4. tejto prílohy) a je vyjadrený v tvare l =...mm.

II. VŠEOBECNÉ CHARAKTERISTIKY A FUNKCIE ZÁZNAMOVÉHO ZARIADENIA

Zariadenie musí byť schopné zaznamenávať nasledovné:

1. vzdialenosť ubehnutú vozidlom;
2. rýchlosť vozidla;
3. dobu jazdy;
4. iné doby práce alebo použiteľnosti;
5. prestávky v práci a doby denného odpočinku;
6. otvorenie puzdra obsahujúceho záznamový list.
7. Pre elektronické záznamové zariadenie, ktoré je zariadením fungujúcim na základe signálu prenášaného elektricky zo snímaču rýchlosti a vzdialenosti, akékoľvek prerušenie dodávky prúdu záznamovému zariadeniu presahujúce 100 milisekúnd (okrem osvetlenia), dodávky prúdu snímaču rýchlosti a vzdialenosti a akékoľvek prerušenie signálneho vedenia snímača rýchlosti a vzdialenosti.

Pre vozidlá používané dvoma vodičmi musí byť zariadenie schopné zaznamenávať súčasne, ale odlišne a na 2 oddelených listoch podrobnosti o dobách uvedených v 3., 4. a 5.

III. KONŠTRUKČNÉ POŽIADAVKY NA ZÁZNAMOVÉ ZARIADENIE

(a) Všeobecné body

1. *Záznamové zariadenie obsahuje nasledovné:*

1.1 Vizuálne prístroje ukazujúce:

- ubehnutú vzdialenosť (zapisovač vzdialeností),
- rýchlosť (rýchlomer),
- čas (hodiny).

1.2 Záznamové prístroje obsahujúce:

- zapisovač ubehnutej vzdialenosti,
- zapisovač rýchlosti,
- jeden alebo viac časových zapisovačov spĺňajúcich požiadavky stanovené v kapitole III (c) 4.

1.3 Značkovacie zariadenie ukazujúce na záznamovom liste jednotlivo:

- každé otvorenie púzdra obsahujúceho tento záznam,
- pre elektronické záznamové zariadenie, ako je definované v bode 7 kapitoly II, akékoľvek prerušenie dodávky prúdu záznamovému zariadeniu presahujúce 100 milisekúnd (okrem osvetlenia), dokiaľ sa znovu nezapne dodávka prúdu,
- pre elektronické záznamové zariadenie, ako je definované v bode 7 kapitoly II, akékoľvek prerušenie dodávky prúdu snímaču rýchlosti a vzdialenosti presahujúce 100 milisekúnd a akékoľvek prerušenie signálneho vedenia snímača rýchlosti a vzdialenosti.

2. Akékoľvek zahrnutie ďalšieho vybavenia prístrojov do vyššie uvedeného zariadenia, nesmie prekážať správnej činnosti povinných zariadení alebo ich odčítaniu údajov z týchto zariadení.

Zariadenie musí byť predložené na schválenie celé s akýmikoľvek doplnkovými prístrojmi.

3. Materiály

3.1 Všetky časti záznamového zariadenia musia byť vyrobené z materiálov s dostatočnou mechanickou pevnosťou a stabilnými elektrickými a magnetickými charakteristikami.

3.2 Akákoľvek modifikácia časti zariadenia alebo charakteru materiálov použitých na jeho výrobu, musí byť pred použitím vo výrobe predložená na schválenie orgánu, ktorý pre zariadenie udelil typové schválenie.

4. *Meranie ubehnutej vzdialenosti*

Ubehnuté vzdialenosti môžu byť merané a zaznamenané buď tak:

- aby zahŕňali pohyb dopredu aj dozadu alebo
- aby zahŕňali len pohyb dopredu.

Akékoľvek zaznamenanie spätných pohybov nesmie za nijakých okolností ovplyvniť zreteľnosť a presnosť iných záznamov.

5. Meranie rýchlosti

5.1 Rozsah merania rýchlosti bude taký, ako je stanovené v osvedčení o typovom schválení.

5.2 Vlastná frekvencia a tlmenie meracieho zariadenia musí byť také, aby prístroje ukazujúce a zaznamenávajúce rýchlosť mohli v rozsahu merania sledovať akceleračné zmeny až do $2 m/s^2$, v hraniciach schválených tolerancií.

6. Meranie času (hodiny)

6.1 Kontrola mechanizmu opätovného nastavenia hodín musí byť umiestnená vo vnútri puzdra obsahujúceho záznamový list, každé otvorenie puzdra musí byť automaticky zaznamenané na záznamovom liste.

6.2 Ak je mechanizmus pohybu dopredu záznamového listu riadený hodinami, musí byť čas, v ktorom hodiny pôjdu správne po úplnom natiahnutí, aspoň o 10 % väčší ako doba zapisovania zodpovedajúca maximálnemu zaťaženiu listu zariadenia.

7. Osvetlenie a ochrana

7.1 Vizuálne prístroje zariadenia musia byť vybavené vhodným neoslňujúcim osvetlením.

7.2 Pre bežné podmienky používania musia byť všetky vnútorné časti zariadenia chránené voči vlhkosti a prachu. Okrem toho musia byť odolné proti zásahom pomocou zaplombovaných krytov.

(b) **Vizuálne prístroje**

1. Indikátor ubehnutej vzdialenosti (záznamový prístroj vzdialenosti)

1.1 Hodnota najmenšieho odstupňovania na prístroji ukazujúcom ubehnutú vzdialenosť musí byť 0,1 km. Čísla ukazujúce hektometre musia byť jasne odlišné od tých, ktoré ukazujú celé kilometre.

1.2 Čísla na záznamovom prístroji vzdialenosti musia byť jasne čitateľné a musia mať výšku aspoň 4 mm.

1.3 Záznamový prístroj vzdialenosti musí byť schopný ukazovať aspoň do 99 999,9 km.

2. Rýchlomery (tachometre)

2.1 V rozsahu merania musí byť rýchlostná škála jednotne odstupňovaná po 1, 2, 5 alebo 10 km/h. Hodnota odstupňovania rýchlosti (priestor medzi 2 následnými značkami) nesmie presahovať 10 % maximálnej rýchlosti ukázanej na stupnici.

2.2 Rozsah naznačený mimo meraného potrebného rozsahu, nemusí byť označený číslami.

2.3 Dĺžka každého intervalu na stupnici predstavujúca rozdiel rýchlosti 10 km/h nesmie byť menšia ako 10 mm.

2.4 Na indikátore s ihlou vzdialenosti medzi ihlou a čelom prístroja nesmie presahovať 3 mm.

3. Ukazovateľ času (hodiny)

Ukazovateľ času musí byť viditeľný zvonku prístroja a musí poskytovať jasný, jednoduchý a jednoznačný údaj.

(c) **Záznamové prístroje**

1. Všeobecné body

1.1 Všetky zariadenia, s akoukoľvek formou záznamového listu (pás alebo disk) musia byť vybavené značkou umožňujúcou správne vloženie záznamového listu, aby sa takýmto spôsobom zabezpečilo, že čas ukazovaný hodinami a značenie času na liste si budú navzájom zodpovedať.

1.2 Mechanizmus pohybujúci záznamovým listom musí byť taký, aby sa zabezpečilo, že sa záznamový list bude pohybovať bez vôle a bude sa môcť voľne vkladať a vyberať.

1.3 Pri záznamových listoch vo forme disku musí byť zariadenie na pohyb dopredu riadené mechanizmom hodín. V tomto prípade rotačný pohyb záznamu musí byť plynulý a rovnomerný s minimálnou rýchlosťou 7 mm/h, meranou na vnútornej strane kruhu označujúceho okraj oblasti registrácie rýchlosti. Pri zariadení pásového typu, kde je pohyb záznamov dopredu riadený hodinovým mechanizmom musí byť rýchlosť priamočiareho pohybu dopredu aspoň 10 mm/h.

1.4 Zapisovanie ubehnutej vzdialenosti, rýchlosti vozidla a akéhokoľvek otvorenia puzdra obsahujúceho záznamový list alebo listy musí byť automatické.

2. Zapisovanie ubehnutej vzdialenosti

2.1 Každý kilometer ubehnutej vzdialenosti musí byť na zázname znázornený zmenou aspoň o 1 mm na príslušnej súradnici.

2.2 Dokonca aj pri rýchlostiach dosahujúcich hornú hranicu rozsahu merania musí byť záznam vzdialenosti zreteľne čitateľný.

3. Zapisovanie rýchlosti

3.1 Pri akejkoľvek forme záznamového listu sa dotykový hrot zapisujúci rýchlosť musí pohybovať v priamke a v pravých uhloch na smer pohybu záznamového listu.

Pohyb dotykového hrotu môže však byť aj krivočiary za predpokladu, že sú splnené tieto podmienky:

- stopa zakreslená dotykovým hrotom musí byť kolmá na priemerný obvod (v prípade záznamov vo forme disku) alebo na os (v prípade záznamov vo forme pásu) v oblasti vyhradenej na zapisovanie rýchlosti,
- pomer medzi polomerom zakrivenia stopy zakreslenej dotykovým hrotom a šírkou oblasti vyhradenej pre zapisovanie rýchlosti nesmie byť menší než 2,4 k l, pri akejkoľvek forme záznamového listu,
- značky na časovom meradle musia prechádzať oblasť záznamu v krivke s rovnakým polomerom, ako má stopa zakreslená dotykovým hrotom. Intervaly medzi značkami na časovom meradle musia predstavovať dobu nepresahujúcu 1 hodinu.

3.2 Každá zmena v rýchlosti 10 km/h musí byť znázornená na zázname pomocou zmeny aspoň 1,5 mm na príslušnej súradnici.

4. Čas zaznamenávania

4.1 Záznamové zariadenie musí byť konštruované tak, aby bolo možné dobu jazdy vždy zaznamenať automaticky a umožniť, kde je nevyhnutné, spínacím zariadením automaticky a oddelene zaznamenávať ostatné časové doby, ako sú označené v článku 15(3), druhá zarážka (b), (c) a (d) nariadenia.

4.2 Z charakteristík stôp, ich vzájomných polôh a v prípade potreby zo znakov stanovených v článku 15 nariadenia, musí byť možné zreteľne rozlíšiť rôzne časové úseky.

Rôzne časové doby by mali byť navzájom odlišné na zázname podľa rozdielov v hrúbke príslušných stôp alebo akýmkoľvek iným systémom s aspoň rovnakou účinnosťou z hľadiska čitateľnosti a jednoduchosti interpretácie záznamu.

4.3 V prípade vozidiel s posádkou zloženou z viac ako jedného vodiča, musí sa zapisovanie, stanovené v bode 4.1, robiť na dvoch oddelených listoch, z ktorých každý bude pridelený jednému vodičovi. V tomto prípade pohyb jednotlivých listov dopredu musí byť ovplyvňovaný alebo jedným mechanizmom alebo oddelenými synchronizovanými mechanizmami.

(d) **Uzamykacie zariadenie**

1. Puzdro obsahujúce záznamový list alebo listy a riadenie mechanizmu pre opätovné nastavenie hodín musí byť zabezpečené zámkou.

2. Každé otvorenie puzdra obsahujúceho záznamový list alebo listy a riadenie mechanizmu pre opätovné nastavenie hodín musí byť automaticky zaznamenané na záznam alebo záznamy.

(e) **Značky**

1. Na čelnej strane zariadenia musia byť tieto značky:

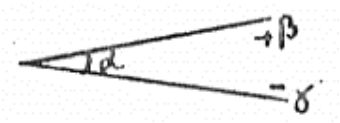
- tesne pri symbole znázornenom záznamovým zariadením vzdialenosti, jednotka merania vzdialenosti, označená skratkou "km",
- blízko stupnice rýchlosti, značka "km/h",

- rozsah merania rýchlomeru vo forme "Vmin ... km/h., Vmax ... km/h". Táto značka nie je potrebná, ak je znázornená na popisnej doske zariadenia.

Tieto požiadavky sa však neuplatňujú na záznamové zariadenia schválené pred 10. augustom 1970.

2. Popisná doska musí byť zabudovaná do zariadenia a musia na nej byť nasledujúce značky, ktoré musia byť viditeľné na zariadení po inštalovaní:

- meno a adresa výrobcu zariadenia,
- číslo výrobcu a rok výroby,
- schvaľovacia značka pre typ zariadenia,
- konštanta zariadenia v tvare "k = ...ot/km" alebo "k =... imp/km",
- voliteľne, rozsah merania rýchlosti vo forme určenej v bode 1,
- ak by citlivosť prístroja na uhol sklonu mohla ovplyvniť údaje poskytované prístrojom za hranice povolených tolerancií, povolený uhol vyjadrený ako:



kde je uhol *a* meraný z horizontálnej polohy čelnej strany (správne upevnenej) zariadenia, na ktorý je prístroj kalibrovaný, zatiaľ čo *b a g* predstavujú v poradí, povolené horné a dolné odchýlky od uhla kalibrovania.

(f) **Maximálne tolerancie (vizuálne a záznamové prístroje)**

1. Na testovacom stave pred inštaláciou:

(a) ubehnutá vzdialenosť:

1 % viac alebo menej ako skutočná vzdialenosť, keď je táto vzdialenosť aspoň 1 kilometer;

(b) rýchlosť:

o 3 km/h. viac alebo menej ako skutočná rýchlosť;

c) čas:

± 2 minúty za deň, maximálne 10 minút za sedem dní v prípadoch, keď doba chodu hodín po natiahnutí nie je menšia ako tento čas.

2. Pri inštalácii:

(a) ubehnutá vzdialenosť:

2 % viac alebo menej ako skutočná vzdialenosť, kde táto vzdialenosť je aspoň 1 km,

(b) rýchlosť:

o 4 km/h. viac alebo menej ako je skutočná rýchlosť,

(c) čas:

± dve minúty za deň, alebo

± 10 minút za sedem dní.

3. Pri použití:

(a) ubehnutá vzdialenosť:

o 4 % viac alebo menej ako reálna vzdialenosť, kde táto vzdialenosť je aspoň 1 km,

(b) rýchlosť:

o 6 km/h. viac alebo menej ako skutočná rýchlosť,

(c) čas:

± dve minúty za deň, alebo

± 10 minút za sedem dní.

4. Maximálne tolerancie stanovené v bodoch 1, 2 a 3 sú platné pre teploty medzi 0°C a 40 °C, teploty sú snímané v tesnej blízkosti zariadenia.

5. Meranie maximálnych tolerancií stanovených v bodoch 2 a 3 sa realizuje za podmienok stanovených v kapitole VI.

IV. ZÁZNAMOVÉ LISTY

(a) **Všeobecné body**

1. Záznamový list musí byť taký, aby nebránil normálnemu fungovaniu prístroja a aby záznamy, ktoré obsahujú boli neodstrániteľné a ľahko čitateľné a identifikovateľné.

Záznamové listy si musia zachovať svoje rozmery a akékoľvek zápisy, ktoré sú na nich, za normálnych podmienok vlhkosti a teploty.

Okrem toho musí byť možné písať záznamy bez toho, že by sa poškodili a bez ovplyvnenia čitateľnosti záznamov, informácií uvedených v článku 15(5) nariadenia.

Za normálnych skladovacích podmienok musia záznamy zostať čitateľné aspoň 1 rok.

2. Minimálna záznamová schopnosť listov bez ohľadu na ich tvar musí byť 24 hodín.

Ak je niekoľko diskov spojených dohromady za účelom zvýšenia plynulej záznamovej kapacity, ktorá sa môže dosiahnuť bez zasahovania personálu, musia byť spoje medzi rôznymi diskami urobené tak, aby nedošlo k prerušeniam alebo k presahom pri zapisovaní záznamov v bode prechodu z jedného disku do druhého.

(b) **Záznamové oblasti a ich odstupňovanie**

1. Záznamové listy majú obsahovať tieto záznamové oblasti:

- oblasť výlučne vyhradenú pre údaje týkajúce sa rýchlosti
- oblasť výlučne vyhradenú pre údaje týkajúce sa ubehnutej vzdialenosti,
- jedna alebo viac oblasti pre údaje týkajúce sa jazdnej doby, iných pracovných dôb a použiteľné aj na prestávky v práci a odpočinkové doby pre vodičov.

2. Oblasť pre zaznamenávanie rýchlosti musí byť rozdelená na úseky 20 km za hodinu alebo menej. Rýchlosť zodpovedajúca každej značke na stupnici musí byť oproti značke vypísaná číslicou. V tejto oblasti musí byť aspoň raz znázornený symbol "km/h". Posledná značka na stupnici sa musí zhodovať s hornou hranicou rozsahu merania.

3. Oblasť pre zaznamenávanie ubehnutej vzdialenosti musí byť stanovená tak, aby sa bez problémov mohol odčítať počet ubehnutých km.

4. Oblasť alebo oblasti vyhradené pre zaznamenávanie časov spomínaných v bode 1 musia byť označené tak, aby sa dali zreteľne rozlíšiť rôzne časové úseky.

(c) **Informácie, ktoré majú byť vytlačené na záznamových listoch**

Na každom liste musia byť strojom (tlačeným písmom) napísané tieto informácie:
- meno a adresa alebo obchodný názov výrobcu,
- schvaľovacia značka pre model listu,
- schvaľovacia značka pre typ alebo typy zariadení, v ktorých sa list môže použiť,

- horná hranica rozsahu merania rýchlosti, tlačeným písmom vypísaná v kilometroch za hodinu.

Pri minimálnych ďalších požiadavkách každý záznam musí mať v tlačenej forme časovú mieru odstupňovanú tak, aby sa čas dal čítať priamo v 15-minútových intervaloch, pričom sa bez ťažkosti môže určiť každý 5-minútový interval.

(d) **Voľný priestor pre ručne písané poznámky**

Na záznamoch musí byť ponechaný voľný priestor, aby vodiči mohli zapísať minimálne tieto údaje:
- priezvisko a rodné meno vodiča,
- dátum a miesto, kde používanie záznamu začína a dátum a miesto, kde končí,
- registračné číslo alebo čísla vozidla alebo vozidiel, na ktoré je vodič pridelený počas používania záznamu,
- údaje z počítača kilometrov z vozidla alebo vozidiel, na ktoré je vodič pridelený počas používania záznamu,
- čas, v ktorom sa uskutoční nejaká zmena vozidla.

V. MONTÁŽ ZÁZNAMOVÉHO ZARIADENIA

1. Záznamové zariadenie musí byť vo vozidle umiestnené tak, aby mal vodič jasný výhľad zo svojho sedadla na rýchlomer, ukazovateľ vzdialenosti a hodiny, pričom súčasne všetky časti týchto prístrojov, vrátane hnacích častí, sú chránené voči náhodnému poškodeniu.

2. Musí byť možné prispôsobenie konštanty záznamového zariadenia charakteristickému koeficientu vozidla pomocou vhodného zariadenia, známeho ako adaptér.

   Vozidlá s 2 alebo viacerými pomermi zadných náprav musia byť vybavené spínačom, aby tieto rôzne pomery mohli byť automaticky zosúladené s pomerom, na ktorý bolo zariadenie vo vozidle adaptované.

3. Po prekontrolovaní zariadenia pri inštalácii bude vo vozidle vedľa prístroja alebo priamo na ňom pripevnená inštalačná doska a to tak, aby bola jasne viditeľná. Po každej kontrole schváleným montérom alebo dielňou požadujúcou zmenu v nastavení samotnej inštalácie musí byť na miesto predošlej dosky pripevnená nová doska.

   Táto doska musí uvádzať aspoň tieto údaje:
   - meno, adresu alebo obchodný názov schváleného montéra alebo dielne,
   - charakteristický koeficient vozidla vo forme "w =...ot/km" alebo "w = ... imp/km",
   - skutočný obvod pneumatík kolies vo forme "l = ... mm",
   - dátumy, kedy bol určený charakteristický koeficient vozidla a skutočný nameraný obvod pneumatík kolies.

4. *Zaplombovanie*

   Zaplombované musia byť tieto časti:

   (a) inštalačná doska, pokiaľ nie je pripevnená tak, aby nemohla byť odstránená bez poškodenia značiek, ktoré sú na nej,

   (b) obe strany spoja medzi záznamovým zariadením samotným a vozidlom,

   (c) samotný adaptér a bod jeho vstupu do obvodu,

   (d) spínací mechanizmus pre vozidlá s 2 alebo viacerými nápravami,

   (e) spoje pripájajúce adaptér a spínač k ostatnému zariadeniu,

   (f) obaly požadované podľa kapitoly III (a) 7.2.

   (g) kryt umožňujúci prístup k prostriedkom prispôsobujúcim konštanty záznamového zariadenia k charakteristickému koeficientu vozidla.

V jednotlivých prípadoch môžu byť požadované ďalšie plomby na schválenie typu zariadenia a poznámky o umiestnení týchto plomb musia byť urobené na osvedčení o tomto schválení.

Plomby uvedené pod písm. (b), (c) a (e) je povolené odstrániť:

- v naliehavom prípade,
- pri inštalácii, úprave alebo oprave zariadenia obmedzujúceho rýchlosť, alebo zariadenia, ktoré prispieva k bezpečnosti na ceste,

za predpokladu, že záznamové zariadenie udržuje funkčnú spoľahlivosť a správnosť a je znovu zaplombované schváleným montérom alebo dielňou bezodkladne po inštalácii zariadenia obmedzujúceho rýchlosť alebo iného zariadenia, ktoré prispieva k bezpečnosti na ceste, alebo v priebehu siedmich dní v ostatných prípadoch; v prípade, že sa tieto plomby porušia, musí byť pripravené písomné vyjadrenie udávajúce dôvody pre takéto konanie a musia byť k dispozícii príslušnému orgánu.

5. Káble spájajúce záznamové zariadenie s prenášačom impulzov musia byť chránené nehrdzavejúcim púzdrom, súvisle pokrytým plastickou hmotou s oblúkovitými koncovkami s výnimkou prípadov, u ktorých je zaručená ekvivalentná ochrana pred manipuláciou inými prostriedkami (napríklad elektronickým monitorovaním ako je signálne zakódovanie), schopnými odhaliť prítomnosť akéhokoľvek zariadenia, ktoré nie je nevyhnutné pre správnu prevádzku záznamového zariadenia, a ktorého účelom je zabrániť presnej prevádzke záznamového zariadenia pomocou skratu alebo prerušenia alebo modifikáciou elektronických údajov snímača rýchlosti alebo snímača vzdialenosti. Spoj zahrnutý v zaplombovaných spojeniach sa považuje za súvislý v zmysle tohto nariadenia.

Vyššie uvedené elektronické monitorovanie sa môže nahradiť elektronickým kontrolným zariadením, ktoré zabezpečí, že záznamové zariadenie je schopné zaznamenať akýkoľvek pohyb vozidla, nezávisle od signálu snímača rýchlosti alebo vzdialenosti.

Na účely tohto bodu vozidlami kategórie M 1 a N 1 sú tie vozidlá, ktoré sú definované v časti A prílohy II k smernici Rady 70/156/EHS[4]. U týchto vozidiel, ktoré sú vybavené tachografmi v súlade s nariadením a nie sú konštruované na inštalovanie pancierových káblov medzi senzormi vzdialenosti a rýchlosti a záznamovým zariadením, sa namontuje adaptér čo možno najbližšie k senzorom vzdialenosti a rýchlosti.
Pancierové káble sa namontujú od adaptéra k záznamovému zariadeniu

VI. KONTROLY A PREHLIADKY

Členské štáty menujú organizácie, ktoré budú vykonávať kontroly a prehliadky.

1. *Osvedčenia na nové alebo opravené prístroje*

Každé jednotlivé zariadenie, či už je nové alebo opravené, sa overí s ohľadom na jeho správnu činnosť a presnosť jeho údajov a záznamov v rámci limitov stanovených v kapitole III (f) 1, a zaplombuje v súlade s kapitolou V (4) (f).

Za týmto účelom si členské štáty môžu vyhradiť úvodné overenie, skladajúce sa z kontroly a potvrdenia o zhode nového alebo opraveného zariadenia s typovo schváleným modelom a alebo s požiadavkami nariadenia a jeho príloh, alebo môžu poveriť týmto osvedčovaním výrobcov alebo ich zmocnených zástupcov.

2. *Montáž*

Po pripevnení vo vozidle musí zariadenie a celá inštalácia vyhovovať opatreniam týkajúcim sa maximálnych tolerancií stanovených v kapitole III (f) 2.

Kontrolné testy vykoná schválený montér alebo dielňa na vlastnú zodpovednosť.

3. *Periodické prehliadky*

[4] Ú. v. ES L 42, 23. 2. 1970, s. 1

(a) Periodické prehliadky zariadenia inštalovaného vo vozidle sa uskutočnia aspoň každé dva roky a môžu sa vykonať zároveň s testami spôsobilosti vozidiel pre prevádzku na cestách.

Tieto prehliadky majú zahŕňať nasledujúce kontroly:
- či zariadenie správne pracuje,
- či zariadenie má typovú schvaľovaciu značku,
- či je pripevnená inštalačná doska,
- či sú plomby na zariadení a iných častiach inštalácie neporušené,
- skutočný obvod pneumatík.

(b) Prehliadka na zabezpečenie zhody s ustanovením kapitoly III (f) 3 o maximálnych toleranciách pri používaní sa uskutoční aspoň raz za každých šesť rokov, hoci každý členský štát si môže vyhradiť kratší interval alebo takúto prehliadku vozidiel registrovaných na jeho území. Takáto prehliadka musí zahŕňať výmenu inštalačnej dosky.

4. *Meranie chýb*

Meranie chýb pri inštalácii a počas používania sa uskutoční za nasledovných podmienok, ktoré majú byť považované za súčasť štandardných testovacích podmienok:

- nezaťažené vozidlo, pri normálnej prevádzke,
- tlak vzduchu v pneumatikách v súlade s pokynmi výrobcu,
- opotrebovanie pneumatík v rámci limitov povolených vnútroštátnym právnym predpisom,
- pohyb vozidla: vozidlo poháňané vlastným motorom sa musí pohybovať v priamke a na rovnom povrchu rýchlosťou 50 ± 5 km/h; test sa môže urobiť aj na vhodnom testovacom povrchu za predpokladu, že má porovnateľnú presnosť.

PRÍLOHA

„PRÍLOHA I B

POŽIADAVKY NA KONŠTRUKCIU, SKÚŠANIE, MONTÁŽ A KONTROLU

OBSAH

6.3 Zápisy špecifických podmienok

7. Podnikové blokovanie

8. Monitorovanie kontrolných činností

9. Zistenie udalostí a/alebo porúch

9.1 „Vloženie neplatnej karty“

9.2 „Sporná karta“

9.3 „Časové prekrývanie“

9.4 „Vedenie bez príslušnej karty“

9.5 „Vloženie karty počas vedenia“

9.6 „Nesprávne uzavretá posledná relácia karty“

9.7 „Prekročenie rýchlosti“

9.8 „Prerušenie napájania“

9.9 „Pohybová dátová chyba“

9.10 „Pokus o narušenie bezpečnosti“

9.11 „Chybná funkcia karty“

9.12 „Záznamové zariadenie“

10. Zabudované skúšky a automatické skúšky

11. Čítanie z dátovej pamäte

12. Zaznamenávanie a uloženie v dátovej pamäti

12.1 Identifikačné dáta zariadenia

12.1.1 Identifikačné dáta jednotky vozidla

12.1.2 Identifikačné dáta snímača pohybu

12.2 Bezpečnostné prvky

12.3 Dáta o vložení a vybratí karty vodiča

12.4 Dáta o činnosti vodiča

12.5 Miesta, kde denný pracovný čas začína a/alebo končí

12.6 Dáta o stave kilometrov

12.7 Podrobné dáta o rýchlosti

12.8 Dáta o udalostiach

12.9 Dáta o poruchách

12.10 Kalibračné dáta

12.11 Dáta nastavenia času

12.12 Dáta o kontrolnej činnosti

12.13 Dáta o podnikovom blokovaní

12.14 Dáta o činnosti sťahovania

12.15 Dáta o špecifických podmienkach

13. Čítanie z tachografových kariet

14. Zaznamenávanie a uloženie na tachografovej karte

I. DEFINÍCIE

V tejto prílohe:

(a) **„aktivácia“ znamená:**

fázu, v ktorej sa záznamové zariadenie stáva plne funkčným a plní všetky funkcie vrátane bezpečnostných funkcií;

Aktivovanie záznamového zariadenia si vyžaduje použitie dielenskej karty a vloženie jej PIN kódu;

(b) **„autentifikácia“ znamená:**

funkciu určenú na určenie a overenie totožnosti;

(c) **„autenticita“ znamená:**

vlastnosť, že informácia prichádza od účastníka, ktorého totožnosť sa môže overiť;

(d) **„zabudovaná skúška (BIT)“ znamená:**

skúšky, ktoré sa vykonávajú na požiadanie, spustené operátorom alebo vonkajším zariadením;

(e) **„kalendárny deň“ znamená:**

deň od 00.00 hodín do 24.00 hodím. Všetky kalendárne dni vzťahujúce sa na UTC čas (koordinovaný svetový čas);

(f) **„kalibrácia“ znamená:**

aktualizácia alebo potvrdenie parametrov vozidla, uložených v dátovej pamäti. Parametre vozidla zahŕňajú identifikáciu vozidla (VIN, VRN a členský štát registrácie) a charakteristiky vozidla (w, k, l, rozmer pneumatík, nastavenie zariadenia obmedzujúceho rýchlosť (ak je), aktuálny UTC čas, aktuálny stav počítadla kilometrov);

kalibrovanie záznamového zariadenia si vyžaduje použitie dielenskej karty;

(g) **„číslo karty“ znamená:**

16 alfanumerických znakov, ktoré jednoznačne identifikujú tachografovú kartu v členskom štáte. Číslo karty (prípadne) obsahuje poradový index, index náhrady a index obnovy;

karta je preto jednoznačne identifikovaná kódom vydávajúceho členského štátu a číslom karty;

(h) **„poradový index karty“ znamená:**

14 miestny alfanumerický znak čísla karty, ktorý sa používa na rozlíšenie rôznych kariet vydaných spoločnosti alebo orgánu, ktorému sa môže vydať niekoľko tachografových kariet. Spoločnosť alebo orgán je jednoznačne identifikovaný 13 prvými znakmi čísla karty;

(i) **„index obnovy karty“ znamená:**

16 miestny alfanumerický znak čísla karty, ktorý zvýši vždy pri obnove karty;

(j) „**index náhrady karty“ znamená:**

15 miestny alfanumerický znak čísla karty, ktorý zvýši vždy pri náhrade karty;

(k) **„charakteristický koeficient vozidla“ znamená:**

numerickú veličinu, udávajúcu hodnotu výstupného signálu emitovaného časťou vozidla, ktorá ho spája so záznamovým zariadením (výstupný hriadeľ prevodovky alebo náprava) zatiaľčo vozidlo prejde vzdialenosť jedného kilometra za štandardných skúšobných podmienok (pozri kapitolu VI(5)). Charakteristický koeficient je vyjadrený v impulzoch na kilometer (w = ... imp/km);

(l) **„podniková karta“ znamená:**

tachografovú kartu vydanú orgánmi členského štátu vlastníkovi alebo držiteľovi vozidiel vybavených záznamovým zariadením;

podniková karta identifikuje podnik a umožňuje zobrazovanie, sťahovanie a tlač dát uložených v záznamovom zariadení; ktoré bolo týmto podnikom zablokované;

(m) **„konštanta záznamového zariadenia“ znamená:**

numerickú veličinu udávajúcu hodnotu vstupného signálu potrebnú na zobrazenie a zaznamenanie prejdenej vzdialenosti 1 km; táto konštanta sa vyjadruje v impulzoch na kilometer (k = ... imp/km);

(n) „**nepretržitý čas vedenia“ počítaný v záznamovom zariadení ako**[(1)]

nepretržitý čas vedenia vypočítaný ako súčet aktuálnych časov vedenia konkrétneho vodiča, od konca jeho posledného časového úseku POHOTOVOSTI alebo PRESTÁVKY/ODPOČINKU alebo NEZNÁMEHO času[(2)] 45 alebo viac minút (tento časový úsek môže byť rozdelený na niekoľko 15–minútových alebo dlhších intervalov). Výpočty podľa potreby berú do úvahy doterajšie činnosti uložené na karte vodiča. Keď vodič nevložil svoju kartu, výpočty vychádzajú z uložených dát zaznamenaných do času, kedy nebola vložená karta a vzťahujúcich sa k príslušnému slotu;

(o) **„kontrolná karta“ znamená:**

tachografovú kartu, ktorú vnútroštátnemu príslušnému kontrolnému orgánu vydali orgány členského štátu;

kontrolná karta identifikuje kontrolný orgán a prípadne kontrolóra a umožňuje získať prístup k uloženým dátam v dátovej pamäti alebo na karte vodiča formou čítania, tlače a/alebo sťahovania;

(p) **„kumulovaný čas prestávok“ sa počíta v záznamovom zariadení ako**[(1)]:

kumulovaný čas prestávky z času vedenia sa vypočíta ako súčet aktuálnych časov POHOTOVOSTI alebo PRESTÁVKY/ODPOČINKU alebo NEZNÁMEHO času[(2)] 15 alebo viac minút pre konkrétneho vodiča od konca jeho posledného časového úseku POHOTOVOSTI alebo PRESTÁVKY/ODPOČINKU alebo NEZNÁMEHO[(2)] času 45 alebo viac minút (tento časový úsek môže byť rozdelený na niekoľko 15–minútových alebo dlhších intervalov).

Výpočty podľa potreby berú do úvahy doterajšie činnosti uložené na karte vodiča. Neznáme časové úseky s negatívnou dobou trvania (začiatok neznámého časového úseku > koniec neznámeho časového úseku) z dôvodu časového prekrývania medzi dvoma rôznymi záznamovými zariadeniami, sa pri výpočte neberú do úvahy.

Keď vodič nevložil svoju kartu, výpočty vychádzajú z uložených dát zaznamenaných do času, kedy nebola vložená karta a vzťahujúcich sa k príslušnému slotu;

(q) „**dátová pamäť“ znamená:**

elektronické pamäťové dátové zariadenie zabudované do záznamového zariadenia;

(r) **„digitálny podpis“ znamená:**

---

(1) Tento spôsob výpočtu súvislého času vedenia vozidla a kumulovaných časov prestávok slúži záznamovému zariadeniu na výpočet výstrahy pri súvislom čase vedenia vozidla. Neprejudikuje právny výklad týchto časov.

(2) Neznámy čas sú časové úseky zodpovedajúce intervalom, počas ktorých nebola karta vodiča vložená v záznamovom zariadení a nevykonal sa žiadny manuálny záznam o činnosti vodiča.

dáta pripojené k bloku dát alebo kryptografická transformácia bloku dát, ktorá umožňuje príjemcovi bloku dát overiť si hodnovernosť a integritu bloku dát;

(s) **„sťahovanie“ znamená:**

kopírovanie, spolu s digitálnym podpisom, časti alebo úplnej sady dát uložených v dátovej pamäti vozidla alebo v pamäti tachografovej karty;

sťahovaním sa nesmú meniť alebo vymazať žiadne uložené dáta;

(t) **„karta vodiča“ znamená:**

tachografovú kartu vydanú vodičovi orgánmi členského štátu;

karta vodiča identifikuje vodiča a umožňuje uloženie dát o činnosti vodiča;

(u) **„účinný obvod pneumatík kolies“ znamená:**

priemernú hodnotu vzdialeností prejdených každým z kolies poháňajúcich vozidlo (hnacie kolesá) v priebehu jednej úplnej otáčky. Meranie týchto vzdialeností sa vykoná podľa štandardných skúšobných podmienok (kapitola VI/5)) a vyjadrí sa vo forme „l = ... mm“. Výrobcovia vozidiel môžu nahradiť meranie týchto vzdialeností teoretickým výpočtom, ktorý berie do úvahy rozloženie hmotnosti na nápravy, nenaloženého vozidla v normálnom pohotovostnom stave[(1)]. Metódu takéhoto teoretického výpočtu schváli príslušný orgán členského štátu;

(v) **„udalosť“ znamená:**

nenormálnu činnosť zistenú záznamovým zariadením, ktorá môže byť spôsobená pokusom o podvod;

(w) **„porucha““ znamená:**

nenormálnu činnosť zistenú záznamovým zariadením, ktorá môže byť spôsobená technickou chybou alebo technickou poruchou;

(x) **„inštalácia“ znamená:**

montáž záznamového zariadenia do vozidla;

(y) **„snímač pohybu“ znamená:**

časť záznamového zariadenia, poskytujúca signál predstavujúci rýchlosť vozidla a/alebo prejdenú vzdialenosť;

(z) **„neplatná karta“ znamená:**

karta, u ktorej bola zistená chyba, alebo u ktorej chýba počiatočná autentifikácia, alebo ešte nenastal začiatok jej platnosti, alebo jej platnosť skončila;

---

(1) Smernica 97/27/ES z 22. júla 1997, týkajúca sa hmotností a rozmerov určitých kategórií motorových a ich prípojných vozidiel, ktorou sa mení a dopĺňa smernica 70/156/EHS (Ú. v. ES L 233, 25. 8. 1997, s. 1).

(aa) **„záznamové zariadenie sa nevyžaduje“ znamená:**

keď sa používanie záznamového zariadenia nevyžaduje podľa ustanovení nariadenia Rady (EHS) č. 3820/85;

(bb) **„prekročenie rýchlosti“ znamená:**

prekročenie povolenej rýchlosti vozidla definované ako každý časový úsek nad 60 sekúnd, počas ktorej nameraná rýchlosť vozidla presiahne limit pre nastavenie zariadenia obmedzujúceho rýchlosť, stanovený v smernici Rady 92/6/EHS z 10. februára 1992 o inštalovaní a používaní zariadení obmedzujúcich rýchlosť pre niektoré kategórie motorových vozidiel v spoločenstve[(2)];

(cc) **„pravidelná prehliadka“ znamená:**

súbor činností vykonávaných za účelom kontroly, či záznamové zariadenia pracuje riadne a či jeho nastavenie zodpovedá parametrom vozidla;

(dd) **„tlačiareň“ znamená:**

komponent záznamového zariadenia, ktorý zabezpečuje tlač uložených dát;

(ee) **„záznamové zariadenia“ znamená:**

úplné vybavenie určené na montáž do cestných vozidiel na automatické alebo poloautomatické zobrazovanie, zaznamenávanie a uloženie dát o pohybe takých vozidiel a o určitých časoch práce ich vodičov;

(ff) **„obnova“ znamená:**

vydanie novej tachografovej karty keď existujúca karta prestane platiť, alebo ak je chybná a bola vrátená vydávajúcemu orgánu. Z obnovy vždy vyplýva istota, že nemôžu súčasne existovať dve platné karty;

(gg) **„oprava“ znamená:**

každá oprava snímača pohybu alebo jednotky vozidla, ktorá vyžaduje odpojenie napájania, alebo odpojenie od iných komponentov záznamového zariadenia, alebo jeho otvorenie;

(hh) **„náhrada“ znamená:**

vydanie tachografovej karty ako náhrady za existujúcu tachografovú kartu, ktorá bola vyhlásená za stratenú, odcudzenú alebo chybnú a nebola vrátená vydávajúcemu orgánu. Z obnovy vždy vyplýva riziko súčasnej existencie dvoch platných kariet;

(ii) **„bezpečnostná certifikácia“ znamená:**

proces ktorým certifikačný orgán ITSEC[(1)] osvedčí, že overované záznamové zariadenie (alebo komponent) alebo tachografová karta spĺňajú bezpečnostné požiadavky definované v doplnku 10 Všeobecných bezpečnostných cieľov;

(jj) **„automatická skúška“ znamená:**

cyklickú a automatickú skúšku vykonávanú záznamovým zariadením na zisťovanie porúch;

---

(2) Ú. v. ES L 57, 2. 3. 1992, s. 27.

(1) Odporúčanie Rady 95/144/ES zo 7. apríla 1995 o spoločných kritériách hodnotenia informačných technológií (Ú. v. ES L 93, 26. 4. 1995, s. 27).

(kk) **„tachografová karta“ znamená:**

inteligentnú (čipovú) používanú záznamovým zariadením. Tachografové karty umožňujú záznamovému zariadeniu určiť totožnosť (skupiny) držiteľa karty a umožňujú prenos a uloženie dát. Tachografová karta môže byť tohto typu:

– karta vodiča,

– kontrolná karta,

– dielenská karta,

– podniková karta;

(ll) **„typové schválenie“ znamená:**

postup, ktorým členský štát potvrdí, že overované záznamové zariadenie (alebo komponent) alebo tachografová karta spĺňajú požiadavky tohto nariadenia;

(mm) **„rozmer pneumatiky“ znamená:**

označenie rozmerov pneumatík (vonkajších hnacích kolies) v súlade so smernicou 92/23/EHS z 31. marca 1992[(2)];

(nn) **„identifikácia vozidla“ znamená:**

čísla identifikujúce vozidlo: registračné číslo vozidla (VRN) s identifikáciou členského štátu registrácie a identifikačným číslom vozidla (VIN)[(3)];

(oo) **„jednotka vozidla“ znamená:**

záznamové zariadenie okrem snímača pohybu a káblov pripojených k snímaču. Jednotka vozidla môže byť buď jedno zariadenie alebo niekoľko zariadení rozmiestnených vo vozidle, pokiaľ spĺňajú bezpečnostné požiadavky tohto nariadenia;

(pp) **na účely výpočtu v záznamovom zariadení „týždeň“ znamená:**

časový úsek od 00.00 hodín UTC v pondelok do 24.00 UTC v nedeľu;

(qq) **„dielenská karta“ znamená:**

tachografovú kartu vydanú orgánmi členského štátu výrobcovi záznamového zariadenia, montérovi, výrobcovi vozidla alebo dielni, ktorých schválil uvedený členský štát.

Dielenská karta identifikuje držiteľa karty a umožňuje skúšanie, kalibráciu a/alebo sťahovanie dát zo záznamového zariadenia;

II. VŠEOBECNÉ CHARAKTERISTIKY A FUNKCIE ZÁZNAMOVÉHO ZARIADENIA

000 každé vozidlo vybavené záznamovým zariadením, ktoré spĺňa ustanovenia tejto prílohy, musí mať k dispozícii ukazovateľ rýchlosti a počítadlo kilometrov. Tieto funkcie môžu byť súčasťou záznamového zariadenia.

---

(2) Ú. v. ES L 129, 14. 5. 1992, s. 95.

(3) Smernica 76/114/EHS z 18. decembra 1976 o aproximácii právnych predpisov členských štátov, týkajúca sa povinných štítkov a nápisov pre motorové a ich prípojné vozidlá a ich umiestnenia a spôsobu pripevnenia (Ú. v. ES L 24, 30. 1. 1976, s. 1).

1. **Všeobecné charakteristiky**

Účelom záznamového zariadenia je zaznamenávať, ukladať, zobrazovať, tlačiť a vydávať dáta týkajúce sa činnosti vodiča.

001 Záznamové zariadenie obsahuje káble, snímač pohybu a jednotku vozidla.

002 Jednotka vozidla obsahuje procesor, dátovú pamäť, hodiny ukazujúce reálny čas, dve rozhrania inteligentnej karty (vodič a druhý vodič), tlačiareň, displej, vizuálne výstražné zariadenie, kalibračný/sťahovací konektor a zariadenie umožňujúce vstup užívateľa.

Záznamové zariadenie môže byť spojené s inými zariadeniami pomocou doplnkových konektorov.

003 Akékoľvek doplnkové funkcie zabudované alebo pripojené k záznamovému zariadeniu, zariadenie alebo zariadenia bez ohľadu na to či sú schválené, nesmú rušiť alebo byť schopné rušiť riadnu a bezpečnú prevádzku záznamového zariadenia a porušovať ustanovenia tohto nariadenia.

Užívatelia záznamového zariadenia sa sami zariadeniu identifikujú tachografovými kartami.

004 Záznamové zariadenie poskytuje selektívne prístupové práva k dátam a funkciám podľa typu užívateľa a/alebo totožnosti.

Záznamové zariadenie zaznamenáva a ukladá dáta vo svojej dátovej pamäti a v tachografovej karte.

To sa uskutočňuje v súlade so smernicou 95/46/ES z 24. októbra 1995 o ochrane jednotlivcov z hľadiska spracovávania osobných údajov a o pohybe takých údajov[(1)].

2. **Funkcie**

005 Záznamové zariadenie zabezpečuje tieto funkcie:

- monitorovanie vkladania a vyberania kariet,
- meranie času a vzdialenosti,
- meranie času,
- monitorovanie činností vodiča,
- monitorovanie stavu vedenia vozidla,
- manuálne záznamy vodiča:
  - záznam o miestach, kde začína a/alebo končí pracovný deň,
  - manuálny záznam o činnostiach vodiča,
  - záznam o špecifických podmienkach,
- podnikové blokovanie,
- monitorovanie kontrolných činností,
- zistenie udalostí a/alebo porúch,
- zabudované a automatické skúšky,
- čítanie z dátovej pamäte,
- zaznamenávanie a uloženie v dátovej pamäti,
- čítanie z tachografovej karty,
- zaznamenávanie a uloženie na tachografovej karte,
- zobrazovanie,
- tlač,

(1) Ú. v. ES L 281, 23. 11. 1995, s. 31.

– výstraha,

– sťahovanie dát do vonkajších médií,

– výstupné dáta pre doplnkové vonkajšie zariadenia,

– kalibrácia,

– nastavenie času.

3. **Prevádzkové režimy**

006 Záznamové zariadenie pracuje v štyroch prevádzkových režimoch:

– režim prevádzky,

– režim kontroly,

– režim kalibrácie,

– režim podniku.

007 Záznamové zariadenie sa po vložení platných tachografových kariet do rozhrania karty prepne do týchto prevádzkových režimov:

Prevádzkový režim		Slot vodiča				
		Žiadna karta	Karta vodiča	Kontrolná karta	Dielenská karta	Podniková karta
Slot druhého vodiča	Žiadna karta	Prevádzka	Prevádzka	Kontrola	Kalibrácia	Podnik
	Karta vodiča	Prevádzka	Prevádzka	Kontrola	Kalibrácia	Podnik
	Kontrolná karta	Kontrola	Kontrola	Kontrola(*)	Prevádzka	Prevádzka
	Dielenská karta	Kalibrácia	Kalibrácia	Prevádzka	Kalibrácia(*)	Prevádzka
	Podniková karta	Podnik	Podnik	Prevádzka	Prevádzka	Podnik (*)

008 (*) V týchto situáciách záznamové zariadenie používa len tachografovú kartu vloženú do slotu vodiča.

009 Záznamové zariadenie ignoruje vložené neplatné karty, musí byť však možné zobraziť, vytlačiť alebo stiahnuť dáta uložené na karte, ktorá je už neplatná.

010 Všetky funkcie uvedené v II.2 musia pracovať v ktoromkoľvek prevádzkovom režime s týmito výnimkami:

– kalibračná funkcia je k dispozícii len v režime kalibrácie,

– funkcia nastavenia času je mimo režimu kalibrácie k dispozícii len obmedzene,

– funkcie manuálneho záznamu vodiča sú k dispozícii len v režime prevádzky alebo kalibrácie,

– funkcia podnikového blokovania je k dispozícii len v režime podniku,

– funkcia monitorovania a kontroly je k dispozícii len v režime kontroly,

– funkcia sťahovania nie je k dispozícii v režime prevádzky (s výnimkou uvedenou v požiadavke 150).

011 Záznamové zariadenie môže poskytnúť ktorékoľvek dáta na zobrazenie, tlač alebo pre vonkajšie rozhrania s týmito výnimkami:

– v režime prevádzky, akékoľvek osobné údaje (priezvisko a meno(á)), ktoré nezodpovedajú vloženej tachografovej karte sa zneviditeľnia a akékoľvek číslo karty, ktoré nezodpovedá vloženej tachografovej karte sa čiastočne zneviditeľní (nepárne znaky – zľava doprava – sa zneviditeľnia),

– v režime podniku, údaje vzťahujúce sa k vodičovi (požiadavka 081, 084 a 087) sa môžu poskytnúť len za časové úseky, ktoré nie sú zablokované druhým podnikom (identifikovaným prvými 13–timi číslicami čísla podnikovej karty),

– ak nie je do záznamového zariadenia vložená žiadna karta, údaje vzťahujúce sa k vodičovi sa môžu poskytnúť len za aktuálny kalendárny deň a osem predchádzajúcich kalendárnych dní.

4. **Bezpečnosť**

Bezpečnosť systému je zameraná na ochranu dátovej pamäti tak, aby bolo zabránené neoprávnenému prístupu k dátam a k ich manipulácii, aby bol odhalený každý taký pokus, na ochranu integrity a autenticity dát vymieňaných medzi senzorom pohybu a jednotkou vozidla, na ochranu integrity a autenticity dát vymieňaných medzi záznamovým zariadením a tachografovými kartami a na overenie integrity a autenticity sťahovaných dát.

012 Aby bola zaručená bezpečnosť systému, musí záznamové zariadenie spĺňať bezpečnostné požiadavky špecifikované vo všeobecných bezpečnostných cieľoch senzoru pohybu a jednotky vozidla (doplnok 10).

III. KONŠTRUKČNÉ A FUNKČNÉ POŽIADAVKY NA ZÁZNAMOVÉ ZARIADENIE

1. **Monitorovanie vkladania a vyberania kariet**

013 Záznamové zariadenie monitoruje rozhrania kariet aby sa zistilo ich vkladanie a vyberanie.

014 Po vložení karty záznamové zariadenie zistí, či je vložená karta platnou tachografovou kartou a v takom prípade identifikuje typ karty.

015 Záznamové zariadenie musí byť konštruované tak, aby sa tachografová karta po jej správnom vložení do rozhrania karty zablokovala v danej polohe.

016 Uvoľnenie karty sa môže uskutočniť len keď vozidlo stojí a potom čo boli príslušné dáta uložené na karte. Uvoľnenie karty môže nastať len po zodpovedajúcej činnosti užívateľa.

2. **Meranie rýchlosti a vzdialenosti**

017 Táto funkcia musí nepretržite merať a udávať počet kilometrov zodpovedajúci celkovej vzdialenosti prejdenej vozidlom.

018 Táto funkcia musí nepretržite merať a udávať rýchlosť vozidla.

019 Funkcia merania rýchlosti musí poskytovať aj informácie o tom, či sa vozidlo pohybuje alebo či stojí. Vozidlo sa považuje za vozidlo v pohybe len čo funkcia zistí viac než 1 imp/s zo senzora pohybu počas minimálne piatich sekúnd, inak sa vozidlo považuje za stojace vozidlo.

Zariadenia ukazujúce rýchlosť(rýchlomer) a celkovú prejdenú vzdialenosť (počítadlo kilometrov) inštalované vo vozidle vybavenom záznamovým zariadením, spĺňajúcim ustanovenia tohto nariadenia, musí spĺňať požiadavky týkajúce sa maximálnych tolerancií stanovené v tejto prílohe (kapitoly III(2)(1) a III(2)(2)).

2.1 ***Meranie prejdenej vzdialenosti***

020 Prejdená vzdialenosť sa môže merať buď:

– tak aby sa spočítali pohyby dopredu a dozadu, alebo

– tak aby sa započítal len pohyb dopredu.

021 Záznamové zariadenie meria vzdialenosť od 0 do 9 999 999,9 km.

022 Meraná vzdialenosť musí byť v rámci nasledovných tolerancií (vzdialenosti minimálne 1000 m):

– ± 1% pred inštaláciou,

– ± 2% pri inštalácii a pri pravidelnej prehliadke,

– ± 4% počas používania.

023 Vzdialenosť sa musí merať s presnosťou 0,1 km.

2.2 ***Meranie rýchlosti***

024 Záznamové zariadenie meria rýchlosť od 0 do 220 km/h.

025 Aby bola zabezpečená maximálna tolerancia udávanej rýchlosti ± 6 km/h a berúc do úvahy:

– toleranciu ± 2 km/h pre odchýlky vstupov (odchýlky pneumatík, ...),

– toleranciu ± 1 km/h pri meraniach vykonávaných počas inštalácie alebo pravidelnej prehliadky,

záznamové zariadenie musí pre rýchlosti od 20 do 180 km/h a pre charakteristické koeficienty vozidla od 4 000 do 25 000 imp/km, merať rýchlosť s toleranciou ± 1 km/h (pri konštantnej rýchlosti).

Poznámka: Z ukladania dát vyplýva ďalšia tolerancia ± 0,5 km/h pre rýchlosti uložené záznamovým zariadením.

025a Rýchlosť sa správne meria v rámci normálnych tolerancií do 2 sekúnd po skončení zmeny rýchlosti, keď sa rýchlosť zmenila zrýchlením do 2 m/s^2.

026 Rýchlosť sa musí merať s presnosťou minimálne 1 km/h.

3. **Meranie času**

027 Funkcia merania času meria čas stále a udáva digitálne UTC dátum a čas.

028 UTC dátum a čas sa používajú pre dátumové údaje záznamového zariadenia (zaznamenávanie, tlač, výmena dát, zobrazovanie, ...).

029 Aby bolo možné udať miestny čas musí sa dať meniť viditeľný časový údaj v polhodinových krokoch.

030 Časová odchýlka v podmienkach typového schválenia smie byť ± 2 sekundy za deň.

031 Čas sa musí merať s presnosťou minimálne 1 sekundy.

032 Meranie času nesmie byť v podmienkach typového schválenia ovplyvnené prerušením vonkajšieho napájania po dobu minimálne 12–tich mesiacov.

4. **Monitorovanie činností vodiča**

033 Táto funkcia nepretržite a osobitne monitoruje činnosti vodiča a druhého vodiča.

034 Činnosťou vodiča je VEDENIE, PRÁCA, POHOTOVOSŤ alebo PRESTÁVKA/ODPOČINOK.

035 Vodič a/alebo druhý vodič musí mať možnosť manuálne zvoliť PRÁCU, POHOTOVOSŤ alebo PRESTÁVKU/ODPOČINOK.

036 Keď sa vozidlo pohybuje pre vodiča sa automaticky zvolí VEDENIE a pre druhého vodiča sa automaticky zvolí POHOTOVOSŤ.

037 Keď vozidlo stojí pre vodiča sa automaticky zvolí PRÁCA.

038 Prvá zmena činnosti do 120 sekúnd po automatickej zmene na PRÁCA v dôsledku zastavenia vozidla sa považuje za zmenu, ktorá nastala v dobe státia vozidla (preto je možné, že sa zruší zmena na PRÁCA).

039 Výstupy tejto funkcie týkajúce sa zmeny činnosti určené pre záznamové funkcie sa vykonajú s presnosťou jednej minúty.

040 Ak k určitému časovému okamihu v rámci jednej kalendárnej minúty nastala činnosť VEDENIE, celá minúta sa berie ako VEDENIE.

041 Ak k určitému časovému okamihu v rámci jednej kalendárnej minúty nastala počas bezprostredne predchádzajúcej a bezprostredne nadchádzajúcej minúty činnosť VEDENIE, celá minúta sa berie ako VEDENIE.

042 Pre kalendárnu minútu, ktorá sa nepovažuje za VEDENIE podľa predchádzajúcich požiadaviek, sa celá minúta priraďuje k tej činnosti, ktorá v priebehu minúty trvala najdlhšie (alebo k poslednej z rovnako dlhých činností).

043 Táto funkcia permanentne monitoruje nepretržitý čas vedenia a kumulovaný čas prestávky vodiča.

5. **Monitorovanie stavu vedenia vozidla**

044 Táto funkcia permanentne monitoruje stav vedenia vozidla.

045 Stav vedenia vozidla POSÁDKA sa zvolí vtedy, keď sú v zariadení vložené dve platné karty vodiča, stav vedenia vozidla JEDEN VODIČ sa zvolí v ostatných prípadoch.

6. **Manuálne zápisy vodiča**

6.1 ***Zápisy o mieste, kde denný pracovný čas začína a/alebo končí***

046 Táto funkcia umožňuje zaznamenať miesta, kde denný pracovný čas začína a/alebo končí pre vodiča alebo druhého vodiča.

047 Miesta sú definované ako štáty a prípadne regióny.

048 Pri vyberaní karty vodiča (alebo dielenskej karty), záznamové zariadenie vyzve (druhého) vodiča, aby zaznamenal „miesto, kde denný pracovný čas končí“.

049 Záznamové zariadenie musí umožniť ignorovanie tejto výzvy.

050 Musí byť možné vložiť dáta o miestach, kde denný pracovný čas začína a/alebo končí bez karty, alebo v mimo času vloženia alebo vybratia karty.

6.2 ***Manuálne zápisy o činnostiach vodiča***

050a Po vložení karty vodiča (alebo dielenskej karty) a len v tomto čase, záznamové zariadenie:

- ukáže držiteľovi karty dátum a čas posledného vybratia karty, a
- vyzve držiteľa karty aby uviedol, či terajšie vloženie karty predstavuje pokračovanie aktuálneho denného pracovného času.

Záznamové zariadenie musí držiteľovi karty umožniť, aby ignoroval otázku alebo aby odpovedal kladne alebo záporne:

– v prípade keď držiteľ karty ignoruje otázku, záznamové zariadenie vyzve držiteľa karty na vloženie záznamu „miesto, kde denný pracovný čas začína“. Záznamové zariadenie musí umožniť ignorovanie tejto výzvy. Ak je údaj o mieste vložený, potom sa zaznamená v dátovej pamäti a v tachografovej karte, a priradí sa k času vloženia karty,

– v prípade kladnej alebo zápornej odpovede, záznamové zariadenie vyzve držiteľa karty aby vložil činnosti PRÁCA, POHOTOVOSŤ alebo PRESTÁVKA/ODPOČINOK manuálne, s ich dátumom a časom začiatku a konca a to len za časový úsek medzi posledným vytiahnutím karty a terajším vložením karty a bez toho, aby nastalo vzájomné prekrývanie takých činností. Toto sa musí uskutočniť podľa nasledovného postupu:

- v prípade, keď držiteľ karty odpovie kladne na otázku, záznamové zariadenie vyzve držiteľa karty aby vložil činnosti manuálne v chronologickom poradí za časový úsek medzi posledným vytiahnutím karty a terajším vložením karty. Proces skončí, keď sa koncový čas manuálne vloženej činnosti rovná času vloženia karty.
- v prípade, keď držiteľ karty odpovie záporne na otázku, záznamové zariadenie:
- vyzve držiteľa karty aby vložil činnosti v chronologickom poradí za časový úsek od vytiahnutia karty do času skončenia príslušného denného pracovného času (alebo činnosti týkajúce sa uvedeného vozidla v prípade, keď denný pracovný čas pokračuje na záznamovom liste). Záznamové zariadenie preto predtým, než umožní držiteľovi karty manuálny záznam činnosti, vyzve držiteľa karty aby uviedol, či čas skončenia poslednej zaznamenanej činnosti predstavuje koniec predchádzajúceho pracovného časového úseku (pozri poznámku nižšie).

Poznámka: v prípade, keď držiteľ karty neuvedie koniec predchádzajúceho pracovného časového úseku a manuálne zaznamená činnosť, ktorej čas sa rovná času vloženia karty, záznamové zariadenie:

– predpokladá, že pracovný deň končí na začiatku časového úseku ODPOČINKU (alebo pretrvávajúcej NEZNÁMOM časovom úseku) po vytiahnutí karty alebo v čase vytiahnutia karty, ak nebol vložený žiadny časový úsek odpočinku (a ak žiadny časový úsek nezostáva NEZNÁMY),

– predpokladá, že počiatočný čas sa rovná času vloženia karty,

– pokračuje v krokoch uvedených nižšie;

– potom, ak čas skončenia príslušného pracovného časového úseku sa líši od času vytiahnutia karty, alebo ak nebolo vložené žiadne miesto skončenia pracovného dňa v uvedenom čase, vyzve držiteľa karty aby „potvrdil alebo vložil miesto skončenia denného pracovného času“ (záznamové zariadenie musí umožniť ignorovanie tejto výzvy). Ak je miesto vložené, zaznamená sa v tachografovej karte len a len vtedy, keď sa líši od miesta vloženého pri vytiahnutí karty (ak bolo vložené) a vzťahuje sa k času skončenia pracovného dňa,

– potom vyzve držiteľa karty aby „vložil čas začiatku“ aktuálneho denného pracovného času (alebo činností vzťahujúcich sa k aktuálnemu vozidlu v prípade, keď držiteľ karty predtým použil záznamový list v priebehu tohto denného pracovného času) a tiež vyzve držiteľa aby vložil „miesto, kde denný pracovný čas začína“ (záznamové zariadenie musí umožniť ignorovanie tejto výzvy). Ak je miesto vložené, zaznamená sa v tachografovej karte a vzťahuje sa k tomuto času začiatku. Ak je tento čas začiatku rovný času vloženia karty, miesto sa zaznamená aj v dátovej pamäti,

– potom, ak sa tento čas začiatku líši od času vloženia karty, vyzve držiteľa karty aby manuálne vložil činnosti v chronologickom poradí od tohto času začiatku až po čas vloženia karty. Proces končí keď sa čas skončenia manuálne vloženej činnosti rovná času vloženia karty,

– záznamové zariadenie potom umožní držiteľovi karty aby zmenil ktorúkoľvek manuálne vloženú činnosť, kým sa pomocou špecifického príkazu nevykoná potvrdenie; potom je zakázaná akákoľvek zmena,

– odpovede na prvú otázku bez vloženia žiadnej činnosti, interpretuje záznamové zariadenie ako ignorovanie otázky zo strany držiteľa karty.

Počas celého procesu záznamové zariadenie čaká na vloženie dát tieto v týchto časových limitoch:

– 1 minúta – ak sa počas týchto 60–tich sekúnd neuskutoční žiadna interakcia s rozhraním zariadenia človek–stroj (s vizuálnou a prípadne zvukovou výstrahou po 30–tich sekundách), alebo

– ak je karta vytiahnutá alebo je vložená karta iného vodiča (alebo dielne), alebo

– len čo sa vozidlo začne pohybovať,

v tomto prípade záznamové zariadenie potvrdí všetky už vložené dáta.

6.3 **Zápisy špecifických podmienok**

050b Záznamové zariadenie musí v reálnom čase vodičovi umožniť zápis týchto dvoch špecifických podmienok:

– „ZÁZNAMOVÉ ZARIADENIE SA NEVYŽADUJE“ (začiatok, koniec)

– „PREVOZ PREVOZNOU LOĎOU/VLAKOM“

Pri otvorenej podmienke „ZÁZNAMOVÉ ZARIADENIE SA NEVYŽADUJE“ nesmie nastať podmienka „PREVOZ PREVOZNOU LOĎOU/VLAKOM“.

Ak je karta vodiča vložená alebo vytiahnutá musí záznamové zariadenie automaticky uzavrieť otvorenú podmienku „ZÁZNAMOVÉ ZARIADENIE SA NEVYŽADUJE“.

7. **Podnikové blokovanie**

051 Táto funkcia umožňuje riadiť blokovania zavedené podnikom, aby si podnik sám obmedzil prístup k dátam v režime podniku.

052 Podnikové blokovania pozostávajú z dátumu/času začiatku (lock–in) a dátumu/času skončenia (lock–out) v súvislosti s identifikáciou podniku na základe čísla podnikovej karty (pri zablokovaní).

053 Blokovania sa môžu zapnúť alebo vypnúť len v reálnom čase.

054 Odblokovanie môže vykonať len podnik, ktorého blokovanie je zapnuté (identifikovaný prvými 13–timi číslicami čísla podnikovej karty), alebo

055 odblokovanie je automatické ak iný podnik zapne blokovanie.

055a V prípade keď podnik aktivuje (lock–in) blokovanie a keď predchádzajúce blokovanie platilo pre rovnaký podnik potom sa predpokladá, že predchádzajúce blokovanie nebolo vypnuté a je stále zapnuté.

8. **Monitorovanie kontrolných činností**

056 Táto funkcia monitoruje ZOBRAZOVANIE, TLAČ, JEDNOTKU VOZIDLA A SŤAHOVACIE činnosti vykonávané v priebehu režimu kontroly.

057 Táto funkcia monitoruje aj KONTROLU PREKROČENIA RÝCHLOSTI v priebehu režimu kontroly. Kontrola prekročenia rýchlosti sa považuje za uskutočnenú, ak v režime kontroly bol výpis „prekročenie kontroly“ poslaný do tlačiarne alebo na displej, alebo keď boli z dátovej pamäti stiahnuté dáta „udalosti a poruchy“.

9. **Zistenie udalostí a/alebo porúch**

058 Táto funkcia zisťuje tieto udalosti a/alebo poruchy:

9.1 ***„Vloženie neplatnej karty“***

059 Táto udalosť sa spustí po vložení akejkoľvek neplatnej karty a/alebo keď skončí platnosť vloženej karty.

9.2 ***„Sporná karta“***

060 Táto udalosť sa spustí, keď vznikne ktorákoľvek z kombinácií platných kariet označená X v nasledovnej tabuľke:

Sporná karta		Slot vodiča				
		Žiadna karta	Karta vodiča	Kontrolná karta	Dielenská karta	Podniková karta
Slot druhého vodiča	Žiadna karta					
	Karta vodiča				X	
	Kontrolná karta			X	X	X
	Dielenská karta		X	X	X	X
	Podniková karta			X	X	X

9.3 ***„Časové prekrývanie“***

061 Táto udalosť sa spustí, keď dátum/čas posledného vytiahnutia karty vodiča, čítaný z karty je neskorší, než aktuálny dátum/čas záznamového zariadenia, do ktorého je karta vložená.

9.4 ***„Vedenie bez príslušnej karty“***

062 Táto udalosť sa spustí pri ktorejkoľvek z kombinácií tachografových kariet označených X v nasledovnej tabuľke, keď sa činnosť vodiča zmení z VEDENIA, alebo keď nastane počas činnosti vodiča VEDENIE zmena prevádzkového režimu:

Vedenie bez príslušnej karty		Slot vodiča				
		Žiadna karta	Karta vodiča	Kontrolná karta	Dielenská karta	Podniková karta
Slot druhého vodiča	Žiadna (alebo neplatná) karta	X		X		X
	Karta vodiča	X		X	X	X
	Kontrolná karta	X	X	X	X	X
	Dielenská karta	X	X	X		X
	Podniková karta	X	X	X	X	X

9.5 ***„Vloženie karty počas vedenia“***

063 Táto udalosť sa spustí, keď sa vloží tachografová karta do ktoréhokoľvek slotu, pričom činnosť vodiča je VEDENIE.

9.6 ***„Nesprávne uzavretá posledná relácia karty“***

064 Táto udalosť sa spustí, keď pri vložení karty záznamové zariadenie zistí, že napriek ustanoveniam uvedeným v odseku III(1), nebola správne uzavretá predchádzajúca relácia karty (karta bola vytiahnutá predtým, než boli na karte uložené všetky relevantné dáta). Túto udalosť sa spustí len kartou vodiča alebo dielne.

9.7 ***„Prekročenie rýchlosti“***

065 Táto udalosť sa spustí pri každom prekročení.

9.8 ***„Prerušenie napájania“***

066 Táto udalosť sa spustí, pokiaľ záznamové zariadenie nie je v režime kalibrácie, v prípade akéhokoľvek viac než 200 milisekúnd trvajúceho prerušenia napájania snímača pohybu a/alebo jednotky vozidla. Prah prerušenia určí výrobca. Pokles dodávky prúdu počas štartovania motora vozidla, nesmie spustiť túto udalosť.

9.9 ***„Pohybová dátová chyba“***

067 Táto udalosť sa spustí v prípade prerušenia normálneho dátového toku medzi snímačom pohybu a jednotkou vozidla a/alebo v prípade chyby v integrite alebo autenticity dát, počas výmeny medzi snímačom pohybu a jednotkou vozidla.

9.10 ***„Pokus o narušenie bezpečnosti“***

068 Táto udalosť sa spustí, pokiaľ záznamové zariadenie nie je v režime kalibrácie, pri akejkoľvek inej udalosti ovplyvňujúcej bezpečnosť snímača pohybu a/alebo jednotky vozidla, špecifikovanej v rámci všeobecných bezpečnostných cieľov týchto komponentov.

9.11 ***„Chybná funkcia karty“***

069 Táto porucha sa spustí, keď počas prevádzky dôjde k chybnej funkcii tachografovej karty.

9.12 ***„Záznamové zariadenie“***

070 Táto porucha sa spustí, pokiaľ záznamové zariadenie nie je v režime kalibrácie, pri ktorejkoľvek z týchto porúch:

– vnútorná porucha jednotky vozidla,

– porucha tlačiarne,

– porucha displeja,

– porucha sťahovania,

– porucha snímača.

10. **Zabudované skúšky a automatické skúšky**

071 Záznamové zariadenie musí automaticky zistiť poruchy pomocou automatických a zabudovaných skúšok podľa tejto tabuľky:

Skúšobná podskupina	Automatická skúška	Zabudovaná skúška
Software		Integrita
Dátová pamäť	Prístup	Prístup, integrita dát
Rozhranie karty	Prístup	Prístup
Klávesnica		Manuálna kontrola
Tlačiareň	(ponecháva sa výrobcovi)	Výpis
Displej		Vizuálna kontrola
Sťahovanie (vykonávané len počas sťahovania)	Správna činnosť	
Snímač	Správna činnosť	Správna činnosť

11. **Čítanie z dátovej pamäti**

072 Záznamovo zariadenie musí umožniť čítanie dát uložených v jeho dátovej pamäti.

12**. Zaznamenávanie a uloženie v dátovej pamäti**

Na účely tohto odseku,

– „365 dní“ je definovaných ako 365 kalendárnych dní priemernej činnosti vodiča v jednom vozidle. Priemerná činnosť za deň vo vozidle je definovaná ako minimálne šesť vodičov alebo druhých vodičov, šesť cyklov vloženia a vybratia karty a 256 zmien činnosti. „365 dní“ preto zahŕňa minimálne 2 190 (druhých) vodičov, 2190 vložení a vybratí karty a 93 440 zmien činnosti,

– časy sa zaznamenávajú s presnosťou jednej minúty, pokiaľ nie je špecifikované inak,

– hodnoty počítadla kilometrov sa zaznamenávajú s presnosťou jedného kilometra,

– rýchlosti sa zaznamenávajú s presnosťou 1 km/h.

073 Dáta ukladané do dátovej pamäti nesmú byť ovplyvnené prerušením vonkajšieho napájania po dobu minimálne dvanástich mesiacov v podmienkach typového schválenia.

074 Záznamové zariadenie musí byť schopné implicitne a explicitne zaznamenávať a ukladať vo svoje pamäti toto:

12.1 ***Identifikačné dáta zariadenia***

12.1.1 *Identifikačné dáta jednotky vozidla*

075 Záznamové zariadenie musí byť schopné uchovávať vo svojej dátovej pamäti tieto údaje:

– meno výrobcu,

– adresa výrobcu,

– číslo časti,

– sériové číslo,

– číslo softwarovej verzie,

– dátum inštalácie softwarovej verzie,

– dátum výroby,

– schvaľovacie číslo.

076 Identifikačné dáta jednotky vozidla sú zaznamenané a natrvalo uchovávané výrobcom jednotky vozidla, s výnimkou dát vzťahujúcich sa k softwaru a schvaľovacieho čísla, ktoré sa môžu zmeniť v prípade aktualizácie softwaru.

12.1.2 *Identifikačné dáta snímača pohybu*

077 Snímač pohybu musí byť schopný uložiť vo svojej pamäti tieto identifikačné dáta:

– meno výrobcu,

– číslo časti,

– sériové číslo,

– schvaľovacie číslo,

– identifikátor vloženého bezpečnostného komponentu (napr. číslo časti vnútorného čipu/procesora),

– identifikátor systému prevádzky (napr. číslo verzie softwaru).

078 Identifikačné dáta snímača pohybu sú zaznamenané a natrvalo uložené výrobcom snímača pohybu.

079 Jednotka vozidla musí byť schopná do svojej pamäti uložiť tieto aktuálne spárené identifikačné dáta snímača pohybu:

– sériové číslo,

– schvaľovacie číslo,

– prvý spárený dátum.

12.2 ***Bezpečnostné prvky***

080 Záznamové zariadenie musí byť schopné uložiť tieto bezpečnostné prvky:

– európsky verejný kľúč,

– osvedčenie členského štátu,

– osvedčenie zariadenia,

– súkromný kľúč zariadenia.

Bezpečnostné prvky záznamového zariadenia vkladá do zariadenia výrobca jednotky vozidla.

12.3 ***Dáta o vložení a vybratí karty vodiča***

081 Pri každom cykle vloženia a vybratia karty vodiča alebo dielenskej karty z a do zariadenia, záznamové zariadenie zaznamená a uloží vo svojej dátovej pamäti:

– priezvisko a meno(á) držiteľa karty uložené na karte,

– číslo karty, vydávajúci členský štát a dátum skončenia platnosti uložený na karte,

– dátum a čas vloženia,

– stav kilometrov pri vložení karty,

– slot, do ktorého je karta vložená,

– dátum a čas vybratia,

– stav kilometrov pri vybratí karty,

– nasledovné informácie o predchádzajúcom vozidle, ktoré vodič použil, uložené na karte:

  – registračné číslo vozidla a členský štát registrácie,

  – dátum a čas vybratia karty,

– značka udávajúca, či pri vložení karty držiteľ karty manuálne zapísal alebo nezapísal činnosti.

082 Dátová pamäť musí byť schopná uchovať tieto dáta aspoň 365 dní.

083 Keď je kapacita pamäte vyčerpaná, najstaršie dáta sa prepíšu novými dátami.

12.4 ***Dáta o činnosti vodiča***

084 Záznamové zariadenie zaznamená a uloží vo svojej dátovej pamäti vždy keď dôjde k zmene činnosti vodiča a/alebo druhého vodiča, a/alebo keď dôjde k zmene stavu vedenia vozidla, a/alebo keď je vložená alebo vybratá karta vodiča alebo dielenská karta:

– stav vedenia vozidla (POSÁDKA, JEDEN VODIČ),

– slot (VODIČ, DRUHÝ VODIČ),

– stav karty v príslušnom slote (VLOŽENÁ, NEVLOŽENÁ) (pozri poznámku),

– činnosť (VEDENIE, POHOTOVOSŤ, PRÁCA, PRESTÁVKA/ODPOČINOK),

– dátum a čas zmeny.

Poznámka: VLOŽENÁ znamená, že je v drážke vložená platná karta vodiča alebo dielenská karta. NEVLOŽENÁ naopak znamená, že v slote nie je vložená žiadna platná karta vodiča alebo dielenská karta).

Poznámka: Dáta o činnosti zapísané manuálne vodičom sa nezaznamenajú v dátovej pamäti.

085 Dátová pamäť musí byť schopná uchovať dáta o činnosti vodiča aspoň 365 dní.

086 Keď je kapacita pamäte vyčerpaná, najstaršie dáta sa prepíšu novými dátami.

12.5 ***Miesta, kde denný pracovný čas začína a/alebo končí***

087 Záznamové zariadenie musí byť schopné zaznamenať a uložiť vo svojej dátovej pamäti vždy keď druhý(vodič) vloží miesto, kde denný pracovný čas začína a/alebo končí:

– prípadne číslo karty (druhého) vodiča a členský štát, ktorý ju vydal,

– dátum a čas zápisu (alebo dátum/čas vzťahujúci sa k zápisu, ak je zápis urobený počas postupu manuálneho zápisu),

– typ zápisu (začiatok alebo koniec, podmienky zápisu),

– zapísaný štát alebo región,

– stav kilometrov.

088 Dátová pamäť musí byť schopná uchovať dáta týkajúce sa času začiatku a/alebo konca denného pracovného času aspoň 365 dní (za predpokladu, že jeden vodič zapíše denne dva záznamy).

089 Keď je kapacita pamäte vyčerpaná, najstaršie dáta sa prepíšu novými dátami.

12.6 ***Dáta o stave kilometrov***

090 Záznamové zariadenie musí byť schopné každý kalendárny deň o polnoci zaznamenať vo svojej dátovej pamäti stav kilometrov vozidla a zodpovedajúci dátum.

091 Dátová pamäť musí byť schopná uchovať polnočné stavy kilometrov aspoň 365 dní.

092 Keď je kapacita pamäte vyčerpaná, najstaršie dáta sa prepíšu novými dátami.

12.7 ***Podrobné dáta o rýchlosti***

093 Záznamové zariadenie musí byť schopné zaznamenať a uložiť vo svojej dátovej pamäti okamžitú rýchlosť vozidla a zodpovedajúci dátum a čas v každej sekunde posledných 24 hodín, v priebehu ktorých sa vozidlo pohybuje.

12.8 ***Dáta o udalostiach***

Na účely tohto pododseku sa čas musí zaznamenať s presnosťou jednej sekundy.

094 Záznamové zariadenie musí byť schopné zaznamenať a uložiť vo svojej dátovej pamäti tieto dáta zodpovedajúce každej udalosti zistenej podľa nasledovných pravidiel uloženia:

Udalosť	Pravidlá uloženia	Dáta zaznamenané podľa udalosti
Sporná karta	– 10 najnovších udalostí	– dátum a čas začiatku udalosti, – dátum a čas skončenia udalosti, – typ karty, číslo a členský štát, ktorý vydal obe karty, predstavujúce spor.
Vedenie vozidla bez príslušnej karty	– najdlhšia udalosť za každých 10 posledných dní výskytu, päť najdlhších udalostí za – posledných 365 dní. –	– dátum a čas začiatku udalosti, – dátum a čas skončenia udalosti, – typ karty, číslo a členský štát, ktorý vydal kartu vloženú na začiatku a/ /alebo konci udalosti, – počet podobných udalostí v tomto dni. –

Vloženie karty počas vedenia vozidla	– posledná udalosť za každých 10 posledných dní výskytu.	– dátum a čas udalosti, – typ karty, číslo a členský štát, ktorý vydal kartu, – počet podobných udalostí v tomto dni.
Nesprávne uzavretá posledná relácia karty	– 10 najnovších udalostí	– dátum a čas vloženia karty, – typ karty, číslo a členský štát, ktorý vydal kartu, – dáta poslednej relácie čítané z karty – dátum a čas vloženia karty – registračné číslo vozidla a členský štát registrácie.
Prekročenie rýchlosti(1)	– najvážnejšia udalosť za každých posledných 10 dní výskytu (t. j. jedna z najvyšších priemerných rýchlostí), – päť najvážnejších udalostí za posledných 365 dní, – prvá udalosť, ktorá sa vyskytla po poslednej kalibrácii	– dátum a čas začiatku udalosti, – dátum a čas skončenia udalosti, – maximálna rýchlosť nameraná počas udalosti, – aritmeticky priemerná rýchlosť name–raná počas udalosti, – typ karty, číslo a vydávajúci členský štát vodiča (ak je to použiteľné), – počet podobných udalostí v tomto dni.
Prerušenie napájania(2)	– najdlhšia udalosť za každých 10 posledných dní výskytu, – päť najdlhších udalostí za posledných 365 dní.	– dátum a čas začiatku udalosti, – dátum a čas skončenia udalosti, – typ karty, číslo a členský štát, ktorý vydal kartu vloženú na začiatku a/ /alebo konci udalosti, – počet podobných udalostí v tomto dni.
Porucha snímača pohybu	– najdlhšia udalosť za každých 10 posledných dní výskytu, – päť najdlhších udalostí za posledných 365 dní.	– dátum a čas začiatku udalosti, – dátum a čas skončenia udalosti, – typ karty, číslo a členský štát, ktorý vydal kartu vloženú na začiatku a/ /alebo konci udalosti, – počet podobných udalostí v tomto dni.
Pokus o narušenie bezpečnosti	– 10 najnovších udalostí za každý typ udalosti	– dátum a čas začiatku udalosti, – dátum a čas skončenia udalosti (ak je relevantný), – typ karty, číslo a členský štát, ktorý vydal kartu vloženú na začiatku a/ /alebo konci udalosti, – typ udalosti.

095 (1) Záznamové zariadenie musí zaznamenať a uložiť vo svoje pamäti:

– dátum a čas poslednej KONTROLY PREKROČENIA RÝCHLOSTI,

– dátum a čas prvého prekročenia rýchlosti po tejto KONTROLE PREKROČENIA RÝCHLOSTI,

– počet udalostí prekročenia rýchlosti od poslednej KONTROLY PREKROČENIA RÝCHLOSTI.

(2) Tieto dáta sa môžu zaznamenať len po obnovení napájania, časy môžu byť známe s presnosťou jednej minúty.

12.9 ***Dáta o poruchách***

Na účely tohto pododseku sa čas musí zaznamenať s presnosťou jednej sekundy.

096 Záznamové zariadenie sa musí pokúsiť zaznamenať a uložiť vo svojej dátovej pamäti tieto dáta za každú poruchu zistenú podľa nasledovných pravidiel uloženia:

Porucha	Pravidlá uloženia	Dáta zaznamenané podľa poruchy
Porucha karty	– 10 najnovších porúch karty vodiča	– dátum a čas začiatku poruchy, – dátum a čas skončenia poruchy, – typ karty, číslo a členský štát, ktorý vydal kartu
Poruchy záznamového zariadenia	– 10 najnovších porúch karty za každý typ poruchy – prvá porucha po posled–nej kalibrácii.	– dátum a čas začiatku poruchy, – dátum a čas skončenia poruchy, – typ poruchy, – typ karty, číslo a členský štát, ktorý vydal kartu vloženú na začiatku a/alebo konci poruchy.

12.10 ***Kalibračné dáta***

097 Záznamové zariadenie musí zaznamenať a uložiť vo svojej dátovej pamäti dáta vzťahujúce sa k:

– známym kalibračným parametrom v okamihu aktivácie,

– jeho skutočne prvej kalibrácii po aktivovaní,

– jeho prvej kalibrácii v súčasnom vozidle (identifikovanom jeho identifikačným číslom),

– piatim najnovším kalibráciám (ak sa niekoľko kalibrácií uskutočnilo v priebehu jedného kalendárneho dňa, uložia sa len posledné v tomto dni).

098 Za každú z týchto kalibrácií sa zaznamenajú nasledovné dáta:

– účel kalibrácie (aktivácia, prvá inštalácia, inštalácia, pravidelná prehliadka),

– názov dielne a adresa,

– číslo dielenskej karty, štát, ktorý kartu vydal a dátum skončenia platnosti karty,

– identifikácia vozidla,

– aktualizované alebo potvrdené parametre: w, k, l, rozmer pneumatika, nastavenia zariadenia obmedzujúceho rýchlosť, počítadlo kilometrov (staré a nové hodnoty), dátum a čas (staré a nové hodnoty).

099 Snímač pohybu musí zaznamenať a uložiť vo svojej dátovej pamäti nasledovné inštalačné dáta senzora pohybu:

– prvé spárovanie s jednotkou vozidla (dátum, čas, schvaľovacie číslo jednotky vozidla, sériové číslo jednotky vozidla),

– posledné spárovanie s jednotkou vozidla (dátum, čas, schvaľovacie číslo jednotky vozidla, sériové číslo jednotky vozidla).

12.11 ***Dáta nastavenia času***

100 Záznamové zariadenie musí zaznamenať a uložiť vo svojej dátovej pamäti dáta vzťahujúce sa k:

– najnovšiemu nastaveniu času,

– posledným piatim najväčším nastaveniam času od poslednej kalibrácie,

vykonané v režime kalibrácie mimo rámca pravidelnej kalibrácie (definícia (f)).

101 Za každé z týchto nastavení času sa zaznamenajú nasledovné dáta:

– dátum čas, staré hodnoty,

– dátum čas, nové hodnoty – názov dielne a adresa,

– číslo dielenskej karty, štát, ktorý kartu vydal a dátum skončenia platnosti karty.

12.12 ***Dáta o kontrolnej činnosti***

102 Záznamové zariadenie musí zaznamenať a uložiť vo svojej dátovej pamäti nasledovné dáta vzťahujúce sa k 20 najnovším kontrolných činnostiam:

– dátum a čas kontroly,

– číslo kontrolnej karty a štát, ktorý kartu vydal,

– druh kontroly (zobrazovanie a/alebo tlač a/alebo stiahnutie z jednotky vozidla a/alebo stiahnutie z karty).

103 Pri sťahovaní dát sa musia zaznamenať aj dátumy najstarších a najnovších stiahnutých dní.

12.13 ***Dáta o podnikovom blokovaní***

104 Záznamové zariadenie musí zaznamenať a uložiť vo svojej dátovej pamäti nasledovné dáta vzťahujúce sa k 20 najnovším podnikovým blokovaniam:

– dátum a čas zablokovania,

– dátum a čas odblokovania,

– číslo podnikovej karty a štát, ktorý kartu vydal,

– meno a adresa podniku.

12.14 ***Dáta o činnosti sťahovania***

105 Záznamové zariadenie musí zaznamenať a uložiť vo svojej dátovej pamäti nasledovné dáta vzťahujúce sa k poslednému stiahnutiu dátovej pamäti na vonkajšie médium, počas režimu podniku alebo kalibrácie:

– dátum a čas stiahnutia,

– číslo podnikovej alebo dielenskej karty a štát, ktorý kartu vydal,

– meno a adresa podniku alebo dielne.

12.15 ***Dáta o špecifických podmienkach***

105a Záznamové zariadenie musí zaznamenať a uložiť vo svojej dátovej pamäti nasledovné dáta vzťahujúce sa k špecifickým podmienkam:

– dátum a čas zápisu,

– typ špecifických podmienok.

105b Dátová pamäť musí byť schopná uchovať dáta o špecifických podmienkach aspoň 365 dní (s predpokladom, že v priemere je denne otvorená a uzatvorená jedna podmienka). Keď je kapacita pamäte vyčerpaná, najstaršie dáta sa prepíšu novými dátami.

13. **Čítanie z tachografovej karty**

106 Záznamové zariadenie musí byť schopné odčítať z tachografovej karty dáta potrebné na

– identifikáciu typu karty, držiteľa karty, predtým použitého vozidla, dátum a čas posledného vytiahnutia karty a činnosť zvolenú v tomto čase,

– kontrolu správneho uzatvorenia poslednej relácie karty,

– výpočet nepretržitého času vedenia vozidla vodičom, kumulovaný čas prestávok a kumulované časy vedenia za predchádzajúci a súčasný týždeň,

– tlač požadovaných výstupov vzťahujúcich sa k dátam zaznamenaným na karte vodiča,

– stiahnutie karty vodiča na vonkajšie médium.

107 V prípade chyby čítania sa musí záznamové zariadenie pokúsiť znovu, a maximálne trikrát, o rovnaký príkaz na čítanie, a potom ak je znovu neúspešný, musí vyhlásiť kartu za chybnú a neplatnú.

14. **Zaznamenávanie a uloženie na tachografovej karte**

108 Záznamové zariadenie nastaví „dáta relácie karty“ na karte vodiča alebo na dielenskej karte hneď po vložení karty.

109 Záznamové zariadenie aktualizuje dáta uložené na platnej karte vodiča, dielenskej a/alebo kontrolnej karte, so všetkými nevyhnutnými dátami relevantnými pre časový úsek, počas ktorého je karta vložená a ktoré sa vzťahujú k držiteľovi karty. Dáta uložené na týchto kartách sú špecifikované v kapitole IV.

109a Záznamové zariadenie aktualizuje dáta o činnosti vodiča a o mieste (špecifikované v kapitole IV, odsekoch 5.2.5 a 5.2.6) uložené na platnej karte vodiča a/alebo dielenskej karte, s dátami o činnosti a mieste zapísanými manuálne držiteľom karty.

110 Aktualizácia dát tachografovej karty prebieha tak, že keď je to potrebné a berúc do úvahy skutočnú kapacitu pamäte, najstaršie dáta sa nahradia najnovšími dátami.

111 V prípade chybného zápisu sa záznamové zariadenie pokúsi znovu, a maximálne trikrát, o rovnaký príkaz zápisu, a potom ak je znovu neúspešný, musí vyhlásiť kartu za chybnú a neplatnú.

112 Pred vytiahnutím karty vodiča a potom čo boli uložené všetky relevantné dáta na karte, záznamové zariadenie znovu nastaví dáta týkajúce sa relácie karty.

15. **Zobrazovanie**

113 Displej musí obsahovať aspoň 20 znakov.

114 Minimálna výška znaku je 5 mm a šírka 3,5 mm.

114a Displej podporuje množinu znakov Latin 1 a Grécke znaky definované ISO 8859 časti 1 a 7, špecifikované v doplnku 1, kapitole 4 „Množina znakov“. Displej môže používať zjednodušené piktogramy (napr. znaky so znamienkami môžu byť zobrazované bez znamienok, alebo malé písmená môžu byť zobrazované ako veľké písmená).

115 Displej musí byť vybavený neoslňujúcim osvetlením

116 Údaje musia byť viditeľné zvonka záznamového zariadenia.

117 Záznamové zariadenie musí byť schopné zobraziť:

– štandardné dáta,

– dáta týkajúce sa výstrah,

– dáta týkajúce sa prístupu k menu,

– ostatné dáta požadované užívateľom.

Záznamové zariadenie môže zobraziť doplňujúce informácie za predpokladu, že sa dajú zreteľne odlíšiť od predchádzajúcich informácií.

118 Displej záznamového zariadenia používa piktogramy alebo kombinácie piktogramov uvedené v doplnku 3. Doplňujúce piktogramy alebo kombinácie piktogramov môže displej zobrazovať za predpokladu, že sa dajú zreteľne odlíšiť od prv uvedených piktogramov.

119 Displej musí byť vždy zapnutý (ON), keď sa vozidlo pohybuje.

120 Záznamové zariadenie môže obsahovať manuálne alebo automatické zariadenie, ktoré vypne displej (OFF), keď sa vozidlo nepohybuje.

Zobrazovací formát je špecifikovaný v doplnku 5.

15.1 ***Štandardný displej***

121 Keď nemusia byť zobrazené žiadne iné informácie, záznamové zariadenie musí štandardne zobraziť toto:

- miestny čas (ako výsledok času UTC + posun nastavený vodičom),
- režim činnosti,
- súčasná činnosť vodiča a súčasná činnosť druhého vodiča,
- informácie vzťahujúce sa k vodičovi:
  - ak jeho súčasná činnosť je VEDENIE, jeho aktuálny nepretržitý čas vedenia vozidla a jeho aktuálny kumulovaný čas prestávok,
  - ak jeho súčasná činnosť nie je VEDENIE, aktuálny čas trvania tejto inej činnosti (od času, kedy bola zvolená) a jeho aktuálny kumulovaný čas prestávok,
  - informácie vzťahujúce sa k druhému vodičovi:
    - aktuálny čas trvania jeho činnosti (od času, kedy bola zvolená).

122 Zobrazenie dát vzťahujúcich sa ku každému vodičovi musí byť jasné, zreteľné a jednoznačné. V prípade, keď sa informácie vzťahujúce sa k vodičovi a druhému vodičovi nemôžu zobraziť súčasne, záznamové zariadenie musí štandardne zobraziť informácie vzťahujúce sa k vodičovi a umožniť užívateľovi zobrazenie informácií vzťahujúcich sa k druhému vodičovi.

123 V prípade, že šírka displeja neumožňuje zobraziť štandardne prevádzkový režim, záznamové zariadenie pri zmene režimu stručne zobrazí nový režim činnosti.

124 Záznamové zariadenie pri vložení karty stručne zobrazí meno držiteľa karty.

124a Keď je otvorená podmienka „ZÁZNAMOVÉ ZARIADENIE SA NEVYŽADUJE“, potom štandardné zobrazenie musí s využitím piktogramu ukázať, že je podmienka otvorená a pripúšťa sa, že súčasne sa nemôže zobraziť aktuálna činnosť vodiča).

15.2 ***Výstražný displej***

125 Záznamové zariadenie musí zobraziť výstražné informácie najmä s použitím piktogramov uvedených v doplnku 3, doplnené v prípade potreby dodatočnými numerickými kódovanými informáciami. Textový popis výstrahy môže byť dodatočne zobrazený v jazyku, ktorý si vodič vyberie.

15.3 **Prístup k menu**

126 Záznamové zariadenie musí poskytovať nevyhnutné príkazy pomocou vhodnej štruktúry menu.

15.4 **Iné displeje**

127 Na požiadanie musí byť možno selektívne zobraziť:

- UTC dátum a čas,
- prevádzkový režim (ak nie je štandardne zobrazený),
- nepretržitý čas vedenia a kumulovaný čas prestávok vodiča,
- nepretržitý čas vedenia a kumulovaný čas prestávok druhého vodiča,

– kumulovaný čas vedenia vodiča za predchádzajúci a prebiehajúci týždeň,

– kumulovaný čas vedenia druhého vodiča za predchádzajúci a prebiehajúci týždeň,

– obsah šiestich výtlačkov v rovnakom formáte v akom sú samotné výtlačky.

128 Zobrazenie obsahu výpisu musí byť sekvenčné, riadok po riadku. Ak je šírka displeja menšia než 24 znakov, užívateľ musí pomocou vhodných prostriedkov dostať úplné informácie (niekoľko riadkov, pretáčanie ...). Tlačené riadky pre ručne písané informácie sa nemusia zobraziť.

16. **Tlač**

129 Záznamové zariadenie musí byť schopné vytlačiť informácie zo svojej dátovej pamäti a/alebo z tachografovej karty v súlade so šiestimi nasledovnými výpismi:

– denný výpis činnosti vodiča z karty,

– denný výpis činnosti vodiča z jednotky vozidla,

– výpis udalostí a porúch z karty,

– výpis udalostí a porúch z jednotky vozidla,

– výpis technických dát,

– výpis prekročenia rýchlosti.

Podrobné formáty a obsah týchto výpisov sú uvedené v doplnku 4.

Na konci výpisov môžu byť poskytnuté doplňujúce výpisy.

Záznamové zariadenie môže poskytnúť aj doplňujúce výpisy za predpokladu, že sa dajú zreteľne odlíšiť od šiestich predchádzajúcich výpisov.

130 „Denný výpis činnosti vodiča z karty“ a „výpis udalostí a porúch z karty“ je k dispozícii len vtedy, keď je karta vodiča alebo dielenská karta vložená do záznamového zariadenia. Záznamové zariadenie aktualizuje dáta uložené na relevantnej karte pred začiatkom tlače.

131 Aby sa vyhotovil „denný výpis činnosti vodiča z karty“ alebo „výpis udalostí a porúch z karty“ záznamové zariadenie:

– buď automaticky vyberie kartu vodiča alebo dielenskú kartu, ak je vložená len jedna z týchto kariet,

– alebo umožní príkaz, ktorým sa zvolí zdroj karty alebo sa zvolí karta v slote vodiča, ak sú do záznamového zariadenia vložené dve tieto karty.

132 Tlačiareň musí byť schopná tlačiť 24 znakov v každom riadku.

133 Minimálna výška znaku je 2,1 mm a šírka 1,5 mm.

133a Tlač podporuje množinu znakov Latin 1 a Grécke znaky definované ISO 8859 časti 1 a 7, špecifikované v doplnku 1, kapitole 4 „Množina znakov“.

134 Tlačiarne musia byť konštruované tak, aby výpisy boli k dispozícii s úrovňou rozlíšenia, ktorá zabráni nejednoznačnosti pri ich čítaní.

135 Rozmery výpisov a údaje nesmú vykazovať žiadne zmeny v normálnych podmienkach vlhkosti (10 až 90%) a teploty.

136 Papier používaný v záznamovom zariadení musí mať relevantnú značku typového schválenia a údaj o type(och) záznamového zariadenia, v ktorom sa môže používať. V normálnych podmienkach uloženia vzhľadom na intenzitu svetla, vlhkosť a teplotu musia zostať výpisy aspoň jeden rok zreteľne čitateľné a identifikovateľné.

137 Musí byť možný doplniť tieto dokumenty rukou písanými poznámkami, ako je podpis vodiča.

138 Ak počas tlače nastane udalosť „v zásobníku nie je papier“, po doplnení papiera naštartuje záznamové zariadenie tlač od začiatku výpisu, alebo pokračuje v tlači, pričom poskytne jednoznačný odkaz na predchádzajúcu vytlačenú časť.

17. **Výstraha**

139 Záznamové zariadenie musí varovať vodiča keď zistí akúkoľvek udalosť a/alebo poruchu.

140 Výstraha pri udalosti „prerušené napájania“ sa môže oneskoriť, kým nie je znovu obnovené napájanie.

141 Záznamové zariadenie musí varovať vodiča 15 minút pred prekročením nepretržitého času vedenia vozidla 4 hodiny a 30 minút a pri prekročení tohto času.

142 Výstrahy musia byť vizuálne. Môžu byť k dispozícii aj zvukové výstrahy za predpokladu, že sú doplnkom k vizuálnym výstrahám.

143 Vizuálne výstrahy musia byť jednoznačne rozpoznateľné zo strany užívateľa, musia byť umiestnené v zornom poli vodiča a musia byť zreteľne čitateľné cez deň ako aj v noci.

144 Vizuálne výstrahy môžu byť zabudované do záznamového zariadenia a/alebo inštalované v určitej vzdialenosti od zariadenia.

145 V tomto druhom prípade musia byť označené symbolom „T“ a musia byť žlté alebo oranžové.

146 Čas trvania výstrah musí byť aspoň 30 sekúnd, kým ich užívateľ určitým kľúčom alebo príkazom záznamového zariadenia nepotvrdí. Toto potvrdenie nesmie vymazať príčina výstrahy uvedená v nasledujúcom odseku.

147 Príčina výstrahy sa musí zobraziť na záznamovom zariadení a zostať viditeľná až kým ju užívateľ nepotvrdí špecifickým kľúčom alebo príkazom záznamového zariadenia.

148 Môžu byť k dispozícii doplnkové výstrahy, pokiaľ si ich vodič nemôže zameniť s predchádzajúcimi výstrahami.

18. **Sťahovanie dát do vonkajších médií**

149 Záznamové zariadenie musí byť na požiadanie schopné stiahnuť dáta zo svojej dátovej pamäti alebo z karty vodiča, do vonkajšieho pamäťového média cez kalibračný/sťahovací konektor. Záznamové zariadenie aktualizuje dáta uložené na príslušnej karte pred začiatkom sťahovania.

150 Okrem toho a nepovinne môže záznamové zariadenie v ktoromkoľvek prevádzkovom režime sťahovať dáta cez iný konektor pre podnik, overený prostredníctvom tohto konektora. V takom prípade platia pre toto sťahovanie prístupové práva k dátam v režime podniku.

151 Sťahovanie nesmie zmeniť alebo vymazať žiadne uložené dáta.

Elektrické rozhranie konektora kalibrácie/sťahovania je špecifikované v doplnku 6.

Protokoly sťahovania sú špecifikované v doplnku 7.

19. **Výstupné dáta pre doplnkové vonkajšie zariadenia**

152 Ak záznamové zariadenie neobsahuje žiadne funkcie na zobrazovanie rýchlosti a/alebo stavu kilometrov, musí poskytovať výstupný(é) signál(y) aby umožnilo zobrazenie rýchlosti vozidla (rýchlomer) a/alebo celkovej vzdialenosti prejdenej vozidlom (počítadlo kilometrov).

153 Jednotka vozidla musí byť schopná poskytnúť nasledovné výstupné dáta využívajúc vhodné vyhradené sériové spojenie nezávislé na ľubovolnom CAN zbernicovom spojení (ISO 11898 Cestné vozidlá – Výmena digitálnych informácií – Controller Area Network (CAN) pre vysokorýchlostné prenosy), aby umožnila ich spracovanie inými elektronickými jednotkami inštalovanými vo vozidle:

– aktuálny UTC dátum a čas,

– rýchlosť vozidla,

– celková vzdialenosť prejdená vozidlom (počítadlo kilometrov),

– súčasná zvolená činnosť vodiča a druhého vodiča,

– informácie o tom, či je v súčasnosti vložená tachografová karta v slote vodiča a slote druhého vodiča a (a prípadne) informácie o zodpovedajúcej identifikácii karty (číslo karty a členský štát, ktorý ju vydal).

Tento minimálny zoznam môže byť doplnený inými výstupnými dátami.

Keď je zapaľovanie vozidla zapnuté (ON), tieto dáta sa musia nepretržite vysielať. Keď je zapaľovanie vozidla vypnuté (OFF), minimálne zmena činnosti vodiča alebo druhého vodiča a/alebo vloženie alebo vytiahnutie tachografovej karty musí vyvolať zodpovedajúci výstup dát. V prípade, že bol výstup dát zadržaný pri vypnutom zapaľovaní, tieto dáta sa musia byť k dispozícii po opätovnom zapnutí motora vozidla.

20. **Kalibrácia**

154 Kalibračná funkcia musí umožniť:

– automatické spárovanie snímača pohybu s jednotkou vozidla,

– digitálne prispôsobenie konštanty záznamového zariadenia (k) k charakteristickému koeficientu vozidla (w) (vozidlá s dvoma alebo viacerými nápravovými prevodovými pomermi musia byť vybavené prepínacím zariadením, ktorým sa automaticky tieto rôzne pomery zladia s pomerom, na ktorý bolo zariadenie na vozidle prispôsobené),

– nastavenie (bez obmedzenia) aktuálneho času,

– nastavenie aktuálneho stavu kilometrov,

– aktualizácia identifikačných dát senzora pohybu, ktoré sú uložené v dátovej pamäti;

– aktualizácia alebo potvrdenie ostatných parametrov, ktoré pozná záznamové zariadenie: identifikácia vozidla, w, l, rozmer pneumatík a prípadne nastavenie zariadenia obmedzujúceho rýchlosť.

155 Spárovanie snímača pohybu s jednotkou vozidla pozostáva minimálne z:

– aktualizácie inštalačných dát snímača pohybu uchovávaných snímačom pohybu (ak je to potrebné),

– kopírovania nevyhnutných identifikačných dát snímača pohybu zo snímača pohybu do dátovej pamäti jednotky vozidla.

156 Kalibračná funkcia musí byť schopná zaviesť nevyhnutné dáta cez kalibračný/sťahovací konektor v súlade s kalibračným protokolom definovaným v doplnku 8. Kalibračná funkcia môže zavádzať nevyhnutné dáta aj cez iné konektory.

21. **Nastavenie času**

157 Funkcia nastavenia času musí umožniť v minimálne sedem dňových intervaloch nastavovanie aktuálneho času maximálne po jednej minúte.

158 Funkcia nastavenia času musí v režime kalibrácie umožniť nastavenie aktuálneho času bez obmedzenia.

22. **Výkonnostné charakteristiky**

159 Jednotka vozidla musí byť plne funkčná v rozsahu teplôt od – 20 °C do 70 °C a snímač pohybu v rozsahu teplôt od – 40 °C do 135 °C. Obsah dátovej pamäti sa musí uchovať pri teplote do – 40 °C.

160 Záznamové zariadenie musí byť plne prevádzkyschopné v rozsahu od 10% do 90% vlhkosti.

161 Záznamové zariadenie musí byť chránené proti prepätiu, zmene polarity jeho napájania a skratom.

162 Záznamové zariadenie musí zodpovedať požiadavkám smernice Komisie 95/54/ES z 31. októbra 1995[(1)], ktorou sa technickému pokroku prispôsobuje smernica Rady 72/245/EHS[(2)] týkajúca sa elektromagnetickej kompatibility, a musí byť chránené proti elektrostatickým výbojom a prechodným javom.

23. **Materiály**

[(1)] Ú. v. ES L 266, 8. 11. 1995, s. 1.
[(2)] Ú. v. ES L 152, 6. 7. 1972, s 15.

163 Všetky konštrukčné časti záznamového zariadenia musia byť vyrobené z materiálov s dostatočnou stabilitou a mechanickou pevnosťou a so stálymi elektrickými a magnetickými charakteristikami.

164 Na zaručenie normálnych podmienok prevádzky musia byť všetky vnútorné časti zariadenia chránené proti vlhkosti a prachu.

165 Jednotka vozidla musí spĺňať stupeň ochrany IP 40 a snímač pohybu musí spĺňať stupeň ochrany IP 64 podľa normy IEC 529.

166 Záznamové zariadenie musí zodpovedať aplikovateľným technickým požiadavkám týkajúcim sa ergonomického dizajnu.

167 Záznamové zariadenie musí byť chránené proti náhodnému poškodeniu.

24. **Označovanie**

168 Ak záznamové zariadenie zobrazuje stav kilometrov a rýchlosť, na displeji sa musia objaviť tieto údaje:

– vedľa čísla udávajúceho vzdialenosť, jednotka merania vzdialenosti, označená skratkou „km“,

– vedľa čísla udávajúceho rýchlosť, skratku „km/h“.

Záznamové zariadenie sa môže prepnúť tak, aby zobrazovalo rýchlosť v míľach za hodinu, v tomto prípade sa ako jednotka merania rýchlosti zobrazí skratka „mph“.

169 Na každý samostatný komponent záznamového zariadenia musí byť pripevnený štítok s týmito údajmi:

– meno a adresa výrobcu zariadenia,

– číslo časti zariadenia a rok výroby,

– sériové číslo zariadenia,

– schvaľovacia značka typu zariadenia.

170 Ak nie je dostatok miesta pre vyššie uvedené údaje, popisný štítok musí udávať aspoň: meno alebo logo výrobcu a číslo časti zariadenia.

IV. KONŠTRUKČNÉ A FUNKČNÉ POŽIADAVKY NA TACHOGRAFOVÉ KARTY

1. **Viditeľné dáta**

Predná strana bude obsahovať:

171 slová „Karta vodiča“ alebo „Kontrolná karta“ alebo „Dielenská karta“ alebo „Podniková karta“, vytlačené veľkými písmenami v úradnom jazyku alebo jazykoch členského štátu, ktorý kartu vydal, podľa typu karty;

172 rovnaké slová v ostatných úradných jazykoch spoločenstva, vytlačené tak aby tvorili pozadie karty:

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 ΟΔΗΟΥ	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 názov členského štátu, ktorý kartu vydal (nepovinné):

174 rozlišujúci znak členského štátu, ktorý kartu vydal, vytlačený v negatíve v modrom obdĺžniku a obklopený 12 žltými hviezdičkami. Rozlišujúci znak je nasledovný:

B Belgicko
DK Dánsko
D Nemecko
GR Grécko
E Španielsko
F Francúzsko
IRL Írsko
I Taliansko
L Luxembursko
NL Holandsko
A Rakúsko
P Portugalsko
FIN Fínsko
S Švédsko
UK Spojené kráľovstvo;

175 informácie špecifické pre vydanú kartu, očíslované takto:

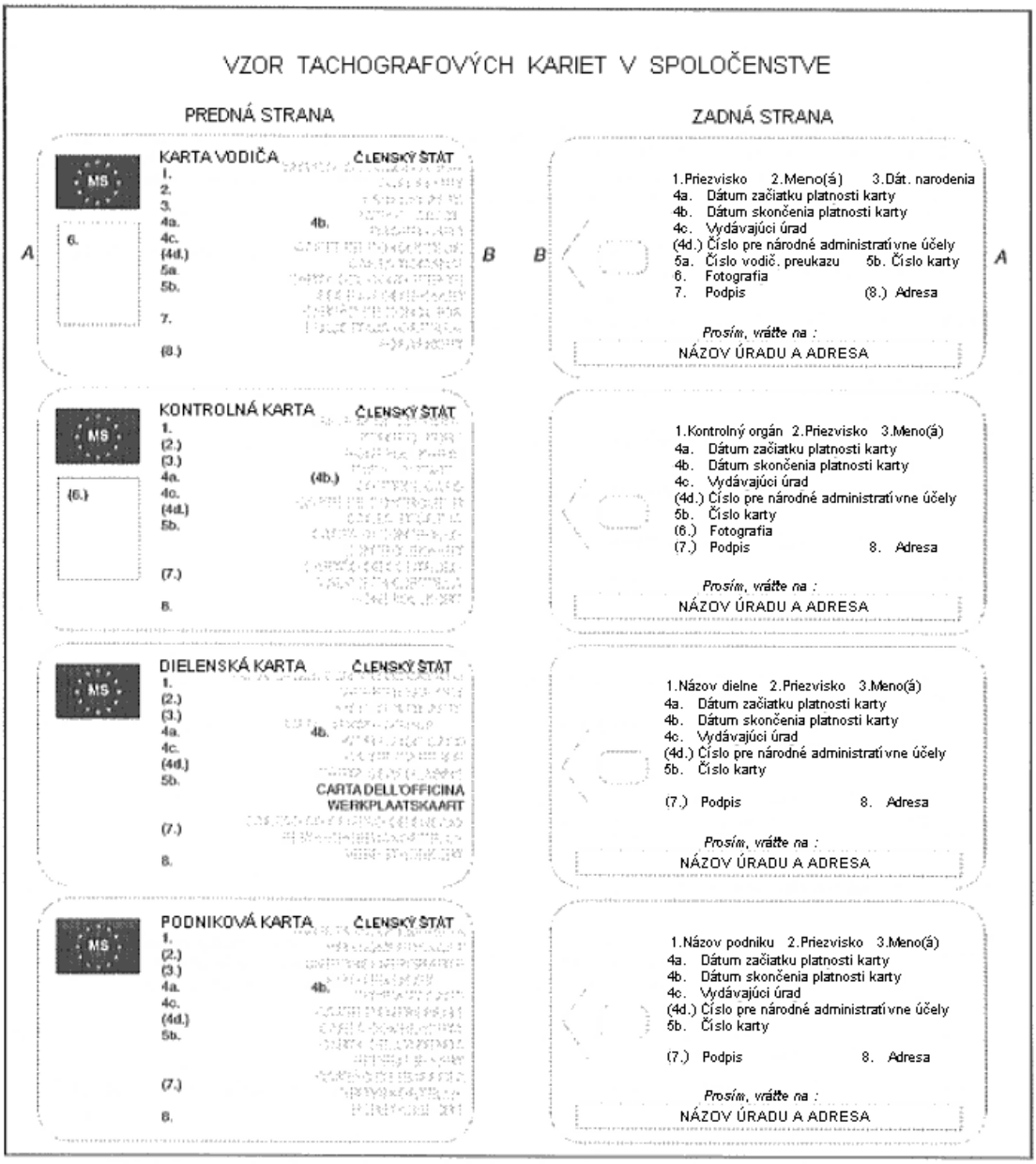
	Karta vodiča	Kontrolná karta	Podniková alebo dielenská karta
1.	Priezvisko vodiča	Názov kontrolného orgánu	Názov podniku alebo dielne
2.	Meno(á) vodiča	(Prípadne) priezvisko kontrolóra	(Prípadne) priezvisko držiteľa karty
3.	Dátum narodenia vodiča	(Prípadne) meno kontrolóra	(Prípadne) meno držiteľa karty
4.(a)	Dátum začiatku platnosti karty		
(b)	Dátum skončenia platnosti karty (ak je)		
(c)	Názov vydávajúceho úradu (môže byť vytlačené na strane 2)		
(d)	Číslo iné než je uvedené v bode 5, pre administratívne účely (nepovinné)		
5.(a)	Číslo vodičského preukazu (k dátumu vydania karty vodiča)		
5.(b)	Číslo karty		
6.	Fotografia vodiča	Fotografia kontrolóra (nepovinná)	–
7.	Podpis vodiča	Podpis držiteľa (nepovinný)	
8.	Bydlisko alebo poštová adresa držiteľa (nepovinné)	Poštová adresa kontrolného orgánu	Poštová adresa podniku alebo dielne

176 forma písania dátumu je „dd/mm/rrrr“ alebo „dd.mm.rrrr“ (deň, mesiac, rok);

zadná strana bude obsahovať:

177 vysvetlenie k očíslovaným údajom na prednej strane karty;

178 s výslovným písomným súhlasom držiteľa môžu byť doplnené aj informácie, ktoré sa netýkajú administratívnych záležitosti súvisiacich s kartou; taký doplnok nebude meniť žiadnym spôsobom používanie modelu ako tachografovej karty.



179 Tachografové karty musia byť vytlačené s týmito farbami pozadia:

- karta vodiča: biela,
- kontrolná karta: modrá,
- dielenská karta: červená,
- podniková karta: žltá.

180 Tachografové karty musia mať aspoň tieto ochranné prvky proti falšovaniu alebo neoprávneným zásahom:

- bezpečnostné vzorkované pozadie s gilošovými vzorkami a dúhovou tlačou,
- v mieste fotografie prekrývanie bezpečnostného vzorkovaného pozadia a fotografie,
- aspoň jeden dvojfarebný mikrotlačový prúžok.

181 Po konzultácii s komisiou môžu členské štáty doplniť farby alebo označenia ako sú symboly členského štátu a bezpečnostné prvky bez toho, aby to malo dopad na ostatné ustanovenia tejto prílohy.

2. **Bezpečnosť**

Cieľom bezpečnosti systému je ochrana integrity a autenticity dát vymieňaných medzi kartami a záznamovým zariadením, ochrana integrity a autenticity dát sťahovaných z kariet, umožnenie určitých písomných operácií na karte len pre záznamové zariadenie, vylúčenie akejkoľvek možnosti falšovania dát uložených na kartách, zabránenie neoprávnenému zásahu a zistenie každého pokusu tohto druhu.

182 Na zaručenie bezpečnosti systému musia tachografové karty spĺňať bezpečnostné požiadavky definované vo všeobecných bezpečnostných cieľoch tachografových kariet (doplnok 10).

183 Tachografové karty musia byť čitateľné inými zariadeniami ako sú napríklad osobné počítače.

3. **Normy**

184 Tachografové karty musia zodpovedať týmto normám:

- ISO/IEC 7810 Identifikačné karty – Fyzikálne vlastnosti,
- ISO/IEC 7816 Identifikačné karty – Integrované obvody s kontaktmi:
  - Časť 1: Fyzikálne vlastnosti,
  - Časť 2: Rozmery a umiestnenie kontaktov,
  - Časť 3: Elektronické signály a protokoly procesu
  - Časť 4: Medziodborové príkazy pre výmenu
  - Časť 8: Medziodborové príkazy vzťahujúce sa k bezpečnosti,
- ISO/IEC 10373 Identifikačné karty – Skúšobný postup.

4. **Environmentálne a elektrické špecifikácie**

185 Tachografové karty musia byť riadne funkčné za všetkých klimatických podmienok, ktoré sú zvyčajne na území spoločenstva a minimálne v rozsahu teplôt od – 25 °C do + 70 °C s príležitostnou špičkou do + 85 °C, „príležitostná“ znamená maximálne 4 hodiny a maximálne 100 krát v priebehu životnosti karty.

186 Tachografové karty musia byť riadne funkčné v rozsahu od 10% do 90% vlhkosti.

187 Tachografové karty musia byť riadne funkčné počas piatich rokov, ak sa používajú v súlade so špecifikáciami pre prostredie a elektrickými špecifikáciami.

188 Počas prevádzky musia tachografové karty zodpovedať smernici Rady 95/54/ES z 31. októbra 1995[(1)], týkajúcej sa elektromagnetickej kompatibility, a musia byť chránené proti elektrostatickým výbojom.

[(1)] Ú. v. ES L 266, 8. 11. 1995, s. 1.

5. **Uloženie dát**

Na účely tohto odseku:

– sa časy zaznamenávajú s presnosťou jednej minúty, pokiaľ nie je špecifikované inak,

– stav kilometrov sa zaznamenáva s presnosťou jedného kilometra,

– rýchlosť sa zaznamenáva s presnosťou 1 km/h.

Funkcie tachografových kariet, príkazy a logické štruktúry, ktoré slúžia na splnenie požiadaviek na uloženie dát, sú špecifikované v doplnku 2.

189 Tento odsek špecifikuje minimálnu kapacitu pamäte súborov dát rôzneho použitia. Tachografové karty musia byť schopné poskytnúť záznamovému zariadeniu údaje o skutočnej kapacite pamäte týchto súborov dát.

Akékoľvek doplnkové dáta, ktoré môžu byť uložené na tachografových kartách a sú určené na iné použitie, na ktoré môžu karty ešte slúžiť, musia byť uložené v súlade so smernicou 95/46/ES z 24. októbra 1995[(2)] o ochrane jednotlivcov z hľadiska spracovávania osobných údajov a o voľnom pohybe takých údajov.

5.1 ***Identifikačné a bezpečnostné dáta karty***

5.1.1 *Identifikácia použitia*

190 Tachografové karty musia byť schopné uložiť nasledovné identifikačné dáta týkajúce sa použitia:

– identifikácia použitia tachometra,

– typ identifikácie tachografovej karty.

5.1.2 *Identifikácia čipu*

191 Tachografové karty musia byť schopné uložiť nasledovné identifikačné dáta integrovaného obvodu (IO):

– sériové číslo IO,

– výrobné údaje IO.

5.1.3 *Identifikácia IO karty*

192 Tachografové karty musia byť schopné uložiť nasledovné identifikačné dáta inteligentnej karty:

– sériové číslo karty (vrátane výrobných údajov),

– číslo typového schválenia karty,

– identifikácia personalizácie karty (ID),

– zhotoviteľ ID,

– identifikátor IO.

5.1.4 *Bezpečnostné prvky*

193 Tachografové karty musia byť schopné uložiť nasledovné dáta bezpečnostných prvkov:

– európsky verejný kľúč,

– osvedčenie členského štátu,

– osvedčenie karty,

– súkromný kľúč karty.

5.2 **Karta vodiča**

5.2.1 *Identifikácia karty*

[(2)] Ú. v. ES L 281, 23. 11. 1995, s. 31.

194 Karta vodiča musí byť schopná uložiť nasledovné identifikačné dáta karty:

– číslo karty,

– členský štát, ktorý kartu vydal, dátum vydania,

– dátum začiatku platnosti karty, dátum skončenia platnosti karty.

5.2.2 *Identifikácia držiteľa karty*

195 Karta vodiča musí byť schopná uložiť nasledovné identifikačné dáta držiteľa karty:

– priezvisko držiteľa,

– meno(á) držiteľa,

– dátum narodenia,

– uprednostnený jazyk.

5.2.3 *Informácie o vodičskom preukaze*

196 Karta vodiča musí byť schopná uložiť nasledovné identifikačné dáta vodičského preukazu:

– členský štát, ktorý preukaz vydal, názov vydávajúceho úradu,

– číslo vodičského preukazu (k dátumu vydania karty).

5.2.4 *Dáta o použitom vozidle*

197 Karta vodiča musí byť schopná uložiť za každý kalendárny deň používania karty a za každý časový úsek používania daného vozidla v uvedenom dni (časový úsek používania zahŕňa všetky po sebe idúce cykly vloženia/vytiahnutia karty vo vozidle, z hľadiska tejto karty), tieto dáta:

– dátum a čas prvého použitia vozidla (t. j. prvé vloženie karty v tomto časovom úseku použitia vozidla, alebo 00.00 ak časový úsek používania v uvedenom čase trvá,

– stav kilometrov v uvedenom čase,

– dátum a čas posledného použitia vozidla (t. j. posledné vytiahnutie karty v tomto časovom úseku použitia vozidla, alebo 23.59 ak časový úsek používania v uvedenom čase trvá,

– stav kilometrov v uvedenom čase,

– registračné číslo vozidla a členský štát registrácie vozidla.

198 Karta vodiča musí byť schopná uložiť aspoň 84 takých záznamov.

5.2.5 *Dáta o činnosti vodiča*

199 Karta vodiča musí byť schopná uložiť za každý kalendárny deň používania karty alebo deň, za ktorý vodič manuálne zapísal činnosti, tieto dáta:

– dátum,

– stav dennej prítomnosti (zvýšený o jeden za každý z týchto kalendárnych dní),

– celková vzdialenosť prejdená vozidlom vedeným vodičom počas tohto dňa,

– stav vodiča o 00.00 hod.,

– vždy keď vodič zmenil činnosť a/alebo zmenil stav vedenia vozidla a/alebo vložil alebo vybral svoju kartu:

  – stav vedenia vozidla (POSÁDKA, JEDEN VODIČ)

  – slot (VODIČ, DRUHÝ VODIČ),

  – stav karty (VLOŽENÁ, NEVLOŽENÁ),

  – činnosť (VEDENIE, POHOTOVOSŤ, PRÁCA, PRESTÁVKA/ODPOČINOK),

  – čas zmeny.

200 Pamäť karty vodiča musí byť schopná uchovať dáta o činnosti vodiča aspoň 28 dní (priemerná činnosť vodiča je definovaná ako 93 zmien činnosti za deň).

201 Dáta uvedené v požiadavke 197 a 199 musia byť uložené spôsobom, ktorý umožní vyvolať činnosti v poradí v akom nastali, dokonca aj v prípade časového prekrývania.

5.2.6 *Miesta, kde denný pracovný čas začína a/alebo končí*

202 Karta vodiča musí byť schopná uložiť nasledovné dáta týkajúce sa miest, kde denný pracovný čas začína a/alebo končí, zapísané vodičom:

– dátum a čas zápisu (alebo dátum/čas vzťahujúci sa k zápisu, ak sa zápis vykoná počas postupu manuálneho zápisu),

– typ zápisu (začiatok alebo koniec, podmienky zápisu),

– zapísaný štát alebo región,

– stav kilometrov.

203 Pamäť karty vodiča musí byť schopná uchovať aspoň 42 párov takých záznamov.

5.2.7 *Dáta o udalostiach*

Na účely tohto pododseku sa čas ukladá s presnosťou jednej sekundy

204 Karta vodiča musí byť schopná uložiť dáta týkajúce sa nasledovných udalostí zistených záznamovým zariadením, zatiaľčo bola karta vložená:

– časové prekrývanie (keď je táto karta príčinou udalosti),

– vloženie karty pri vedení vozidla (keď je táto karta predmetom udalosti),

– nesprávne uzavretie poslednej relácie karty (keď je táto karta predmetom udalosti),

– prerušenie napájania,

– porucha snímača pohybu,

– pokus o narušenie bezpečnosti.

205 Karta vodiča musí byť schopná za tieto udalostí uložiť nasledovné dáta:

– kód udalosti,

– dátum a čas začiatku udalosti (alebo vloženia karty, ak udalosť v uvedenom čase trvala),

– dátum a čas skončenia udalosti (alebo vybratia karty, ak udalosť v uvedenom čase trvala),

– registračné číslo vozidla a členský štát registrácie vozidla, v ktorom udalosť nastala.

Poznámka: pre udalosť „časové prekrývanie“:

– dátum a čas začiatku udalosti musí zodpovedať dátumu a času vytiahnutia karty z prechádzajúceho vozidla,

– dátum a čas skončenia udalosti musí zodpovedať dátumu a času vloženia karty do súčasného vozidla,

– dáta o vozidle musia zodpovedať súčasnému vozidlu, ktoré bolo príčinou vzniku udalosti.

Poznámka pre udalosť „nesprávne uzavretie poslednej relácie karty“:

– dátum a čas začiatku udalosti musí zodpovedať dátumu a času vloženia karty pri nesprávne uzavretej poslednej relácii karty,

– dátum a čas skončenia udalosti musí zodpovedať dátumu a času vloženia karty pri relácii, počas ktorej bola zistená udalosť (súčasná relácia),

– dáta o vozidle musia zodpovedať vozidlu, v ktorom bola nesprávne uzavretá relácia.

206 Karta vodiča musí byť schopná uložiť dáta za posledných šesť najnovších udalostí každého typu (t. j. 36 udalostí).

5.2.8 *Dáta o poruchách*

Na účely tohto pododseku sa čas zaznamená s presnosťou jednej sekundy.

207 Karta vodiča musí byť schopná uložiť dáta týkajúce sa nasledovných porúch zistených záznamovým zariadením, zatiaľčo bola karta vložená:

– porucha karty (keď je táto karta predmetom udalosti),

– porucha záznamového zariadenia.

208 Karta vodiča musí byť schopná za tieto poruchy uložiť nasledovné dáta:

– kód poruchy,

– dátum a čas začiatku poruchy (alebo vloženia karty, ak porucha v uvedenom čase trvala),

– dátum a čas skončenia poruchy (alebo vybratia karty, ak udalosť v uvedenom čase trvala),

– registračné číslo vozidla a členský štát registrácie vozidla, v ktorom porucha nastala.

209 Karta vodiča musí byť schopná uložiť dáta za dvanásť posledných porúch každého typu (t. j. 24 porúch).

5.2.9 *Dáta o kontrolnej činnosti*

210 Karta vodiča musí byť schopná uložiť nasledovné dáta týkajúce sa kontrolných činností:

– dátum a čas kontroly,

– číslo kontrolnej karty a členský štát, ktorý kartu vydal,

– druh kontroly (zobrazovanie a/alebo tlač a/alebo sťahovanie z jednotky vozidla a/alebo sťahovanie z karty (pozri poznámku)),

– časový úsek sťahovania, v prípade sťahovania,

– registračné číslo vozidla a členský štát registrácie vozidla, v ktorom sa kontrola uskutočnila.

Poznámka: z bezpečnostných požiadaviek vyplýva, že sťahovanie z karty sa zaznamená len vtedy, keď sa vykonáva cez záznamové zariadenie.

211 Karta vodiča musí byť schopná uchovať jeden taký záznam.

5.2.10 *Dáta o relácii karty*

212 Karta vodiča musí byť schopná uložiť dáta týkajúce sa vozidla, v ktorom bola otvorená prebiehajúca relácia:

– dátum a čas otvorenej relácie (t. j. vloženie karty) s presnosťou jednej sekundy,

– registračné číslo vozidla a členský štát registrácie.

5.2.11 *Dáta o špecifických podmienkach*

212a Karta vodiča musí byť schopná uložiť nasledovné dáta týkajúce sa špecifických podmienok zapísaných, zatiaľčo bola karta vložená (bez ohľadu na slot):

– dátum a čas zápisu,

– druh špecifickej podmienky.

212b Karta vodiča musí byť schopná uchovať 56 takých záznamov.

5.3 ***Dielenská karta***

5.3.1 *Bezpečnostné prvky*

213 Dielenská karta musí byť schopná uložiť osobné identifikačné číslo (PIN kód).

214 Dielenská karta musí byť schopná uložiť kryptografické kľúče potrebné na spárovanie senzorov pohybu s jednotkami vozidla.

5.3.2 *Identifikácia karty*

215 Dielenská karta musí byť schopná uložiť nasledovné identifikačné dáta karty:

– číslo karty,

– členský štát, ktorý kartu vydal, názov vydávajúceho úradu, dátum vydania,

– dátum začiatku platnosti karty, dátum skončenia platnosti karty.

5.3.3 *Identifikácia držiteľa karty*

216 Dielenská karta musí byť schopná uložiť nasledovné identifikačné dáta držiteľa karty:

– názov dielne,

– adresa dielne,

– priezvisko držiteľa,

– meno(á) držiteľa,

– uprednostnený jazyk.

5.3.4 *Dáta o použitom vozidle*

217 Dielenská karta musí byť schopná uložiť záznamy dát o použitom vozidle rovnako ako karta vodiča.

218 Dielenská karta musí byť schopná uložiť aspoň štyri také záznamy.

5.3.5 *Dáta o činnosti vodiča*

219 Dielenská karta musí byť schopná uložiť dáta o činnosti vodiča rovnako ako karta vodiča.

220 Dielenská karta musí byť schopná uchovať dáta o činnosti vodiča za aspoň jeden deň priemernej činnosti vodiča.

5.3.6 *Dáta o začiatku a/alebo konci denného pracovného času*

221 Dielenská karta musí byť schopná uložiť záznamy dát o začiatku a/alebo konci denného pracovného času rovnako ako karta vodiča.

222 Dielenská karta musí byť schopná uchovať aspoň tri páry takých záznamov.

5.3.7 *Dáta o udalostiach a poruchách*

223 Dielenská karta musí byť schopná uložiť záznamy dát o udalostiach a poruchách rovnako ako karta vodiča.

224 Dielenská karta musí byť schopná uložiť dáta za tri najnovšie udalosti každého typu (t. j. 18 udalostí) a za šesť najnovších porúch každého typu (t. j. 12 porúch).

5.3.8 *Dáta o kontrolnej činnosti*

225 Dielenská karta musí byť schopná uložiť záznamy dát o kontrolnej činnosti rovnako ako karta vodiča.

5.3.9 *Dáta o kalibrácii a časovom nastavení*

226 Dielenská karta musí byť schopná uchovať záznamy o kalibrácii a/alebo časovom nastavení, ktoré sa vykonávali zatiaľčo bola karta vložená v záznamovom zariadení.

227 Každý záznam o kalibrácii musí byť schopný uchovať tieto dáta:

– účel kalibrácie (aktivácia, prvá inštalácia, inštalácia, pravidelná prehliadka),

– identifikácia vozidla,

– aktualizované alebo potvrdené parametre (w, k, l, rozmer pneumatika, nastavenia zariadenia obmedzujúceho rýchlosť, počítadlo kilometrov (nové a staré hodnoty), dátum a čas (nové a staré hodnoty),

– identifikácia záznamového zariadenia (číslo časti jednotky vozidla, sériové číslo jednotky vozidla, sériové číslo snímača pohybu).

228 Dielenská karta musí byť schopná uložiť aspoň 88 takých záznamov.

229 Dielenská karta musí mať počítadlo udávajúce celkový počet kalibrácií vykonaných s kartou.

230 Dielenská karta musí mať počítadlo udávajúce počet kalibrácií vykonaných od jej posledného stiahnutia.

5.3.10 Dáta o špecifických podmienkach

230a Dielenská karta musí byť schopná uložiť dáta relevantné pre špecifické podmienky rovnako ako karta vodiča.

5.4 ***Kontrolná karta***

5.4.1 *Identifikácia karty*

231 Kontrolná karta musí byť schopná uložiť nasledovné identifikačné dáta karty:

– číslo karty,

– členský štát, ktorý kartu vydal, názov vydávajúceho úradu, dátum vydania,

– dátum začiatku platnosti karty, dátum skončenia platnosti karty (ak je).

5.4.2 *Identifikácia držiteľa karty*

232 Kontrolná karta musí byť schopná uložiť nasledovné identifikačné dáta držiteľa karty:

– názov kontrolného orgánu,

– adresa kontrolného orgánu,

– priezvisko držiteľa,

– meno(á) držiteľa,

– uprednostnený jazyk.

5.4.3 *Dáta o kontrolnej činnosti*

233 Kontrolná karta musí byť schopná uložiť tieto dáta o kontrolnej činnosti:

– dátum a čas kontroly,

– druh kontroly (zobrazovanie a/alebo tlač a/alebo stiahnutie z jednotky vozidla a/alebo stiahnutie z karty).

– (prípadne) časový úsek sťahovania,

– registračné číslo vozidla a členský štát registrácie kontrolovaného vozidla,

– číslo karty a členský štát, ktorý vydal kontrolovanú kartu vodiča.

234 Kontrolná karta musí byť schopná uchovať aspoň 230 takých záznamov.

5.5 ***Podniková karta***

5.5.1 *Identifikácia karty*

235 Podniková karta musí byť schopná uložiť nasledovné identifikačné dáta karty:

– číslo karty,

– členský štát, ktorý kartu vydal, názov vydávajúceho úradu, dátum vydania,

– dátum začiatku platnosti karty, dátum skončenia platnosti karty (ak je).

5.5.2 *Identifikácia držiteľa karty*

236 Podniková karta musí byť schopná uložiť nasledovné identifikačné dáta držiteľa karty:

– názov podniku,

– adresa podniku.

5.5.3 *Dáta o činnosti podniku*

237 Podniková karta musí byť schopná uložiť nasledovné dáta o činnosti podniku:

– dátum a čas činnosti,

– druh činnosti (zablokovanie a/alebo odblokovanie jednotky vozidla, a/alebo stiahnutie z jednotky vozidla a/alebo stiahnutie z karty),

– (prípadne) časový úsek sťahovania,

– registračné číslo vozidla a registrujúci úrad členského štátu,

– číslo karty a členský štát, ktorý vydal kartu (v prípade sťahovania).

238 Podniková karta musí byť schopná uchovať aspoň 230 takých záznamov.

V. MONTÁŽ ZÁZNAMOVÉHO ZARIADENIA

1. **Montáž**

239 Nové záznamové zariadenie sa musí dodať v neaktivovanom stave montérom alebo výrobcovi vozidla, so všetkými kalibračnými parametrami uvedenými v kapitole III(20), nastavenými na vhodné a platné štandardné hodnoty. Ak nie je uvedená žiadna vhodná hodnota, písmenový parameter sa nastaví na reťazec „?“ a numerický parameter na „0“.

240 Pred svojou aktiváciou musí záznamové zariadenie zaručiť prístup ku kalibračnej funkcii dokonca aj vtedy, keď nie je v režime kalibrácie.

241 Pred svojou aktiváciou nesmie záznamové zariadenie ani zaznamenávať ale ani ukladať dáta uvedené v bodoch III.12.3 až III.12.9 a III.12.12 až III.12.14 vrátane.

242 Počas montáže musí výrobca vozidla predbežne nastaviť všetky známe parametre.

243 Výrobcovia vozidla alebo montéri musia aktivovať záznamové zariadenie predtým, než opustí prevádzkové priestory, v ktorých sa montáž uskutočnila.

244 Aktivácia záznamového zariadenia sa spustí automaticky pri prvom vložení dielenskej karty do jedného z jej rozhraní.

245 Špecifické párovacie operácie medzi snímačom pohybu a jednotkou vozidla sa uskutočnia automaticky pred alebo počas aktivácie.

246 Po svojej aktivácii záznamové zariadenie zabezpečuje všetky funkcie a prístupové práva k dátam.

247 Záznamové a ukladacie funkcie záznamového zariadenia musia byť po jeho aktivácii úplne prevádzkyschopné.

248 Po montáži nasleduje kalibrácia. Prvá kalibrácia bude obsahovať zápis registračného čísla vozidla a uskutoční sa do dvoch týždňov po montáži alebo po pridelení registračného čísla vozidla podľa toho, čo sa udeje neskôr.

248a Záznamové zariadenie musí byť umiestnené vo vozidle tak, aby umožňovalo vodičovi z jeho sedadla prístup k potrebným funkciám.

2. **Montážny štítok**

249 Potom čo bolo záznamové zariadenie skontrolované pri montáži, pripevní sa na záznamové zariadenie alebo vedľa neho montážny štítok, ktorý musí byť zreteľne viditeľný a ľahko prístupný. Po každom zásahu vykonanom schváleným montérom alebo dielňou sa namiesto predchádzajúceho štítku pripevní nový.

250 Na montážnom štítku musia byť aspoň tieto údaje:

– meno, adresa alebo obchodný názov schváleného montéra alebo dielne,

– charakteristický koeficient vozidla vo forme „W = ... imp/km“,

– konštanta záznamového zariadenia vo forme „k = ... imp/km“,

– účinný obvod pneumatík kolies vo forme „l = ... mm“,

– rozmer pneumatík,

– dátum, kedy bol stanovený charakteristický koeficient vozidla a meraný účinný obvod pneumatík kolies,

– identifikačné číslo vozidla.

3. **Zaplombovanie**

251 Musia sa zaplombovať nasledovné časti:

– každý spoj, ktorý ak je rozpojený, by mohol spôsobiť nezistiteľnú zmenu alebo nezistiteľnú stratu dát,

– montážny štítok, pokiaľ nie je pripevnený tak, že sa nedá odstrániť bez toho, aby označenia, ktoré je na ňom.

252 Uvedené plomby sa môžu odstrániť:

– v prípade núdze,

– v prípade montáže, nastavenia alebo opravy zariadenia obmedzujúceho rýchlosť alebo akéhokoľvek iného zariadenia, ktoré prispeje k zvýšeniu cestnej bezpečnosti za predpokladu, že záznamové zaradenie naďalej funguje spoľahlivo a správne a že ho opäť zaplombuje schválený montér alebo dielňa (v súlade s kapitolou VI) ihneď po namontovaní zariadenia obmedzujúceho rýchlosť alebo akéhokoľvek iného zariadenia, ktoré prispeje k zvýšeniu cestnej bezpečnosti, alebo do siedmich dní v ostatných prípadoch.

253 Pri každom porušení týchto plomb sa musí vyhotoviť písomné vyhlásenie s uvedením dôvodov takého porušenia a musí sa poskytnúť príslušnému orgánu.

VI. SKÚŠKY, KONTROLY A OPRAVY

Okolnosti, za ktorých môžu byť plomby odstránené, ako je uvedené v článku 12.5 nariadenia (EHS) č. 3821/85, naposledy zmeneného a doplneného nariadením (EHS) č. 2135/98, sú definované v kapitole V(3) tejto prílohy.

1. **Schvaľovanie montérov a dielní**

Členské štáty budú schvaľovať, pravidelne kontrolovať a certifikovať subjekty, ktoré vykonávajú:

– montáž,

– skúšky,

– kontroly,

– opravy.

V rámci článku 12 ods. 1 tohto nariadenia bude dielenská karta vydaná len montérom a/alebo dielňam schváleným a riadne oprávneným na vykonávanie aktivácie a/alebo kalibrácie záznamového zariadenia podľa tejto prílohy:

– ktorí(é) nemajú nárok na podnikovú kartu.

– a ktorých odborné činnosti nepredstavujú možné ohrozenie celkovej bezpečnosti systému podľa doplnku 10.

2. **Kontrola nových alebo opravených prístrojov**

254 Každé jednotlivé zariadenie bez ohľadu na to, či je nové alebo opravené, sa musí skontrolovať z hľadiska jeho správnej činnosti a presnosti jeho čítaných hodnôt a záznamov, v rámci limitov stanovených v kapitole III.2.1 a III.2.2, pomocou plombovania v súlade s kapitolou V.3 a kalibrácie.

3. **Kontrola montáže**

255 Po namontovaní na vozidlo musí celková montáž (vrátane záznamového zariadenia) spĺňať ustanovenia týkajúce sa maximálnych tolerancií stanovených v kapitole III.2.1 a III.2.2.

4. **Pravidelné prehliadky**

256 Pravidelné prehliadky zariadenia namontovaného vo vozidle sa uskutočnia po každej oprave alebo po každej zmene charakteristického koeficientu vozidla, alebo účinného obvodu pneumatík alebo potom, čo sa UTC čas zariadenia odchyľuje o viac než 20 minút od správneho času, alebo keď bolo zmenené registračné číslo vozidla a aspoň raz za dva roky (24 mesiacov) od poslednej kontroly.

257 Tieto prehliadky zahŕňajú nasledovné kontroly:

– správne fungovanie záznamového zariadenia, vrátane funkcie ukladania dát na tachografových kartách,

– dodržanie ustanovení kapitoly III.2.1 a III.2.2 o maximálnych toleranciách po montáži,

– prítomnosť typovej schvaľovacej značky na zariadení,

– prítomnosť montážneho štítku,

– neporušenosť plomb na zariadení a na ostatných montážnych častiach,

– rozmer pneumatík a skutočný účinný obvod pneumatík kolies.

258 Súčasťou týchto prehliadok musí byť aj kalibrácia.

5. **Meranie chýb**

259 Meranie chýb pri montáži a počas používania sa vykonáva podľa nasledovných podmienok, ktoré sa považujú za časť štandardných skúšobných podmienok:

– nenaložené vozidlo v normálnom pohotovostnom stave;

– tlak pneumatík v súlade s pokynmi výrobcu,

– opotrebenie pneumatík v rámci limitov povolených vnútroštátnymi právnymi predpismi,

– pohyb vozidla:

  – vozidlo sa pohybuje dopredu hnacou silou svojho motora po priamke na rovnom podklade rýchlosťou 50 ± 5 km/h. Meracia vzdialenosť musí byť minimálne 1 000 m.

– za predpokladu, že sú porovnateľne presné, môžu sa na skúšku použiť alternatívne metódy ako je napríklad skúšobné zariadenie.

6. **Opravy**

260 Dielne musia byť schopné stiahnuť dáta zo záznamového zariadenia, aby mohli dáta odovzdať príslušnému dopravnému podniku.

261 Schválené dielne vydajú dopravným podnikom osvedčenie o nemožnosti stiahnutia dát, keď porucha záznamového zariadenia bráni tomu, aby boli predchádzajúce zaznamenané dáta stiahnuté, dokonca aj po oprave v tejto dielni. Dielne musia minimálne jeden rok uchovávať kópiu každého vydaného osvedčenia.

VII.VYDANIE KARTY

Postup vydávania kariet zavedený členským štátom musí zodpovedať nasledovnému:

262 Číslo karty prvého vydania tachografovej karty žiadateľovi musí mať postupný index (ak je to aplikovateľné) ako aj index náhrady a index obnovy nastavený na „0“.

263 Čísla kariet všetkých tachografových kariet, ktoré nie sú vztiahnuté k osobe, vydaných jednému kontrolnému orgánu, jednej dielni alebo jednému dopravnému podniku, musia mať rovnakých prvých 13 číslic a musia mať rôzne poradové čísla.

264 Tachografová karta vydaná ako náhrada existujúcej tachografovej karty musí mať rovnaké číslo ako karta, ktorú nahrádza, no index náhrady sa zvýši o „1“ (v poradí 0, ..., 9, A, ..., Z).

265 Tachografová karta vydaná ako náhrada existujúcej tachografovej karty musí mať rovnaký dátum skončenia platnosti ako karta, ktorú nahrádza.

266 Tachografová karta vydaná ako obnova existujúcej tachografovej karty musí mať rovnaké číslo ako karta, ktorú obnovuje, pričom sa však index náhrady znova nastaví na „0“ a index obnovy sa zvýši o „1“ (v poradí 0, ..., 9, A, ..., Z).

267 Výmena existujúcej tachografovej karty za účelom zmeny administratívnych údajov, sa riadi pravidlami obnovy príslušného členského štátu, alebo pravidlami prvého vydania, ak bola vykonaná iným členským štátom.

268 Do rubriky „Priezvisko držiteľa karty“ u dielenskej alebo kontrolnej karty, ktorá nie je vztiahnutá na osobu, sa uvedie názov dielne alebo kontrolného orgánu.

VIII. TYPOVÉ SCHVÁLENIE ZÁZNAMOVÉHO ZARIADENIA A TACHOGRAFOVÝCH KARIET

1. **Všeobecné body**

Na účely tejto kapitoly slová „záznamové zariadenie“ znamenajú „záznamové zariadenie alebo jeho komponenty. Žiadne typové schválenie sa nevyžaduje pre spojovacie káble snímača pohybu a jednotky vozidla. Papier používaný záznamovým zariadením sa považuje za komponent záznamového zariadenia.

269 Záznamové zariadenie musí byť na schválenie dodané úplné so všetkými zabudovanými doplnkovými zariadeniami.

270 Typové schválenie záznamového zariadenia a tachografových kariet zahŕňa skúšky vzťahujúce sa k bezpečnosti, funkčné skúšky a skúšky interoperability. Kladné výsledky každého z týchto skúšok sú uvedené na príslušnom osvedčení.

271 Typovo schvaľovacie úrady členských štátov neudelia osvedčenie o typovom schválení v súlade s článkom 5 tohto nariadenia, pokiaľ nedostanú:

– bezpečnostné osvedčenie,

– funkčné osvedčenie,

– a osvedčenie o interoperabilite,

za záznamové zariadenie alebo tachografovú kartu, ktoré sú predmetom žiadosti o typové schválenie.

272 Každá zmena softwaru alebo hardwaru zariadenia alebo zmena vlastností materiálov použitých jeho výrobcom, predtým než sa použije, musí byť oznámená orgánu, ktorý udelil typové schválenie pre zariadenie. Tento orgán potvrdí výrobcovi rozšírenie typového schválenia, alebo môže požadovať aktualizáciu alebo potvrdenie príslušných funkčných, bezpečnostných osvedčení a/alebo osvedčení o interoperabilite.

273 Postupy modernizácie *na mieste* softwaru záznamového zariadenia musí schváliť orgán, ktorý udelil typového schválenie pre záznamové zariadenie. Modernizácia softwaru nesmie meniť ani vymazať žiadne dáta o činnosti vodiča uložené v záznamovom zariadení. Software sa môže modernizovať len na zodpovednosť výrobcu zariadenia.

2. **Bezpečnostné osvedčenie**

274 Bezpečnostné osvedčenie sa udelí v súlade s ustanoveniami doplnku 10 tejto prílohy.

3. **Funkčné osvedčenie**

275 Každý uchádzač o typové schválenie poskytne schvaľovaciemu úradu členského štátu všetky materiály a dokumentáciu, ktoré považuje tento úrad za potrebné.

276 Funkčné osvedčenie dostane výrobca len po úspešnom absolvovaní minimálne všetkých funkčných skúšok špecifikovaných v doplnku 9.

277 Typovo schvaľovací úrad udeľuje funkčné osvedčenie. Toto osvedčenie musí okrem mena užívateľa a identifikácie modelu obsahovať podrobný zoznam vykonaných skúšok a dosiahnutých výsledkov.

4. **Osvedčenie o interoperabilite**

278 Skúšky interoperability vykonáva len skúšobňa ktorá podlieha Európskej komisii a je pod jej zodpovednosťou.

279 Skúšobňa registruje žiadosti výrobcu o skúšky interoperability v poradí, v ktorom boli doručené.

280 Žiadosti sa oficiálne zaregistrujú len vtedy, keď skúšobňa má k dispozícii:

– úplný súbor materiálov a dokumentov potrebných na také skúšky interoperability,

– zodpovedajúce bezpečnostné osvedčenie,

– zodpovedajúce funkčné osvedčenie,

Dátum registrácie žiadosti sa oznámi výrobcovi.

281 Skúšobňa nevykoná žiadne skúšky interoperability pre záznamové zariadenie alebo tachografovú kartu, ktorým nebolo udelené bezpečnostné a funkčné osvedčenie.

282 Každý výrobca žiadajúci o vykonanie skúšok interoperability je povinný ponechať skúšobni poverenej vykonávaním týchto skúšok, úplný súbor materiálov a dokumentov, ktoré poskytol za účelom vykonania skúšok.

283 Skúšky interoperability sa v súlade s ustanoveniami odseku 5 doplnku 9 tejto prílohy, vykonajú vždy pre všetky typy záznamového zariadenia alebo tachografových kariet:

– ktoré majú ešte platné typové schválenia, alebo

– pre ktoré sa požaduje typové schválenie a ktoré majú platné osvedčenie o interoperabilite.

284 Osvedčenie o interoperabilite udelí skúšobňa výrobcovi len po všetkých úspešne absolvovaných skúškach interoperability.

285 Ak neboli skúšky interoperability úspešné s jedným alebo niekoľkými záznamovými zariadeniami alebo tachografovými kartami, podľa požiadavky 283, osvedčenie o interoperabilite sa nesmie vydať, kým žiadajúci výrobca nevykoná potrebné zmeny a neabsolvuje úspešne skúšky interoperability. Skúšobňa musí s pomocou výrobcu, ktorého sa táto chyba v interoperabilite týka, zistiť príčinu problému a musí sa pokúsiť pomôcť výrobcovi pri hľadaní technického riešenia. V prípade, že výrobca zmenil svoj výrobok, musí všetkým relevantným orgánom preukázať, že bezpečnostné a funkčné osvedčenia sú stále platné.

286 Osvedčenie o interoperabilite je platné šesť mesiacov. Odoberie sa na konci tohto obdobia, ak výrobca nedostal zodpovedajúce osvedčenie o typovom schválení. Osvedčenie o interoperabilite predloží výrobca typovému schvaľovaciemu úradu členského štátu, ktorý udelil funkčné osvedčenie.

287 Každý prvok, ktorý by mohol byť príčinou chyby v interoperabilite sa nesmie použiť na získanie prospechu alebo na získanie dominantného postavenia.

5. **Osvedčenie o typovom schválení**

288 Typovo schvaľovací úrad členského štátu môže udeliť osvedčenie o typovom schválení pokiaľ mu budú predložené tri požadované osvedčenia.

289 Kópiu osvedčenia o typovom schválení vyhotoví typovo schvaľovací úrad pre skúšobňu poverenú vykonávaním skúšok interoperability, v čase udelenia osvedčenia výrobcovi.

290 Skúšobňa príslušná na vykonávanie skúšok interoperability musí udržiavať webovú stránku, na ktorej bude aktualizovať zoznam modelov záznamových zariadení alebo tachografových kariet:

– za ktoré bola zaregistrovaná žiadosť na vykonanie skúšok interoperability,

– ktorým bolo udelené osvedčenie o interoperabilite (aj keď len predbežné),

– ktorým bolo udelené osvedčenia o typovom schválení.

6. **Výnimočný postup: prvé skúšky interoperability**

291 Do štyroch mesiacov potom, čo bola prvá sada záznamového zariadenia a tachografových kariet (karty vodiča, dielenské, kontrolné a podnikové karty) certifikovaná ako interoperabilná, každé udelené osvedčenie o interoperabilite (vrátane skutočne prvého) vzťahujúce sa k žiadostiam zaregistrovaným počas tohto obdobia, sa považuje za predbežné.

292 Ak na konci tohto obdobia sú všetky príslušné výrobky interoperabilné, všetky zodpovedajúce osvedčenia o interoperabilite sa stávajú definitívnymi.

293 Ak sa počas tohto obdobia zistia chyby v interoperabilite, skúšobňa poverená vykonávaním skúšok interoperability musí s pomocou všetkých príslušných výrobcov zistiť príčiny problému a vyzve ich aby vykonali nevyhnutné úpravy.

294 Ak na konci tohto obdobia pretrvávajú problémy z hľadiska interoperability, skúšobňa poverená vykonávaním skúšok interoperability, v spolupráci s príslušnými výrobcami a s typovo schvaľovacími úradmi, ktoré udelili zodpovedajúce funkčné osvedčenia, musí zistiť príčiny chýb v interoperabilite a určiť zmeny, ktoré musí vykonať každý príslušný výrobca. Hľadanie technických riešení môže trvať maximálne dva mesiace, po uplynutí ktorých, ak sa nenašlo žiadne spoločné riešenie, komisia po konzultácii so skúšobňou poverenou vykonávaním skúšok interoperability rozhodne o tom, ktoré zariadenie(a) a karta(y) dostanú definitívne osvedčenie o interoperabilite s uvedením dôvodov pre také rozhodnutie.

295 Každá žiadosť o vykonanie skúšok interoperability registrovaná skúšobňou od konca štvormesačného obdobia po udelení prvého predbežného osvedčenia o interoperabilite, do dátumu rozhodnutia komisie uvedeného v požiadavke 294, sa odloží do doby, kým nebudú vyriešené pôvodné problémy interoperability. Také žiadosti sa potom spracujú v poradí, v akom boli zaregistrované.

Doplnok 1

SLOVNÍK DÁT

OBSAH

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

2.69 MemberStatePublicKey
2.70 Name
2.71 NationAlpha
2.72 NationNumeric
2.73 NoOfCalibrationRecords
2.74 NoOfCalibrationSinceDonwload
2.75 NoOfCardPlaceRecords
2.76 NoOfCardVehicleRecords
2.77 NoOfCompanyActivityRecords
2.78 NoOfControlActivityRecords
2.79 NoOfEventsPerType
2.80 NoOfFaultsPerType
2.81 OdometerValueMidnight
2.82 OdometerShort
2.83 OverspeedNumber
2.84 PlaceRecord
2.85 PreviousVehicleInfo
2.86 PublicKey
2.87 RegionAlpha
2.88 RegionNumeric
2.89 RSAKeyModulus
2.90 RSAKeyPrivateExponent
2.91 RSAKeyPublicExponent
2.92 SensorApprovalNumber
2.93 SensorIdentification
2.94 SensorInstallation
2.95 SensorInstallationSecData
2.96 SensorOSIdentifier
2.97 SensorPaired
2.98 SensorPairingDate
2.99 SensorSerialNumber
2.100 SensorSCIdentifier
2.101 Signature
2.102 SimilarEventsNumber
2.103 SpecificConditionType
2.104 SpecificConditionRecord
2.105 Speed
2.106 SpeedAuthorised

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

1. ÚVOD

Tento doplnok špecifikuje dátové formáty, dátové prvky a dátové štruktúry používané v záznamovom zariadení a tachografových kartách.

1.1 **Základňa pre definíciu typov dát**

Tento doplnok používa špecifikáciu abstraktnej syntaktickej notácie jedna (ASN.1) na definovanie typov dát. To umožňuje aby boli definované jednoduché a štruktúrované dáta bez toho, aby z toho vyplýval akýkoľvek špecifický syntax (pravidlá kódovania), ktorý bude závislý na aplikácii a prostredí.

Pomenovanie typov ASN.1 sa používa podľa ISO/IEC 8824–1. To znamená, že:

– pokiaľ je to možné, význam typu dát vyplýva zo zvoleného názvu,

– ak je typ dát zložený z iných typov dát, názov typu dát je naďalej jediným sledom abecedných znakov začínajúcim veľkým písmenom, avšak v názve sa používajú veľké písmená na oznámenie zodpovedajúceho významu,

– vo všeobecnosti sa názvy typov dát vzťahujú na názov typu dát, z ktorého sú vytvorené, na zariadenie, v ktorom sú uložené a na funkciu vzťahujúcu sa k dátam.

Ak je typ ASN.1 už definovaný ako časť inej normy a ak je relevantný pre použitie v záznamovom zariadení, potom tento typ ASN.1 bude definovaný v tomto doplnku.

Aby boli možné viaceré kódovacie pravidlá, niektoré typy ASN.1 v tomto doplnku sú ohraničené identifikátormi rozsahu hodnôt. Identifikátory rozsahu hodnôt sú definované v odseku 3.

1.2 **Referenčné dokumenty**

V tomto doplnku sú použité tieto referenčné dokumenty:

ISO 639	Code for the representation of names of languages. First Edition: 1988 (Kód pre vyjadrenie názvov jazykov. Prvé vydanie: 1988)
EN 726–3	Identification cards systems – Telecommunications integrated circuit(s) cards and terminals – Part 3: Application independent card requirements. December 1994 (Systémy identifikačných kariet – telekomunikačné karty s integrovanými obvodmi a koncové zariadenia – Časť 3 – Požiadavky na karty nezávislé na aplikácii. December 1994)
ISO 3779	Road vehicles – Vehicle identification number (VIN) – Content and structure. Edition 3: 1983 (Cestné vozidlá – Identifikačné číslo vozidla (VIN) – Obsah a stavba. Vydanie 3: 1983)
ISO/IEC 7816–5	Information technology – Identification cards – Integrated circuit(s) cards with contacts – Part 5: Numbering system and registration procedure for application identifiers. First edition: 1994 + Amendment 1: 1996 (Informačné technológie – Identifikačné karty – Karty s integrovanými obvodmi a s kontaktmi – Časť 5: Systém číslovania a registračný postup identifikátorov aplikácií: prvé vydanie: 1994 + zmena 1:1996)
ISO/IEC 8824–1	Information technology – Abstract Syntax Notation 1 (ASN.1): Specification of basic notation. Edition 2: 1998 (Informačné technológie – Abstraktná syntaktická notácia – Špecifikácia základnej notácie. Vydanie 2: 1998)
ISO/IEC 8825–2	Information technology – ASN.1 encoding rules: Specification of Packed Encoding Rules (PER). Edition 2: 1998 (Informačné technológie – kódovacie pravidlá ASN.1: špecifikácia paketových kódovacích pravidiel (PER). Vydanie 2: 1998)
ISO/IEC 8859–1	Information technology – 8 bit single–byte coded graphic character sets – Part 1: Latin alphabet No 1. First edition: 1998 (Informačné technológie – Množiny grafických znakov kódované jednou 8–bitovou slabikou (jedným oktetom) – časť 1: Latinská abeceda č. 1, Prvé vydanie:1998)

ISO/IEC 8859–7	Information technology – 8 bit single–byte coded graphic character sets – Part 7: Latin/Greek alphabet. First edition: 1987 (Informačné technológie – Množiny grafických znakov kódované jednou 8–bitovou slabikou (jedným oktetom) – časť 7: Latinská abeceda/Grécka abeceda. Prvé vydanie:1997)
ISO 16844–3	Road vehicles – Tachograph systems – Motion Sensor Interface. WD 3–20/05/99 (Cestné vozidlá – Tachografové systémy – Rozhranie snímača pohybu. WD 3–20/05/99).

2. DEFINÍCIE TYPOV DÁT

Pri všetkých nasledovných typoch dát štandardná hodnota pre „neznámy“ alebo „neaplikovateľný“ obsah pozostáva z vyplnenia dátového prvku s „FF“–bajtami.

2.1 **ActivityChangeInfo**

Tento typ dát umožňuje, v rámci dvoj bajtového slova, kódovanie stavu slotu pri 00.00 a stavu vedenia pri 00.00 a pre vodiča a druhého vodiča zmeny činnosti a/alebo zmeny stavu vedenia a/alebo zmeny stavu karty. Tento typ sa vzťahuje k požiadavkám 084, 109a, 199 a 219.

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

Priradenie hodnoty – Usporiadaný oktet: ‘scpaatttttttttttt’B (16 bitov)

Pre záznamy v dátovej pamäti (alebo stav slotu):

‘s’B	Slot:
	‘0’B: VODIČ,
	‘1’B: DRUHÝ VODIČ,
‘c’B	Stav vedenia vozidla:
	‘0’B: SAMOTNÝ VODIČ,
	‘1’B: POSÁDKA,
‘p’B:	Stav karty vodiča (alebo dielenskej karty) v príslušnom slote:
	‘0’B: VLOŽENÁ, karta je vložená,
	‘1’B: NEVLOŽENÁ, nie je vložená žiadna karta (alebo karta je vytiahnutá),
‘aa’B:	Činnosť:
	‘00’B: PRESTÁVKA/ODPOČINOK,
	‘01’B: POHOTOVOSŤ,
	‘10’B: PRÁCA,
	‘11’B: VEDENIE,
‘ttttttttttt’B	Čas zmeny: počet minút od 00.00 hod. v danom dni.

Pre záznamy na karte vodiča (alebo dielenskej karte) (a stav vodiča):

‘s’B	Slot (irelevantný keď ‘p’ = 1, okrem poznámky nižšie):	
	‘0’B: VODIČ,	
	‘1’B: DRUHÝ VODIČ,	
‘c’B	Stav vedenia vozidla (prípad keď ‘p’= 0)	Stav ďalšej činnosti (keď ‘p’ = 1)
	‘0’B: SAMOTNÝ VODIČ,	‘0’B: NEZNÁMY
	‘1’B: POSÁDKA,	‘1’B: ZNÁMY (manuálne zapísané)
‘p’B:	Stav karty:	

‘0’B: VLOŽENÁ, karta je vložená v záznamovom zariadení,

‘1’B: NEVLOŽENÁ, karta nie je vložená (alebo karta je vytiahnutá),

‘aa’B: Činnosť (irelevantné keď ‘p’ = 1 a ‘c’ = 0, okrem poznámky nižšie):

‘00’B: PRESTÁVKA/ODPOČINOK,

‘01’B: POHOTOVOSŤ,

‘10’B: PRÁCA,

‘11’B: VEDENIE,

‘tttttttttt’B Čas zmeny: počet minút od 00.00 hod. v danom dni.

Poznámka pre prípad „vytiahnutie karty“:

Keď je karta vytiahnutá:

– ‘s’ je relevantné a udáva slot, z ktorého je karta vytiahnutá,
– ‘c’ musí byť nastavené na 0,
– ‘p’ musí byť nastavené na 1,
– ‘aa’ musí zakódovať prebiehajúcu činnosť zvolenú v tomto čase,

Následkom manuálneho zápisu sa bity ‘c’ a ‘aa‘ slova (uložené na karte) môžu neskôr prepísať, aby zohľadnili zápis.

2.2 **Address**

Adresa:

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

codePage špecifikuje časť ISO/IEC 8859 používaná na kódovanie adries,

address je adresa kódovaná v súlade s ISO/IEC 8859–codePage.

2.3 BCDString

BCDString sa používa na prezentáciu dvojkovo kódovaných dekadických čísiel. Tento typ dát sa používa na prezentáciu jednej dekadickej číslice v jednej 4–bitovej skupine. BCDString je založený na ISO/IEC 8824–1 ‘CharacterStringType‘.

BCDString ::= CHARACTER STRING (WITH COMPONENTS {

identification (WITH COMPONENTS {

fixed PRESENT }) })

BCDString používa „hstring“ notáciu. Najkrajnejšia ľavá šestnástková číslica je najvýznamnejšou 4–bitovou skupinou prvého oktetu. Na získanie násobku oktetov sa podľa potreby od polohy najkrajnejšej ľavej 4–bitovej skupiny v prvom oktete, pripoja 4–bitové skupiny s nulami na pravej strane.

Povolené číslice sú: 0, 1, ... 9.

2.4 **CalibrationPurpose**

Kód vysvetľujúci prečo bol zaznamenaný súbor kalibračných parametrov. Tento typ dát sa vzťahuje k požiadavkám 097 a 098.

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

Priradenie hodnoty:

‘00’H vyhradená hodnota,

‘01’H aktivácia: záznam kalibračných parametrov známych v okamihu aktivácie jednotky vozidla (JV),

‘02’H prvá montáž: prvá kalibrácia JV po jej aktivácii,

‘03’H montáž: prvá kalibrácia JV po súčasnom vozidle,

‘04’H pravidelná prehliadka.

2.5 **CardActivityDailyRecord**

Informácie uložené na karte, ktoré sa vzťahujú k činnostiam vodiča v určitom kalendárnom dni. Tento typ dát sa vzťahuje k požiadavkám 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 dĺžka predchádzajúceho denného záznamu v bajtoch. Maximálna hodnota je daná dĺžkou OCTET STRING obsahujúceho tieto záznamy (pozri CardActivityLengthRange odsek 3). Keď je tento záznam najstarším denným záznamom, hodnota activityPreviousRecordLength sa musí nastaviť na 0.

activityRecordLength je celková dĺžka tohoto záznamu. Maximálna hodnota je daná dĺžkou OCTET STRING obsahujúceho tieto záznamy.

activityRecordDate je dátum záznamu.

activityDailyPresenceCounter je počítadlo dennej prítomnosti pre kartu v tomto dni.

activityDayDistance je celková vzdialenosť prejdená v tomto dni.

activityChangeInfo je súbor ActivityChangeInfo dát pre vodiča v tomto dni. Môže obsahovať maximálne 1440 hodnôt (jedna zmena činnosti za minútu). Tento súbor vždy zahŕňa activityChangeInfo kódovanie stavu vodiča o 00.00 hod.

2.6 **CardActivityLengthRange**

Počet bajtov na karte vodiča alebo dielenskej karte, ktorý je k dispozícii na uloženie záznamov činnosti vodiča.

CardActivityLengthRange ::= INTEGER(0..2^{16}–1)

Priradenie hodnoty: pozri odsek 3.

2.7 **CardApprovalNumber**

Typové schvaľovacie číslo karty.

CardApprovalNumber ::= IA5String(SIZE(8))

Priradenie hodnoty: nešpecifikované.

2.8 **CardCertificate**

Osvedčenie verejného kľúča karty.

CardCertificate ::= Certificate.

2.9 **CardChipIdentification**

Informácia uložená na karte, ktorá sa vzťahuje k identifikácii integrovaného obvodu karty (IO) (požiadavka 191).

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

icSerialNumber je sériové číslo karty definované v EN 726–3.

icManufacturingReferences je identifikátor výrobcu IO a výrobných prvkov definovaných v EN 726–3.

2.10 **CardConsecutiveIndex**

Poradový index karty (definícia (h)).

CardConsecutiveIndex ::= IA5String(SIZE(1))

Priradenie hodnoty: (pozri kapitolu VII v tejto prílohe)

Poradie zvyšovania: ‘0, ..., 9, A, ..., Z, a, ..., z’.

2.11 **CardControlActivityDataRecord**

Informácie uložené na karte vodiča alebo dielenskej karte, ktoré sa vzťahujú k poslednej kontrole vodiča, ktorej sa vodič podrobil (požiadavky 210 a 225).

CardControlActivityDataRecord ::= SEQUENCE {

controlType	controlType,
controlTime	TimeReal,
controlCardNumber	FullCardNumber,
controlVehicleRegistration	VehicleRegistrationIdentification,
controlDownloadPeriodBegin	TimeReal,
controlDownloadPeriodEnd	TimeReal,

}

controlType je typ kontroly.

controlTime je dátum a čas kontroly.

controlCardNumber je FullCardNumber kontrolóra vykonávajúceho kontrolu.

controlVehicleRegistration je registračné číslo vozidla a registrujúci členský štát vozidla, v ktorom sa kontrola uskutočnila.

controlDownloadPeriodBegin a **controlDownloadPeriodEnd** je časový úsek pri sťahovaní.

2.12 **CardCurrentUse**

Informácie o aktuálnom použití karty (požiadavka 212).

CardCurrentUse ::= SEQUENCE {

sessionOpenTime	TimeReal,
sessionOpenVehicle	VehicleRegistrationIdentification

}

sessionOpenTime je čas, kedy je karta vložená pre aktuálne použitie. Tento prvok je nastavený na nulu pri odstránení karty.

sessionOpenVehicle je identifikácia súčasne používaného vozidla nastavená pri vložení karty. Tento prvok je nastavený na nulu pri odstránení karty.

2.13 **CardDriverActivity**

Informácie uložené na karte vodiča alebo dielenskej karte, ktoré sa vzťahujú činnostiam vodiča (požiadavky 199 a 219).

CardDriverActivity ::= SEQUENCE {

activityPointerOldestDayRecord	INTEGER(0..CardActivityLengthRange–1),
activityPointerNewestRecord	INTEGER(0..CardActivityLengthRange–1),
activityDailyRecords	OCTET STRING (SIZE(CardActivityLengthRange))

}

activityPointerOldestDayRecord je špecifikácia začiatku miesta uloženia (počet bajtov od začiatku reťazca) najstaršieho úplného denného záznamu v activityDailyRecords reťazci. Maximálna hodnota je daná dĺžkou reťazca.

activityPointerNewestRecord je špecifikácia začiatku miesta uloženia (počet bajtov od začiatku reťazca) najnovšieho úplného denného záznamu v activityDailyRecords reťazci. Maximálna hodnota je daná dĺžkou reťazca.

activityDailyRecords je miesto, ktoré je k dispozícii na uloženie dát o činnosti vodiča (dátové štruktúra: CardActivityDailyRecord) za každý kalendárny deň, v ktorom sa karta použila.

Priradenie hodnoty: tento oktet sa cyklicky vypĺňa záznamami CardActivityDailyRecord. Pri prvom použití sa ukladanie začína v prvom bajte reťazca. Všetky nové záznamy sa pripájajú na koniec predchádzajúceho. Keď je reťazec plný, ukladanie pokračuje v prvom bajte reťazca nezávisle na prerušení vo vnútri dátového prvku. Pred umiestnením dát o novej činnosti (na zväčšenie súčasného activityDailyRecord, alebo umiestnenie nového, activityDailyRecord), ktorý nahradí dáta o staršej činnosti, activityPointerOldestDayRecord sa musí aktualizovať aby odrážal novú polohu najstaršieho úplného denného záznamu a activityPreviousRecordLength tohto (nového) najstaršieho úplného denného záznamu sa musí nastaviť na 0.

2.14 **CardDrivingLicenceInformation**

Informácie uložené na karte vodiča, ktoré sa vzťahujú k dátam vodičského preukazu držiteľa karty (požiadavka 196).

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

drivingLicenceIssuingAuthority je orgán zodpovedný za vydanie vodičského preukazu.

drivingLicenceIssuingNation je štátna príslušnosť orgánu, ktorý vydal vodičský preukaz.

drivingLicenceNumber je číslo vodičského preukazu.

2.15 **CardEventData**

Informácie uložené na karte vodiča alebo dielenskej karte, ktoré sa vzťahujú k udalostiam súvisiacim s držiteľom karty (požiadavky 204 a 223).

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

CardEventData je sled usporiadaný podľa vzostupnej hodnoty EventFaultType, cardEventRecords (s výnimkou pokusov o narušenie bezpečnosti vzťahujúcich sa k záznamom, ktoré sú zhromaždené v poslednom súbore sledu).

cardEventRecords je súbor záznamov o udalostiach daného typu udalostí (alebo kategória pri udalostiach pokusov o narušenie bezpečnosti).

2.16 **CardEventRecord**

Informácie uložené na karte vodiča alebo dielenskej karte, ktoré sa vzťahujú k udalostiam súvisiacim s držiteľom karty (požiadavky 205 a 223).

CardEventRecord ::= SEQUENCE {

eventType	EventFaultType,
eventBeginTime	TimeReal,
eventEndTime	TimeReal,
eventVehicleRegistration	VehicleRegistrationIdentification

}

eventType je typ udalosti.

eventBeginTime je dátum a čas začiatku udalosti.

eventEndTime je dátum a čas skončenia udalosti.

eventVehicleRegistration je registračné číslo vozidla a registrujúci členský štát vozidla, u ktorého udalosť nastala.

2.17 **CardFaultData**

Informácie uložené na karte vodiča alebo dielenskej karte, ktoré sa vzťahujú k poruchám v súvislosti držiteľom karty (požiadavky 207 a 223).

CardFaultData ::= SEQUENCE SIZE(2) OF {

cardFaultRecords	SET SIZE(NoOfFaultsPerType) OF CardFaultRecord

}

CardFaultData je sled súboru porúch záznamov záznamového zariadenia, za ktorým nasleduje súbor porúch záznamov karty.

cardFaultRecords je súbor záznamov o poruchách danej kategórie poruchy (záznamové zariadenie alebo karta).

2.18 **CardFaultRecord**

Informácie uložené na karte vodiča alebo dielenskej karte, ktoré sa vzťahujú k poruchám v súvislosti držiteľom karty (požiadavky 208 a 223).

CardFaultRecord ::= SEQUENCE {

faultType	EventFaultType,
faultBeginTime	TimeReal,
faultEndTime	TimeReal,
faultVehicleRegistration	VehicleRegistrationIdentification

}

faultType je typ poruchy.

faultBeginTime je dátum a čas začiatku poruchy.

faultEndTime je dátum a čas skončenia poruchy.

faultVehicleRegistration je registračné číslo vozidla a registrujúci členský štát vozidla, u ktorého porucha nastala.

2.19 **CardIccIdentification**

Informácie uložené na karte vzťahujúce sa k identifikácii karty s integrovanými obvodmi (IO) (požiadavka 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 Clockstop režim definovaný v EN 726–3.

cardExtendedSerialNumber je sériové číslo karty a výrobný údaj karty podľa EN 726–3, ďalej špecifikované pomocou typu dát ExtendedSerialNumber.

cardApprovalNumber je typové schvaľovacie číslo karty.

cardPersonaliserID je identifikácia personalizácie karty definovaná v EN 726–3.

embedderIcAssemblerId je identifikátor zhotoviteľa/asemblera IC definovaný v EN 726–3.
icIdentifier je identifikátor IC na karte a výrobcu IC definovaný v EN 726–3.

2.20 **CardIdentification**

Informácie uložené na karte vzťahujúce sa k identifikácii karty (požiadavky 194, 215, 231, 235).

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

cardIssuingMemberState je kód členského štátu, ktorý kartu vydal.

cardNumber je číslo karty.

cardIssuingAuthorityName je názov orgánu, ktorý kartu vydal.

cardIssueDate je dátum vydania karty súčasnému držiteľovi.

cardValidityBegin je prvý dátum, ktorým začína platnosť karty.

cardExpiryDate je dátum, ktorým končí platnosť karty.

2.21 **CardNumber**

Číslo karty definované v (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 identifikácia vodiča v členskom štáte.

ownerIdentification je jednoznačná identifikácia podniku alebo dielne alebo kontrolného orgánu v členskom štáte.

cardConsecutiveIndex je poradový index karty.

cardReplacementIndex je index náhrady karty.

cardRenewalIndex je index obnovy karty.

Prvý sled voľby je vhodný na kódovanie čísla karty vodiča, druhý sled voľby je vhodný na kódovanie čísla dielenskej, kontrolnej a podnikovej karty.

2.22 **CardPlaceDailyWorkPeriod**

Informácie uložené na karte vodiča alebo dielenskej karte vzťahujúce sa k miestam, kde denný pracovný čas začína (požiadavky 202 a 221).

```
CardPlaceDailyWorkPeriod ::= SEQUENCE {
    placePointerNewestRecord        INTEGER(0..NoOfCardPlaceRecords–1),
    placeRecords                    SIZE(NoOfCardPlaceRecords) OF PlaceRecord
}
```

placePointerNewestRecord je index naposledy aktualizovaného záznamu o mieste.

Priradenie hodnoty: číslo zodpovedajúce počítadlu záznamu o mieste začínajúce od ‘0’ pre prvý výskyt záznamov o mieste v štruktúre.

placeRecords je súbor záznamov, obsahujúcich informácie vzťahujúce sa zaznamenaným miestam.

2.23 **CardPrivateKey**

Súkromný kľúč karty.

CardPrivateKey ::= RSAKeyPrivateExponent.

2.24 **CardPublicKey**

Verejný kľúč karty.

CardPublicKey ::= PublicKey.

2.25 **CardRenewalIndex**

Index obnovy karty (definícia v (i)).

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

Priradenie hodnoty: (pozri kapitolu VII v tejto prílohe).

‘0’ Prvé vydanie.

Poradie zvyšovania: ‘0, ..., 9, A, ..., Z’

2.26 **CardReplacementIndex**

Index náhrady karty (definícia v (j)).

CardReplacementIndex::=IA5String(SIZE(1))

Priradenie hodnoty: (pozri kapitolu VII v tejto prílohe).

‘0’ Pôvodná karta.

Poradie zvyšovania: ‘0, ..., 9, A, ..., Z’

2.27 **CardSlotNumber**

Kód na rozlíšenie dvoch slotov jednotky vozidla.

CardSlotNumber ::= INTEGER {

driverSlot	(0),
co–driverSlot	(1)

}

Priradenie hodnoty: nie je bližšie špecifikované.

2.28 **CardSlotsStatus**

Kód udávajúci typ karty vloženej do dvoch slotov jednotky vozidla.

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

Priradenie hodnoty: **Usporiadaný oktet: ‘**ccccdddd**‘**B:

‘cccc**‘**B identifikácia typu karty vloženej do slotu druhého vodiča,

‘dddd**‘**B identifikácia typu karty vloženej do slotu vodiča,

s nasledovnými identifikačnými kódmi:

‘0000**‘**B nie je vložená žiadna karta,

‘0001**‘**B je vložená karta vodiča,

‘0010**‘**B je vložená dielenská karta,

‘0011**‘**B je vložená kontrolná karta,

‘0100‘B je vložená podniková karta.

2.29 **CardStructureVersion**

Kód udávajúci verziu štruktúry implementovanej v tachografovej karte.

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

Priradenie hodnoty: ‘aabb‘H:

„aa**“**H index pre zmeny štruktúry, „00h“ pre túto verziu,

„bb**“**H index pre zmeny týkajúci sa používania dátových prvkov definovaných pre štruktúru danú horným bytom „00h“ pre túto verziu.

2.30 **CardVehicleRecord**

Informácie uložené na karte vodiča alebo dielenskej karte, vzťahujúce sa k časovému úseku používania vozidla počas kalendárneho dňa (požiadavky 197 a 217).

CardVehicleRecord ::= SEQUENCE {

vehicleOdometerBegin	OdometerShort,
vehicleOdometerEnd	OdometerShort,
vehicleFirstUse	TimeReal,
vehicleLastUse	TimeReal,
vehicleRegistration	VehicleRegistrationIdentification,
vuDataBlockCounter	VuDataBlockCounter

}

vehicleOdometerBegin je stav kilometrov na začiatku časového úseku používania vozidla.

vehicleOdometerEnd je stav kilometrov na konci časového úseku používania vozidla.

vehicleFirstUse je dátum a čas začiatku časového úseku používania vozidla.

vehicleLastUse je dátum a čas skončenia časového úseku používania vozidla.

vehicleRegistration je registračné číslo vozidla a registrujúci členský štát vozidla.

vuDataBlockCounter je hodnota VuDataBlockCounter pri poslednom vytiahnutí časového úseku používania vozidla.

2.31 **CardVehiclesUsed**

Informácie uložené na karte vodiča alebo dielenskej karte, vzťahujúce sa k vozidlu používanému držiteľom karty (požiadavky 197 a 217).

CardVehiclesUsed := SEQUENCE {

vehiclePointerNewestRecord	INTEGER(0..NoOfCardVehicleRecords–1),
cardVehicleRecords	SET SIZE(NoOfCardVehicleRecords) OF CardVehicleRecord

}

vehiclePointerNewestRecord je index naposledy aktualizovaného záznamu o vozidle.

Priradenie hodnoty: číslo zodpovedajúce počítadlu záznamu o vozidle začínajúce od ‘0’ pre prvý výskyt záznamov o vozidle v štruktúre.

cardVehicleRecords je súbor záznamov, obsahujúcich informácie o použitých vozidlách.

2.32 **Certificate**

Osvedčenie verejného kľúča vydané certifikačným orgánom.

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

Priradenie hodnoty: digitálny podpis s čiastočnou obnovou CertificateContent podľa doplnku 11 „spoločné bezpečnostné mechanizmy“: Signature (128 bytes) || Public Key remainder (58 Byte) || Certification Authority Reference (8 bytes).

2.33 **CertificateContent**

(Jasný) obsah osvedčenia verejného kľúča podľa doplnku 11 „spoločné bezpečnostné mechanizmy“.

CertificateContent ::= SEQUENCE {

certificateProfileIdentifier	INTEGER(0..255),
certificationAuthorityReference	KeyIdentifier,
certificateHolderAuthorisation	CertificateHolderAuthorisation,
certificateEndOfValidity	TimeReal,
certificateHolderReference	KeyIdentifier,
publicKey	PublicKey

}

certificateProfileIdentifier je verzia zodpovedajúceho osvedčenia.

Priradenie hodnoty: ‘01h‘ pre túto verziu.

CertificationAuthorityReference identifikuje certifikačný orgán vydávajúci osvedčenie. Okrem toho obsahuje odkaz na verejný kľúč tohoto certifikačného orgánu.

certificateHolderAuthorisation identifikuje práva držiteľa osvedčenia.

certificateEndOfValidity je dátum, ktorým končí administratívna platnosť osvedčenia.

certificateHolderReference identifikuje držiteľa osvedčenia. Okrem toho obsahuje odkaz na jeho verejný kľúč.

publicKey je verejný kľúč, ktorý je týmto osvedčením potvrdený.

2.34 **CertificateHolderAuthorisation**

Identifikácia práv držiteľa osvedčenia.

CertificateHolderAuthorisation ::= SEQUENCE {

tachographApplicationID	OCTET STRING(SIZE(6))
equipmentType	EquipmentType

}

tachographApplicationID je identifikátor aplikácie pre tachografovú aplikáciu.

Priradenie hodnoty: ‘FFh’ ’54h’ ’41h’ ’43h’ ’48h’ ’4Fh’. Tento AID je špeciálny neregistrovaný identifikátor aplikácie v súlade s ISO/IEC 7816–5.

equipmentType je identifikácia typu zariadenia, pre ktoré je osvedčenie určené.

Priradenie hodnoty: v súlade s typom dát EquipmentType. 0 ak ide o osvedčenie jedného členského štátu.

2.35 **CertificateRequestID**

Jednoznačná identifikácia žiadosti o osvedčenie. Môže sa použiť aj ako identifikátor verejného kľúča jednotky vozidla, ak nie je v dobe vyhotovenia osvedčenia známe sériové číslo jednotky vozidla, ktorej je kľúč určený.

CertificateRequestID ::= SEQUENCE {

requestSerialNumber	INTEGER(0..2^{32}–1)
requestMonthYear	BCDString(SIZE(2))
crIdentifier	OCTET STRING(SIZE(1))
manufacturerCode	ManufacturerCode

}

requestSerialNumber je sériové číslo žiadosti o osvedčenie, jednotné pre nižšie uvedeného výrobcu a mesiac.

requestMonthYear je identifikácia mesiaca a roku žiadosti o osvedčenie.

Priradenie hodnoty: BCD kódovanie mesiaca (dve číslice) a roku (dve posledné číslice).

crIdentifier: je identifikátor na rozlíšenie žiadosti o osvedčenie od rozšíreného sériového čísla.

Priradenie hodnoty: ‘FFh‘.

manufacturerCode: je numerický kód výrobcu, ktorý žiada o vydanie osvedčenia.

2.36 **CertificationAuthorityKID**

Identifikátor verejného kľúča certifikačného orgánu (členský štát alebo Európsky certifikačný úrad).

CertificationAuthorityKID ::= SEQUENCE {

nationNumeric	NationNumeric
nationAlpha	NationAlpha
keySerialNumber	INTEGER(0..255)
additionalInfo	OCTET STRING(SIZE(2))
caIdentifier	OCTET STRING(SIZE(1))

}

nationNumeric je numerický kód certifikačného orgánu členského štátu.

nationAlpha je alfanumerický kód certifikačného orgánu členského štátu.

keySerialNumber je sériové číslo na rozlíšenie rôznych kľúčov certifikačného orgánu v prípade zmeny kľúčov.

additionalInfo je dvojbajtové pole pre doplnkové kódovanie (podľa certifikačného orgánu).

caIdentifier je identifikátor na rozlíšenie identifikátora kľúča certifikačného orgánu od iných identifikátorov kľúča.

Priradenie hodnoty: ‘01h‘.

2.37 **CompanyActivityData**

Informácie uložené na podnikovej karte vzťahujúce sa k činnostiam, ktoré sa s kartou vykonávajú (požiadavka 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 naposledy aktualizovaného companyActivityRecord.

Priradenie hodnoty: **:** číslo zodpovedajúce počítadlu záznamu o mieste začínajúce od '0' pre prvý výskyt záznamu o činnosti podniku v štruktúre.

companyActivityRecords je súbor všetkých záznamov o činnosti podniku.

companyActivityRecord je sled informácií vzťahujúcich sa k jednej činnosti podniku.

companyActivityType je typ činnosti podniku.

companyActivityTime je dátum a čas činnosti podniku.

cardNumberInformation prípadne číslo karty a členský štát, ktorý vydal sťahovanú kartu.

vehicleRegistrationInformation registračné číslo vozidla a registrujúci členský štát sťahovaného, zablokovaného alebo odblokovaného vozidla.

downloadPeriodBegin a **downloadPeriodEnd** je prípadne časový úsek sťahovania z jednotky vozidla.

2.38 **CompanyActivityType**

Kód udávajúci činnosť vykonávanú podnikom, ktorý používa svoju podnikovú kartu.

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

2.39 **CompanyCardApplicationIdentification**

Informácie uložené na podnikovej karte vzťahujúce sa k identifikácii aplikácie karty (požiadavka 190).

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

typeOfTachographCardId špecifikuje implementovaný typ karty.

cardStructureVersion špecifikuje verziu štruktúry implementovanej v karte.

noOfCompanyActivityRecords je počet záznamov o činnosti podniku, ktorý sa môže na karte uložiť.

2.40 **CompanyCardHolderIdentification**

Informácie uložené na podnikovej karte vzťahujúce sa k identifikácii držiteľa karty (požiadavka 236).

```
CompanyCardHolderIdentification ::= SEQUENCE {
    companyName                     Name,
```

companyAddress Address,

cardHolderPreferredLanguage Language

}

companyName je názov podniku, ktorý je držiteľom karty.

companyAddress je adresa podniku, ktorý je držiteľom karty.

cardHolderPreferredLanguage je uprednostnený jazyk držiteľa karty.

2.41 **ControlCardApplicationIdentification**

Informácie uložené na kontrolnej karte vzťahujúce sa k identifikácii aplikácie karty (požiadavka 190).

ControlCardApplicationIdentification ::= SEQUENCE {

typeOfTachographCardId EquipmentType,

cardStructureVersion CardStructureVersion,

noOfControlActivityRecords NoOfControlActivityRecords

}

typeOfTachographCardId špecifikuje implementovaný typ karty.

cardStructureVersion špecifikuje verziu štruktúry implementovanej v karte.

noOfControlActivityRecords je počet záznamov o kontrolnej činnosti, ktorý sa môže na karte uložiť.

2.42 **ControlCardControlActivityData**

Informácie uložené na kontrolnej karte vzťahujúce sa ku kontrolnej činnosti vykonávanej s kartou (požiadavka 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 naposledy aktualizovaného záznamu o kontrolnej činnosti.

Priradenie hodnoty: číslo zodpovedajúce počítadlu záznamu o kontrolnej činnosti začínajúce od ‘0’ pre prvý výskyt záznamu o kontrolnej činnosti v štruktúre.

controlActivityRecords je súbor všetkých záznamov o kontrolnej činnosti.

controlActivityRecord je sled informácií vzťahujúcich sa k jednej kontrole.

controlType je typ kontroly.

controlTime je dátum a čas kontroly.

controlledCardNumber je číslo karty a členský štát, ktorý vydal kontrolovanú kartu.

controlledVehicleRegistration je registračné číslo vozidla a registrujúci členský štát vozidla, ktorého kontrola sa uskutočnila.

controlDownloadPeriodBegin and **controlDownloadPeriodEnd** je eventuálne sťahovaný časový úsek.

2.43. **ControlCardHolderIdentification**

Informácie uložené na kontrolnej karte vzťahujúce sa k identifikácii držiteľa karty (požiadavka 232).

ControlCardHolderIdentification ::= SEQUENCE {

controlBodyName	Name,
controlBodyAddress	Address,
cardHolderName	HolderName,
cardHolderPreferredLanguage	Language

}

controlBodyName je názov kontrolného orgánu držiteľa karty.

controlBodyAddress je adresa kontrolného orgánu držiteľa karty.

cardHolderName je priezvisko a meno(á) držiteľa kontrolnej karty.

cardHolderPreferredLanguage je uprednostňovaný jazyk držiteľa karty.

2.44 **ControlType**

Kód udávajúci činnosti vykonávané počas kontroly. Tento typ dát sa vzťahuje k požiadavkám 102, 210 a 225.

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

Priradenie hodnoty – Usporiadaný oktet: ‘cvpdxxxx‘B (8 bitov)

‘c‘°B	sťahovanie karty:
	‘0‘B: karta sa nesťahuje počas tejto kontrolnej činnosti,
	‘1‘B: karta sa sťahuje počas tejto kontrolnej činnosti
‘v‘B	sťahovanie JV:
	‘0‘B: JV sa nesťahuje počas tejto kontrolnej činnosti,
	‘1‘B: JV sa nesťahuje počas tejto kontrolnej činnosti,
‘p‘B	tlač:
	‘0‘B: počas tejto kontrolnej činnosti sa tlač nevykonáva,
	‘1‘B: počas tejto kontrolnej činnosti sa tlač vykonáva
‘d‘B	displej:
	‘0‘B: počas tejto kontrolnej činnosti sa displej nepoužíva,
	‘1‘B: počas tejto kontrolnej činnosti sa displej používa
‘xxxx‘B	nevyužité.

2.45 **CurrentDateTime**

Aktuálny dátum a čas záznamového zariadenia.

CurrentDateTime ::= TimeReal

Priradenie hodnoty: nie je bližšie špecifikované.

2.46 **DailyPresenceCounter**

Počítadlo uložené na karte vodiča alebo na dielenskej karte, sa zvýši o jedno za každý kalendárny deň, v ktorom bola karta vložená v jednotke vozidla. Tento typ dát sa vzťahuje k požiadavkám 199 a 219.

DailyPresenceCounter ::= BCDString(SIZE(2))

Priradenie hodnoty: postupné čísla s maximálnou hodnotou = 9999, začínajúc opäť s 0. V čase prvého vydania karty je číslo nastavené na 0.

2.47 **Datef**

Dátum vyjadrený v ľahko vytlačiteľnom numerickom formáte.

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

Priradenie hodnoty:

yyyy	Rok
mm	Mesiac
dd	Deň

‘00000000‘H neoznačuje explicitne žiadny dátum.

2.48 **Distance**

Prejdená vzdialenosť (výsledok výpočtu rozdielu medzi dvoma hodnotami počítadla v kilometroch.

Distance ::= INTEGER(0..2^{16}–1)

Priradenie hodnoty: dvojkové číslo bez znamienka. Hodnota v km v prevádzkovom rozsahu od 0 do 9999 km.

2.49 **DriverCardApplicationIdentification**

Informácie uložené na karte vodiča vzťahujúce sa k identifikácii aplikácie karty (požiadavka 190).

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

typeOfTachographCardId špecifikuje implementovaný typ karty.

cardStructureVersion špecifikuje verziu štruktúry implementovanej v karte.

noOfEventsPerType je počet udalostí podľa typu udalosti, ktorý sa môže na karte zaznamenať.

noOfFaultsPerType je počet porúch podľa typu poruchy, ktorý sa môže na karte zaznamenať.

activityStructureLength udáva počet bajtov, ktoré sú k dispozícii na uloženie záznamov o činnost.

noOfCardVehicleRecords je počet záznamov o vozidle, ktorý môže karta obsahovať.

noOfCardPlaceRecords je počet miest, ktorý sa môže na karte zaznamenať.

2.50 **DriverCardHolderIdentification**

Informácie uložené na karte vodiča vzťahujúce sa k identifikácii držiteľa karty (požiadavka 195).

DriverCardHolderIdentification ::= SEQUENCE {

cardHolderName	HolderName,
cardHolderBirthDate	Datef,
cardHolderPreferredLanguage	Language

}

cardHolderName priezvisko a meno(á) držiteľa karty vodiča.

cardHolderBirthDate je dátum narodenia držiteľa karty vodiča.

cardHolderPreferredLanguage je uprednostnený jazyk držiteľa karty.

2.51 **EntryTypeDailyWorkPeriod**

Kód na rozlíšenie začiatku a konca zápisu denného pracovného času, miesta a podmienok zápisu.

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)

}

Priradenie hodnoty: podľa ISO/IEC8824–1.

2.52 **EquipmentType**

Kód na rozlíšenie typov zariadenia pre tachografovú aplikáciu.

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)

Priradenie hodnoty: podľa ISO/IEC 8824–1.

Hodnota 0 je vyhradená na účely označenia členského štátu alebo Európy v poli CHA osvedčení.

2.53 **EuropeanPublicKey**

Európsky verejný kľúč.

EuropeanPublicKey ::= PublicKey.

2.54 **EventFaultType**

Kód bližšie popisujúci udalosť alebo poruchu.

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

Priradenie hodnoty:

‘0x‘H	všeobecné udalosti,
‘00‘H	žiadne ďalšie údaje,
‘01‘H	vloženie neplatnej karty,
‘02‘H	sporná karta,
‘03‘H	časové prekrývanie,
‘04‘H	vedenie bez príslušnej karty,
‘05‘H	vloženie karty počas vedenia,
‘06‘H	nesprávne uzavretá posledná relácia karty,
‘07‘H	prekročenie rýchlosti,
‘08‘H	prerušenie napájania,
‘09‘H	pohybová dátová chyba,
‘0A‘H to ‘0F‘H	RFU (vyhradené pre budúce funkcie),
‘1x‘H	pokus o narušenie bezpečnosti na jednotke vozidla,
‘10‘H	žiadne ďalšie údaje,
‘11‘H	chybné overenie snímača pohybu,
‘12‘H	chybné overenie tachografovej karty,
‘13‘H	neoprávnená zmena snímača pohybu,
‘14‘H	Chyba integrity vložených dát na kartu
‘15‘H	Chyba integrity uložených dát užívateľa,
‘16‘H	vnútorná chyba prenosu dát,
‘17‘H	neoprávnené otvorenie krytu,
‘18‘H	manipulácia s hardwarom,
‘19‘H to ‘1F‘H	RFU,
‘2x‘H	pokus o narušenie bezpečnosti snímača pohybu,
‘20‘H	žiadne ďalšie údaje,
‘21‘H	chybné overenie,
‘22‘H	chyba integrity uložených dát,
‘23‘H	vnútorná chyba prenosu dát,
‘24‘H	neoprávnené otvorenie krytu,
‘25‘H	manipulácia s hardwarom,
‘26‘H to ‘2F‘H	RFU,
‘3x‘H	poruchy záznamového zariadenia,
‘30‘H	žiadne ďalšie údaje,
‘31‘H	vnútorná porucha JV,
‘32‘H	porucha tlačiarne,

‘33‘H	porucha displeja,
‘34‘H	porucha sťahovania,
‘35‘H	porucha snímača,
‘36‘H to ‘3F‘H	RFU
‘4x‘H	poruchy karty,
‘40‘H	žiadne ďalšie údaje,
‘41‘H to ‘4F‘H	RFU
‘50‘H to ‘7F‘H	RFU,
‘80‘H to ‘FF’H	špecifické podľa výrobcu.

2.55 **EventFaultRecordPurpose**

Kód vysvetľujúci prečo bola zaznamenaná udalosť alebo porucha.

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

Priradenie hodnoty:

‘00‘H	jedna z 10 najnovších (alebo posledných) udalostí alebo porúch
‘01‘H	najdlhšia udalosť v jednom z posledných desiatich dní výskytu
‘02‘H	jedna z piatich najdlhších udalostí počas posledných 365 dní
‘03‘H	posledná udalosť v jednom z posledných desiatich dní výskytu
‘04‘H	najvážnejšia udalosť v jednom z posledných desiatich dní výskytu
‘05‘H	jedna z piatich najvážnejších udalostí počas posledných 365 dní
‘06‘H	prvá udalosť alebo porucha, ktorá nastala po poslednej kalibrácii
‘07‘H	aktívna/prebiehajúca udalosť alebo porucha
‘08‘H to ‘7F‘H	RFU
‘80‘H to ‘FF‘H	špecifické podľa výrobcu.

2.56 **ExtendedSerialNumber**

Jednoznačná identifikácia zariadenia. Môže sa použiť aj ako identifikátor verejného kľúča zariadenia.

ExtendedSerialNumber ::= SEQUENCE {

serialNumber	INTEGER(0..2^{32}–1)
monthYear	BCDString(SIZE(2))
type OCTET	STRING(SIZE(1))
manufacturerCode	ManufacturerCode

}

serialNumber je sériové číslo zariadenia, osobitné pre výrobcu, typ zariadenia a mesiac uvedený nižšie.

monthYear je identifikácia mesiaca a roku výroby (alebo pridelenia sériového čísla).

Priradenie hodnoty: BCD kódovanie mesiaca (dve číslice) a roku (dve posledné číslice).

type je identifikátor typu zariadenia.

Priradenie hodnoty: špecifické podľa výrobcu, s vyhradenou hodnotou FFh'.

manufacturerCode: je numerický kód výrobcu zariadenia.

2.57 **FullCardNumber**

Kód na úplnú identifikáciu tachografovej karty.

FullCardNumber ::= SEQUENCE {

cardType	EquipmentType,
cardIssuingMemberState	NationNumeric,
cardNumber	CardNumber

}

cardType je typ tachografovej karty.

cardIssuingMemberState je kód členského štátu, ktorý vydal kartu.

cardNumber je číslo karty.

2.58. **HighResOdometer**

Stav kilometrov udávaný počítadlom vozidla: Akumulovaná vzdialenosť prejdená vozidlom počas prevádzky.

HighResOdometer ::= INTEGER(0..2^{32}–1)

Priradenie hodnoty: dvojkové číslo bez znamienka. Hodnota v 1/200 km v prevádzkovom rozsahu od 0 do 21 055 406 km.

2.59 **HighResTripDistance**

HighResTripDistance ::= INTEGER(0..2^{32}–1)

Priradenie hodnoty: dvojkové číslo bez znamienka. Hodnota v 1/200 km v prevádzkovom rozsahu od 0 do 21 055 406 km.

2.60 **HolderName**

Priezvisko a meno(á) držiteľa karty.

HolderName ::= SEQUENCE {

holderSurname	Name,

holderFirstNames Name

}

holderSurname je priezvisko držiteľa bez titulu.

Priradenie hodnoty: Pokiaľ nejde o kartu vydanú určitej osobe, holderSurname obsahuje rovnaké informácie ako companyName alebo workshopName alebo controlBodyName.

holderFirstNames meno(á) a iniciály držiteľa.

2.61 **K–ConstantOfRecordingEquipment**

Konštanta záznamového zariadenia (definícia (m)).

K–ConstantOfRecordingEquipment ::= INTEGER(0..2^{16}–1)

Priradenie hodnoty: Impulzy na kilometer v prevádzkovom rozsahu 0 až 64 255 impulzov/km.

2.62 **KeyIdentifier**

Jednoznačný identifikátor verejného kľúča použitý ako odkaz na kľúč a na jeho voľbu. Identifikuje aj držiteľa kľúča.

KeyIdentifier ::= CHOICE {

extendedSerialNumber ExtendedSerialNumber,

certificateRequestID CertificateRequestID,

certificationAuthorityKID CertificationAuthorityKID

}

Prvá voľba je vhodná ako odkaz na verejný kľúč jednotky vozidla alebo tachografovej karty.

Druhá voľba je vhodná ako odkaz na verejný kľúč jednotky vozidla (v prípade, že sériové číslo jednotky vozidla nie je známe v čase vyhotovenia osvedčenia).

Tretia voľba je vhodná ako odkaz na verejný kľúč členského štátu.

2.63 **L–TyreCircumference**

Účinný obvod pneumatík kolies (definícia (u)).

L–TyreCircumference ::= INTEGER(0..2^{16}–1)

Priradenie hodnoty: dvojkové číslo bez znamienka. Hodnota v 1/8 mm v prevádzkovom rozsahu od 0 do 8 031 mm.

2.64 **Language**

Kód identifikujúci jazyk.

Language ::= IA5String(SIZE(2))

Priradenie hodnoty: dve malé písmená podľa ISO 639.

2.65 **LastCardDownload**

Dátum a čas posledného sťahovania dát z karty, uložené na karte vodiča (na iné účely než je kontrola). Tento dátum sa môže meniť pomocou ľubovolnej jednotky vozidla alebo prístroja na čítanie karty.

LastCardDownload ::= TimeReal

Priradenie hodnoty: nie je bližšie špecifikované.

2.66 **ManualInputFlag**

Kód, ktorý udáva, či držiteľ karty manuálne zapísal alebo nezapísal činnosti vodiča pri vložení karty (požiadavka 081).

ManualInputFlag ::= INTEGER {

noEntry	(0)
manualEntries	(1)

}

Priradenie hodnoty: nie je bližšie špecifikované.

2.67 **ManufacturerCode**[5]

Kód identifikujúci výrobcu.

ManufacturerCode ::= INTEGER(0..255)

Priradenie hodnoty:

‘00‘H	Nie sú k dispozícii žiadne informácie
‘01’H	Vyhradená hodnota
‘02‘H .. ‘0F‘H	Vyhradené pre budúce použitie
‘10‘H	ACTIA
‘11‘H .. ‘17‘H	Vyhradené pre výrobcov, ktorých meno začína na „A“
‘18‘H .. ‘1F‘H	Vyhradené pre výrobcov, ktorých meno začína na „B“
‘20‘H .. ‘27‘H	Vyhradené pre výrobcov, ktorých meno začína na „C“
‘28‘H .. ‘2F‘H	Vyhradené pre výrobcov, ktorých meno začína na „D“
‘30‘H .. ‘37‘H	Vyhradené pre výrobcov, ktorých meno začína na „E“
‘38‘H .. ‘3F‘H	Vyhradené pre výrobcov, ktorých meno začína na „F“
‘40‘H	Giesecke & Devrient GmbH
‘41‘H	GEM plus
‘42‘H .. ‘47‘H	Vyhradené pre výrobcov, ktorých meno začína na „G“
‘48‘H .. ‘4F‘H	Vyhradené pre výrobcov, ktorých meno začína na „H“
‘50‘H .. ‘57‘H	Vyhradené pre výrobcov, ktorých meno začína na „I“
‘58‘H .. ‘5F‘H	Vyhradené pre výrobcov, ktorých meno začína na „J“
‘60‘H .. ‘67‘H	Vyhradené pre výrobcov, ktorých meno začína na „K“
‘68‘H .. ‘6F‘H	Vyhradené pre výrobcov, ktorých meno začína na „L“
‘70‘H .. ‘77‘H	Vyhradené pre výrobcov, ktorých meno začína na „M“
‘78‘H .. ‘7F‘H	Vyhradené pre výrobcov, ktorých meno začína na „N“
‘80‘H	OSCARD
‘81‘H .. ‘87‘H	Vyhradené pre výrobcov, ktorých meno začína na „O“
‘88‘H .. ‘8F‘H	Vyhradené pre výrobcov, ktorých meno začína na „P“
‘90‘H .. ‘97‘H	Vyhradené pre výrobcov, ktorých meno začína na „Q“
‘98‘H .. ‘9F‘H	Vyhradené pre výrobcov, ktorých meno začína na „R“

[5] Aktualizovaný zoznam kódov identifikujúcich výrobcu bude dostupný na webovej stránke Európskeho certifikačného orgánu.

‘A0‘H	SETEC
‘A1‘H	SIEMENS VDO
‘A2‘H	STONERIDGE
‘A3‘H .. ‘A7‘H	Vyhradené pre výrobcov, ktorých meno začína na „S“
‘AA‘H	TACHOCONTROL
‘AB‘H .. ‘AF‘H	Vyhradené pre výrobcov, ktorých meno začína na „T“
‘B0‘H .. ‘B7‘H	Vyhradené pre výrobcov, ktorých meno začína na „U“
‘B8‘H .. ‘BF‘H	Vyhradené pre výrobcov, ktorých meno začína na „V“
‘C0‘H .. ‘C7‘H	Vyhradené pre výrobcov, ktorých meno začína na „W“
‘C8‘H .. ‘CF‘H	Vyhradené pre výrobcov, ktorých meno začína na „X“
‘D0‘H .. ‘D7‘H	Vyhradené pre výrobcov, ktorých meno začína na „Y“
‘D8‘H .. ‘DF‘H	Vyhradené pre výrobcov, ktorých meno začína na „Z“

2.68 **MemberStateCertificate**

Osvedčenie verejného kľúča členského štátu, vydané Európskym certifikačným úradom.

MemberStateCertificate ::= Certificate

2.69 **MemberStatePublicKey**

Verejný kľúč členského štátu.

MemberStatePublicKey ::= PublicKey.

2.70 **Name**

Meno.

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

codePage špecifikuje časť ISO/IEC 8859 používaná na kódovanie mien,

name je meno kódované v súlade s ISO/IEC 8859–codePage.

2.71 **NationAlpha**

Abecedný odkaz na štát, v súlade s dohodnutou značkou štátov na vozidlách a/alebo používaný v medzinárodne harmonizovaných dokumentoch o poistení vozidla (zelená karta).

NationAlpha ::= IA5String(SIZE(3))

Priradenie hodnoty:

‘ ’	Nie sú k dispozícii žiadne informácie
‘A‘	Rakúsko
‘AL‘	Albánsko
‘AND‘	Andorra
‘ARM‘	Arménsko
‘AZ‘	Azerbajdžan
‘B‘	Belgicko
‘BG‘	Bulharsko
‘BIH‘	Bosna a Hercegovina
‘BY‘	Bielorusko
‘CH‘	Švajčiarsko
‘CY‘	Cyprus
‘CZ‘	Česká republika
‘D‘	Nemecko
‘DK‘	Dánsko
‘E‘	Španielsko
‘EST‘	Estónsko
‘F‘	Francúzsko
‘FIN‘	Fínsko
‘FL‘	Lichtensteinsko
‘FR‘	Faerské ostrovy
‘UK‘	Spojené kráľovstvo, Alderney, Guernsey, Jersey, Isle of Man, Gibraltar
‘GE‘	Gruzínsko
‘GR‘	Grécko
‘H‘	Maďarsko
‘HR‘	Chorvátsko
‘I‘	Taliansko
‘IRL‘	Írsko
‘IS‘	Island
‘KZ‘	Kazachstan
‘L‘	Luxembursko
‘LT‘	Litva
‘LV‘	Lotyšsko

‘M‘	Malta
‘MC‘	Monako
‘MD‘	Moldavská republika
‘MK‘	Macedónsko
‘N‘	Nórsko
‘NL‘	Holandsko
‘P‘	Portugalsko
‘PL‘	Polsko
‘RO‘	Rumunsko
‘RSM‘	San Marino
‘RUS‘	Ruská federácia
‘S‘	Švédsko
‘SK‘	Slovensko
‘SLO‘	Slovinsko
‘TM‘	Turkménsko
‘TR‘	Turecko
‘UA‘	Ukrajina
‘V‘	Vatikán
‘YU‘	Juhoslávia
‘UNK‘	Neznáme
‘EC‘	Európske spoločenstvo
‘EUR‘	zvyšok Európy
‘WLD‘	zvyšok sveta.

2.72. **NationNumeric**

Numerické označenie štátu.

NationNumeric ::= INTEGER(0..255)

Priradenie hodnoty:

– – Nie sú k dispozícii žiadne informácie	(00)H,
– – Rakúsko	(01)H,
– – Albánsko	(02)H,
– – Andorra	(03)H,
– – Arménsko	(04)H,
– – Azerbajdžan	(05)H,
– – Belgicko	(06)H,
– – Bulharsko	(07)H,
– – Bosna a Hercegovina	(08)H,
– – Bielorusko	(09)H,
– – Švajčiarsko	(0A)H,

– – Cyprus (0B)H,
– – Česká republika (0C)H,
– – Nemecko (0D)H,
– – Dánsko (0E)H,
– – Španielsko (0F)H,
– – Estónsko (10)H,
– – Francúzsko (11)H,
– – Fínsko (12)H,
– – Lichtenštajnsko (13)H,
– – Faerské ostrovy (14)H,
– – Spojené kráľovstvo (15)H,
– – Gruzínsko (16)H,
– – Grécko (17)H,
– – Maďarsko (18)H,
– – Chorvátsko (19)H,
– – Taliansko (1A)H,
– – Írsko (1B)H,
– – Island (1C)H,
– – Kazachstan (1D)H,
– – Luxembursko (1E)H,
– – Litva (1F)H,
– – Lotyšsko (20)H,
– – Malta (21)H,
– – Monako (22)H,
– – Moldavská republika (23)H,
– – Macedónsko (24)H,
– – Nórsko (25)H,
– – Holandsko (26)H,
– – Portugalsko (27)H,
– – Poľsko (28)H,
– – Rumunsko (29)H,
– – San Marino (2A)H,
– – Ruská federácia (2B)H,
– – Švédsko (2C)H,
– – Slovensko (2D)H,
– – Slovinsko (2E)H,
– – Turkménsko (2F)H,
– – Turecko (30)H,

– – Ukrajina	(31)H,
– – Vatikán	(32)H,
– – Juhoslávia	(33)H,
– – RFU	(34..FC)H,
– – Európske spoločenstvo	(FD)H,
– – zvyšok Európy	(FE)H,
– – zvyšok sveta	(FF)H

2.73 **NoOfCalibrationRecords**

Počet kalibračných záznamov, ktoré môžu byť uložené na dielenskej karte.

NoOfCalibrationRecords ::= INTEGER(0..255)

Priradenie hodnoty: pozri odsek 3.

2.74 **NoOfCalibrationsSinceDownload**

Počítadlo udávajúce počet kalibrácií vykonaných s dielenskou kartou od jeho posledného stiahnutia (požiadavka 230).

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

Priradenie hodnoty: Nie je bližšie špecifikované.

2.75 **NoOfCardPlaceRecords**

Počet záznamov o mieste, ktoré môžu byť uložené na karte vodiča alebo na dielenskej karte.

NoOfCardPlaceRecords ::= INTEGER(0..255)

Priradenie hodnoty: pozri odsek 3.

2.76 **NoOfCardVehicleRecords**

Počet záznamov o použitých vozidlách, ktoré môžu byť uložené na karte vodiča alebo na dielenskej karte.

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

Priradenie hodnoty: pozri odsek 3.

2.77 **NoOfCompanyActivityRecords**

Počet záznamov o činnosti podniku, ktoré môžu byť uložené na karte vodiča alebo na dielenskej karte.

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

Priradenie hodnoty: pozri odsek 3.

2.78 **NoOfControlActivityRecords**

Počet záznamov o kontrolnej činnosti podniku, ktoré môžu byť uložené na kontrolnej karte.

NoOfControlActivityRecords ::= INTEGER(0..2^{16}–1)

Priradenie hodnoty: pozri odsek 3.

2.79 **NoOfEventsPerType**

Počet udalostí podľa typu udalosti, ktoré môžu byť uložené na karte.

NoOfEventsPerType ::= INTEGER(0..255)

Priradenie hodnoty: pozri odsek 3.

2.80 **NoOfFaultsPerType**

Počet porúch podľa typu poruchy, ktoré môžu byť uložené na karte.

NoOfFaultsPerType ::= INTEGER(0..255)

Priradenie hodnoty: pozri odsek 3.

2.81 **OdometerValueMidnight**

Hodnota počítadla kilometrov o polnoci daného dňa (požiadavka 090).

OdometerValueMidnight ::= OdometerShort

Priradenie hodnoty: Nie je bližšie špecifikované.

2.82 **OdometerShort**

Stav kilometrov vozidla v skrátenej forme.

OdometerShort ::= INTEGER(0..2^{24}–1)

Priradenie hodnoty: dvojkové číslo bez znamienka. Hodnota v km v prevádzkovom rozsahu od 0 do 9 999 999 km.

2.83 **OverspeedNumber**

Počet prekročení rýchlosti od poslednej kontroly prekročenia rýchlosti.

OverspeedNumber ::= INTEGER(0..255)

Priradenie hodnoty: 0 znamená, že od poslednej kontroly prekročenia rýchlosti nebola prekročená rýchlosť, 1 znamená, že od poslednej kontroly bola raz prekročená rýchlosť … 255 znamená, že od poslednej kontroly bola 255 alebo viackrát prekročená rýchlosť.

2.84 **PlaceRecord**

Informácie vzťahujúce sa k miestu, kde denný pracovný čas začína alebo končí (požiadavky 087, 202, 221).

PlaceRecord ::= SEQUENCE {

entryTime	TimeReal,
entryTypeDailyWorkPeriod	EntryTypeDailyWorkPeriod,
dailyWorkPeriodCountry	NationNumeric,
dailyWorkPeriodRegion	RegionNumeric,
vehicleOdometerValue	OdometerShort

}

entryTime je dátum a čas vzťahujúci sa k zápisu.

entryTypeDailyWorkPeriod je typ zápisu.

dailyWorkPeriodCountry je zapísaný štát.

dailyWorkPeriodRegion je zapísaný región.

vehicleOdometerValue je stav kilometrov v čase zápisu miesta.

2.85 **PreviousVehicleInfo**

Informácie vzťahujúce sa k predchádzajúcemu vozidlu použitému vodičom pri vložení jeho karty do jednotky vozidla (požiadavka 081).

PreviousVehicleInfo ::= SEQUENCE {

vehicleRegistrationIdentification	VehicleRegistrationIdentification,
cardWithdrawalTime	TimeReal

}

vehicleRegistrationIdentification je registračné číslo vozidla a registrujúci členský štát vozidla.

cardWithdrawalTime je dátum a čas vytiahnutia karty.

2.86 **PublicKey**

Verejný RSA kľúč.

PublicKey ::= SEQUENCE {

rsaKeyModulus	RSAKeyModulus,
rsaKeyPublicExponent	RSAKeyPublicExponent

}

rsaKeyModulus je modul kľúčového páru.

rsaKeyPublicExponent je verejný exponent kľúčového páru.

2.87 **RegionAlpha**

Abecedný odkaz na región v rámci špecifikovaného štátu.

RegionAlpha ::= IA5STRING(SIZE(3))

Priradenie hodnoty:

‘ ’ Nie sú k dispozícii žiadne informácie

Španielsko:

‘AN‘	Andalucía
‘AR‘	Aragón
‘AST‘	Asturias
‘C‘	Cantabria
‘CAT‘	Cataluña
‘CL‘	Castilla–León
‘CM‘	Castilla–La–Mancha
‘CV‘	Valencia
‘EXT‘	Extremadura
‘G‘	Galicia
‘IB‘	Baleares
‘IC‘	Canarias
‘LR‘	La Rioja
‘M‘	Madrid
‘MU‘	Murcia
‘NA‘	Navarra
‘PV‘	País Vasco.

2.88 **RegionNumeric**

Numerický odkaz na región v rámci špecifikovaného štátu.

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

Priradenie hodnoty:

‘00’H	Nie sú k dispozícii žiadne informácie

Španielsko:

‘01‘H	Andalucía
‘02‘H	Aragón
‘03‘H	Asturias
‘04‘H	Cantabria
‘05‘H	Cataluña
‘06‘H	Castilla–León
‘07‘H	Castilla–La–Mancha
‘08‘H	Valencia
‘09‘H	Extremadura
‘0A‘H	Galicia
‘0B‘H	Baleares
‘0C‘H	Canarias
‘0D‘H	La Rioja
‘0E‘H	Madrid
‘0F‘H	Murcia

‘10‘H Navarra

‘11‘H País Vasco.

2.89 **RSAKeyModulus**

Modul RSA kľúčového páru.

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

Priradenie hodnoty: nešpecifikované.

2.90 **RSAKeyPrivateExponent**

Súkromný exponent RSA kľúčového páru.

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

Priradenie hodnoty: nešpecifikované.

2.91 **RSAKeyPublicExponent**

Verejný exponent RSA kľúčového páru.

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

Priradenie hodnoty: nešpecifikované.

2.92 **SensorApprovalNumber**

Typové schvaľovacie číslo snímača.

SensorApprovalNumber ::= IA5String(SIZE(8))

Priradenie hodnoty: nešpecifikované.

2.93 **SensorIdentification**

Informácie uložené v snímači pohybu, ktoré sa vzťahujú k identifikácii snímača pohybu (požiadavka 077).

SensorIdentification ::= SEQUENCE {

sensorSerialNumber	SensorSerialNumber,
sensorApprovalNumber	SensorApprovalNumber,
sensorSCIdentifier	SensorSCIdentifier,
sensorOSIdentifier	SensorOSIdentifier

}

sensorSerialNumber je rozšírené sériové číslo snímača pohybu (číslo časti a kód výrobcu).

sensorApprovalNumber je schvaľovacie číslo snímača pohybu.

sensorSCIdentifier je identifikátor bezpečnostného komponentu the snímača pohybu.

sensorOSIdentifier je identifikátor operačného systému snímača pohybu.

2.94 **SensorInstallation**

Informácie uložené v snímači pohybu, ktoré sa vzťahujú k montáži snímača pohybu (požiadavka 099).

SensorInstallation ::= SEQUENCE {

sensorPairingDateFirst	SensorPairingDate,
firstVuApprovalNumber	VuApprovalNumber,
firstVuSerialNumber	VuSerialNumber,
sensorPairingDateCurrent	SensorPairingDate,

currentVuApprovalNumber VuApprovalNumber,

currentVUSerialNumber VuSerialNumber

}

sensorPairingDateFirst je dátum prvého spárovania snímača pohybu s jednotkou vozidla.

firstVuApprovalNumber je schvaľovacie číslo prvej jednotky vozidla spárovanej so snímačom pohybu.

firstVuSerialNumber je sériové číslo prvej jednotky vozidla spárovanej so snímačom pohybu.

sensorPairingDateCurrent je dátum súčasného spárovania snímača pohybu s jednotkou vozidla.

currentVuApprovalNumber je schvaľovacie číslo jednotky vozidla v súčasnosti spárovanej so snímačom pohybu.

currentVUSerialNumber je sériové číslo jednotky vozidla v súčasnosti spárovanej so snímačom pohybu.

2.95 **SensorInstallationSecData**

Informácie uložené na dielenskej karte, ktoré sa vzťahujú k bezpečnostným dátam potrebným na spárovanie snímačov pohybu s jednotkami vozidla (požiadavka 214).

SensorInstallationSecData ::= TDesSessionKey

Priradenie hodnoty: v súlade s ISO 16844–3.

2.96 **SensorOSIdentifier**

Identifikátor operačného systému snímača pohybu

SensorOSIdentifier ::= IA5String(SIZE(2))

Priradenie hodnoty: špecifické podľa výrobcu.

2.97 **SensorPaired**

Informácie uložené v jednotke vozidla, vzťahujúce sa k identifikácii snímača pohybu spárovaného s jednotkou vozidla (požiadavka 079).

SensorPaired ::= SEQUENCE {

sensorSerialNumber SensorSerialNumber,

sensorApprovalNumber SensorApprovalNumber,

sensorPairingDateFirst S ensorPairingDate

}

sensorSerialNumber je sériové číslo snímača pohybu spárovaného v súčasnosti s jednotkou vozidla.

sensorApprovalNumber je schvaľovacie snímača pohybu spárovaného v súčasnosti s jednotkou vozidla.

sensorPairingDateFirst je dátum prvého spárovania snímača pohybu s jednotkou vozidla, ktorý je v súčasnosti spárovaný s jednotkou vozidla

2.98 **SensorPairingDate**

Dátum spárovania snímača pohybu s jednotkou vozidla

SensorPairingDate ::= TimeReal

Priradenie hodnoty: nešpecifikované.

2.99 **SensorSerialNumber**

Sériové číslo snímača pohybu.

SensorSerialNumber ::= ExtendedSerialNumber:

2.100 **SensorSCIdentifier**

Identifikátor bezpečnostného komponentu snímača pohybu.

SensorSCIdentifier ::= IA5String(SIZE(8))

Priradenie hodnoty: špecifické podľa výrobcu komponentu.

2.101 **Signature**

Digitálny podpis.

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

Priradenie hodnoty: v súlade s doplnkom 11, „Spoločný bezpečnostný mechanizmus“.

2.102 **SimilarEventsNumber**

Počet podobných udalosti v jednom určitom dni (požiadavka 094).

SimilarEventsNumber ::= INTEGER(0..255)

Priradenie hodnoty: 0 sa nepoužíva, 1 znamená, že v uvedenom dni nastala len jedna udalosť daného typu, 2 znamená, že v uvedenom dni nastali dve udalosti daného typu (len jedna bola uložená), … 255 znamená, že v uvedenom dni nastalo 255 alebo viac udalostí.

2.103 **SpecificConditionType**

Kód identifikujúci špecifickú podmienku (požiadavky 050b, 105a, 212a a 230a).

SpecificConditionType ::= INTEGER(0..255)

Priradenie hodnoty:

‘00’H	RFU
‘01‘H	Záznamové zariadenie sa nevyžaduje – začiatok
‘02‘H	Záznamové zariadenie sa nevyžaduje – koniec
‘03‘H	jazda prevoznej lode/vlaku
‘04‘H .. ‘FF‘H	RFU.

2.104 **SpecificConditionRecord**

Informácie uložené na karte vodiča, dielenskej karte alebo jednotke vozidla, ktoré sa vzťahujú k špecifickej podmienke (požiadavky 105a, 212a a 230a).

SpecificConditionRecord ::= SEQUENCE {

entryTime	TimeReal,
specificConditionType	SpecificConditionType

}

entryTime je dátum a čas zápisu.

specificConditionType je kód identifikujúci špecifickú podmienku.

2.105 **Speed**

Rýchlosť vozidla (km/h).

Speed ::= INTEGER(0..255)

Priradenie hodnoty: kilometre za hodinu v prevádzkovom rozsahu od 0 do 220 km/h.

2.106 **SpeedAuthorised**

Maximálna povolená rýchlosť vozidla (definícia bb)).

SpeedAuthorised ::= Speed.

2.107 **SpeedAverage**

Priemerná rýchlosť vo vopred stanovenom časovom úseku (km/h).

SpeedAverage ::= Speed.

2.108 **SpeedMax**

Maximálna rýchlosť vo vopred stanovenom časovom úseku.

SpeedMax ::= Speed.

2.109 **TDesSessionKey**

Trojnásobný DES relačný kľúč.

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

Priradenie hodnoty: nie je bližšie špecifikované.

2.110 **TimeReal**

Kód pre kombinované pole dátum a čas, kde sú dátum a čas vyjadrené ako sekundy po 1. januári 1970 00h.00m.00s. GMT.

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

Priradenie hodnoty – Usporiadaný oktet: počet sekúnd od polnoci 1. januára 1970 GMT.

Maximálny možný dátum/čas je rok 2106.

2.111 **TyreSize**

Označenie rozmerov pneumatík.

TyreSize ::= IA5String(SIZE(15))

Priradenie hodnoty: v súlade so smernicou (EHS) 92/23 31.3.1992, Ú. v. ES L 129, s. 95.

2.112 **VehicleIdentificationNumber**

Identifikačné číslo vozidla (VIN) vzťahujúce sa k vozidlu ako celku,, spravidla sériové číslo podvozku alebo rámu.

VehicleIdentificationNumber ::= IA5String(SIZE(17))

Priradenie hodnoty: definované v ISO 3779.

2.113 **VehicleRegistrationIdentification**

Identifikácia vozidla, jednoznačná pre Európu (registračné číslo vozidla a členský štát).

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

vehicleRegistrationNation je štát, v ktorom je vozidlo zaregistrované.

vehicleRegistrationNumber je registračné číslo vozidla (VRN).

2.114 **VehicleRegistrationNumber**

Registračné číslo vozidla (VRN). Registračné číslo, ktoré vozidlu pridelil oprávnený orgán.

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

codePage špecifikuje časť ISO/IEC 8859 používaná na kódovanie vehicleRegNumber,

vehicleRegNumber je VRN kódované v súlade s ISO/IEC 8859–codePage.

Priradenie hodnoty: špecifické podľa štátu.

2.115 **VuActivityDailyData**

Informácie uložené v jednotke vozidla, vzťahujúce sa k zmenám činnosti a/alebo zmenám stavu vedenia a/alebo zmenám stavu karty v danom kalendárnom dni (požiadavka 084) a k stavu slotov o 00.00 h daného dňa.

VuActivityDailyData ::= SEQUENCE {

noOfActivityChanges	INTEGER SIZE(0..1440),
activityChangeInfos	SET SIZE(noOfActivityChanges) OF ActivityChangeInfo

}

noOfActivityChanges je počet slov ActivityChangeInfo v súbore activityChangeInfos.

activityChangeInfos je súbor slov ActivityChangeInfo uložených v jednotke vozidla za deň. Vždy obsahuje dve slová ActivityChangeInfo udávajúce stav dvoch slotov o 00.00 h daného dňa.

2.116 **VuApprovalNumber**

Typové schvaľovacie číslo jednotky vozidla.

VuApprovalNumber ::= IA5String(SIZE(8))

Priradenie hodnoty: nešpecifikované.

2.117 **VuCalibrationData**

Informácie uložené v jednotke vozidla, vzťahujúce sa ku kalibráciám záznamového zariadenia (požiadavka 098).

VuCalibrationData ::= SEQUENCE {

noOfVuCalibrationRecords	INTEGER(0..255),
vuCalibrationRecords	SET SIZE(noOfVuCalibrationRecords) OF VuCalibrationRecord

}

noOfVuCalibrationRecords je počet záznamov obsiahnutých v súbore vuCalibrationRecords.

vuCalibrationRecords je súbor záznamov o kalibrácii.

2.118 **VuCalibrationRecord**

Informácie uložené v jednotke vozidla, vzťahujúce sa ku kalibrácii záznamového zariadenia (požiadavka 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 kalibrácie.

workshopName, **workshopAddress** je názov a adresa dielne.

workshopCardNumber identifikuje dielenskú kartu použitú počas kalibrácie.

workshopCardExpiryDate dátum skončenia platnosti karty.

vehicleIdentificationNumber je VIN.

vehicleRegistrationIdentification obsahuje VRN a registrujúci členský štát.

wVehicleCharacteristicConstant je charakteristický koeficient vozidla.

kConstantOfRecordingEquipment je konštanta záznamového zariadenia.

lTyreCircumference účinný obvod pneumatík kolies.

tyreSize je označenie rozmerov pneumatík montovaných na vozidlo.

authorisedSpeed povolená rýchlosť vozidla.

oldOdometerValue, **newOdometerValue** sú staré a nové hodnoty počítadla kilometrov.

oldTimeValue, **newTimeValue** sú staré a nové hodnoty dátumu a času.

nextCalibrationDate je dátum budúcej kalibrácie typu špecifikovaného v CalibrationPurpose, ktorú má vykonať oprávnený kontrolný orgán.

2.119 **VuCardIWData**

Informácie uložené v jednotke vozidla, vzťahujúce sa k cyklom vloženia a vytiahnutia kariet vodiča alebo dielenských kariet do a z jednotky vozidla (požiadavka 081).

VuCardIWData ::= SEQUENCE {

noOfIWRecords	INTEGER(0..216–1),
vuCardIWRecords SET	SIZE(noOfIWRecords) OF VuCardIWRecord

}

noOfIWRecords je počet záznamov v súbore vuCardIWRecords.

vuCardIWRecords je súbor záznamov vzťahujúcich sa k cyklom vloženia a vytiahnutia karty.

2.120 **VuCardIWRecord**

Informácie uložené v jednotke vozidla, vzťahujúce sa k cyklom vloženia a vytiahnutia karty vodiča alebo dielenskej karty do a z jednotky vozidla (požiadavka 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 priezvisko a meno(á) držiteľa karty vodiča alebo dielenskej karty, uložené na karte.

fullCardNumber je typ karty, členský štát, ktorý ju vydal a číslo karty uložené na karte.

cardExpiryDate je dátum skončenia platnosti uložený na karte.

cardInsertionTime je dátum a čas vloženia.

vehicleOdometerValueAtInsertion stav kilometrov vozidla pri vložení karty.

cardSlotNumber je slot, v ktorom je karta vložená.

cardWithdrawalTime je dátum a čas vytiahnutia.

vehicleOdometerValueAtWithdrawal stav kilometrov vozidla pri vytiahnutí karty.

previousVehicleInfo obsahuje informácie o predchádzajúcom vozidle, ktoré vodič použil, uložené na karte.

manualInputFlag je kód udávajúci, že držiteľ karty manuálne zapísal činnosti vodiča pri vložení karty.

2.121 **VuCertificate**

Osvedčenie verejného kľúča jednotky vozidla.

VuCertificate ::= Certificate

2.122 **VuCompanyLocksData**

Informácie uložené v jednotke vozidla, vzťahujúce sa k podnikovým blokovaniam (požiadavka 104).

VuCompanyLocksData ::= SEQUENCE {

noOfLocks	INTEGER(0..20),
vuCompanyLocksRecords	SET SIZE(noOfLocks) OF VuCompanyLocksRecord

}

noOfLocks je počet blokovaní uvedených v vuCompanyLocksRecords.

vuCompanyLocksRecords je súbor záznamov o podnikových blokovaniach.

2.123 **VuCompanyLocksRecord**

Informácie uložené v jednotke vozidla, vzťahujúce sa k jednému podnikovému blokovaniu (požiadavka 104).

VuCompanyLocksRecord ::= SEQUENCE {

lockInTime	TimeReal,
lockOutTime	TimeReal,
companyName	Name,
companyAddress	Address,
companyCardNumber	FullCardNumber

}

lockInTime, **lockOutTime** sú dátum a čas zablokovania a odblokovania.

companyName, **companyAddress** sú názov a adresa podniku, na ktorý sa zablokovanie vzťahuje.

companyCardNumber identifikuje kartu použitú pri zablokovaní.

2.124 **VuControlActivityData**

Informácie uložené v jednotke vozidla, vzťahujúce sa ku kontrolám vykonaným s použitím tejto JV (požiadavka 102).

VuControlActivityData ::= SEQUENCE {

noOfControls	INTEGER(0..20),
vuControlActivityRecords	SET SIZE(noOfControls) OF VuControlActivityRecord

}

noOfControls je počet kontrol uvedených v vuControlActivityRecords.

vuControlActivityRecords je súbor záznamov o kontrolnej činnosti.

2.125 **VuControlActivityRecord**

Informácie uložené v jednotke vozidla, vzťahujúce sa ku kontrole vykonanej s použitím tejto JV (požiadavka 102).

VuControlActivityRecord ::= SEQUENCE {

controlType	ControlType,
controlTime	TimeReal,
controlCardNumber	FullCardNumber,

downloadPeriodBeginTime	TimeReal,
downloadPeriodEndTime	TimeReal

}

controlType je typ kontroly.

controlTime je dátum a čas kontroly.

ControlCardNumber identifikuje kontrolnú kartu použitú pri kontrole.

downloadPeriodBeginTime je čas začiatku časového úseku sťahovania v prípade sťahovania.

downloadPeriodEndTime je čas skončenia časového úseku sťahovania v prípade sťahovania.

2.126 **VuDataBlockCounter**

Počítadlo uložené na karte, identifikujúce postupne cykly vloženia a vytiahnutia karty do a z jednotiek vozidla.

VuDataBlockCounter ::= BCDString(SIZE(2))

Priradenie hodnoty: postupné čísla s maximálnou hodnotou = 9999, začínajúc opäť s 0.

2.127 **VuDetailedSpeedBlock**

Informácie uložené v jednotke vozidla, vzťahujúce sa k presnej rýchlosti vozidla za minútu, počas ktorej sa vozidlo pohybuje (požiadavka 093).

VuDetailedSpeedBlock ::= SEQUENCE {

speedBlockBeginDate	TimeReal,
speedsPerSecond	SEQUENCE SIZE(60) OF Speed

}

speedBlockBeginDate je dátum a čas prvej hodnoty rýchlosti v rámci bloku.

speedsPerSecond je chronologické poradie rýchlostí meraných každú sekundu v rámci minúty, začínajúc pri speedBlockBeginDate (vrátane).

2.128 **VuDetailedSpeedData**

Informácie uložené v jednotke vozidla, vzťahujúce sa k presnej rýchlosti vozidla

VuDetailedSpeedData ::= SEQUENCE

noOfSpeedBlocks	INTEGER(0.2^{16}–1),
vuDetailedSpeedBlocks	SET SIZE(noOfSpeedBlocks) OF VuDetailedSpeedBlock

}

noOfSpeedBlocks je počet blokov rýchlostí v súbore vuDetailedSpeedBlocks.

vuDetailedSpeedBlocks je súbor blokov presných rýchlostí.

2.129 **VuDownloadablePeriod**

Najstaršie alebo najnovšie dátumy, za ktoré jednotka vozidla uchováva dáta vzťahujúce sa k činnostiam vodiča (požiadavky 081, 084 alebo 087).

VuDownloadablePeriod ::= SEQUENCE {

minDownloadableTime	TimeReal
maxDownloadableTime	TimeReal

}

minDownloadableTime je najstarší dátum a čas vloženia karty alebo zmeny činnosti alebo zápisu miesta, uložený v JV.

maxDownloadableTime je posledný dátum a čas vloženia karty alebo zmeny činnosti alebo zápisu miesta, uložený v JV.

2.130 **VuDownloadActivityData**

Informácie uložené v jednotke vozidla, vzťahujúce sa k jej poslednému stiahnutiu (požiadavka 105).

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

downloadingTime je dátum a čas stiahnutia.

fullCardNumber identifikuje kartu použitú oprávňujúcu stiahnutie.

companyOrWorkshopName je názov podniku alebo dielne.

2.131 **VuEventData**

Informácie uložené v jednotke vozidla, vzťahujúce sa k udalostiam (požiadavka 094, okrem udalosti prekročenia rýchlosti).

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

noOfVuEvents je počet udalostí uvedených v súbore vuEventRecords.

vuEventRecords je súbor záznamov o udalostiach.

2.132 **VuEventRecord**

Informácie uložené v jednotke vozidla, vzťahujúce sa k udalosti (požiadavka 094, okrem udalosti prekročenia rýchlosti).

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

eventType je typ udalosti.

eventRecordPurpose je účel, pre ktorý bola táto udalosť zaznamenaná.

eventBeginTime je dátum a čas začiatku udalosti.

eventEndTime je dátum a čas skončenia udalosti.

cardNumberDriverSlotBegin identifikuje kartu vloženú v slote vodiča na začiatku udalosti.

cardNumberCodriverSlotBegin identifikuje kartu vloženú v slote druhého vodiča na začiatku udalosti.

cardNumberDriverSlotEnd identifikuje kartu vloženú v slote vodiča na konci udalosti.

cardNumberCodriverSlotEnd identifikuje kartu vloženú v slote druhého vodiča na konci udalosti.

similarEventsNumber je počet podobných udalostí v tomto dni.

Toto poradie sa môže použiť pre všetky udalosti, okrem udalostí prekročenia rýchlosti.

2.133 **VuFaultData**

Informácie uložené v jednotke vozidla, vzťahujúce sa k poruchám (požiadavka 096).

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

noOfVuFaults je počet porúch uvedených v súbore vuFaultRecords.

vuFaultRecords je súbor záznamov o poruchách.

2.134 **VuFaultRecord**

Informácie uložené v jednotke vozidla, vzťahujúce sa k poruche (požiadavka 096).

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

faultType je typ poruchy záznamového zariadenia.

faultRecordPurpose je účel, pre ktorý bola táto porucha zaznamenaná.

faultBeginTime je dátum a čas začiatku poruchy.

faultEndTime je dátum a čas skončenia poruchy.

cardNumberDriverSlotBegin identifikuje kartu vloženú v slote vodiča na začiatku poruchy.

cardNumberCodriverSlotBegin identifikuje kartu vloženú v slote druhého vodiča na začiatku poruchy.

cardNumberDriverSlotEnd identifikuje kartu vloženú v slote vodiča na konci poruchy.

cardNumberCodriverSlotEnd identifikuje kartu vloženú v slote druhého vodiča na konci poruchy.

2.135 **VuIdentification**

Informácie uložené v jednotke vozidla, vzťahujúce sa k identifikácii jednotky vozidla (požiadavka 075).

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

vuManufacturerName je názov výrobcu jednotky vozidla.

vuManufacturerAddress je adresa výrobcu jednotky vozidla.

vuPartNumber je číslo časti jednotky vozidla.

vuSerialNumber je sériové číslo jednotky vozidla.

vuSoftwareIdentification identifikuje software implementovaný v jednotke vozidla.

vuManufacturingDate je dátum výroby jednotky vozidla.

vuApprovalNumber je typové schvaľovacie číslo jednotky vozidla.

2.136 **VuManufacturerAddress**

Adresa výrobcu jednotky vozidla.

VuManufacturerAddress ::= Address

Priradenie hodnoty: nešpecifikované.

2.137 **VuManufacturerName**

Názov výrobcu jednotky vozidla.

VuManufacturerName ::= Name

Priradenie hodnoty: nešpecifikované.

2.138 **VuManufacturingDate**

Dátum výroby jednotky vozidla.

VuManufacturingDate ::= TimeReal

Priradenie hodnoty: nešpecifikované.

2.139 **VuOverSpeedingControlData**

Informácie uložené v jednotke vozidla, vzťahujúce sa k udalostiam prekročenia rýchlosti od poslednej kontroly prekročenia rýchlosti (požiadavka 095).

VuOverSpeedingControlData ::= SEQUENCE {

lastOverspeedControlTime	TimeReal,
firstOverspeedSince	TimeReal,
numberOfOverspeedSince	OverspeedNumber

}

lastOverspeedControlTime je dátum a čas poslednej kontroly prekročenia rýchlosti.

firstOverspeedSince je dátum a čas prvej kontroly prekročenia rýchlosti nasledujúcej po tejto kontrole prekročenia rýchlosti.

numberOfOverspeedSince je počet udalostí prekročenia rýchlosti od poslednej kontroly prekročenia rýchlosti

2.140 **VuOverSpeedingEventData**

Informácie uložené v jednotke vozidla, vzťahujúce sa k udalostiam prekročenia rýchlosti (požiadavka 094).

VuOverSpeedingEventData ::= SEQUENCE {

noOfVuOverSpeedingEvents	INTEGER(0..255),
vuOverSpeedingEventRecords	SET SIZE(noOfVuOverSpeedingEvents) OF VuOverSpeedingEventRecord

}

noOfVuOverSpeedingEvents je počet udalostí uvedený v súbore vuOverSpeedingEventRecords.

vuOverSpeedingEventRecords je súbor záznamov o udalostiach prekročenia rýchlosti.

2.141 **VuOverSpeedingEventRecord**

Informácie uložené v jednotke vozidla, vzťahujúce sa k udalostiam prekročenia rýchlosti (požiadavka 094).

VuOverSpeedingEventRecord ::= SEQUENCE {

eventType	EventFaultType,
eventRecordPurpose	EventFaultRecordPurpose,
eventBeginTime	TimeReal,
eventEndTime	TimeReal,
maxSpeedValue	SpeedMax,
averageSpeedValue	SpeedAverage,
cardNumberDriverSlotBegin	FullCardNumber,
similarEventsNumber	SimilarEventsNumber

}

eventType je typ udalosti.

eventRecordPurpose je účel, pre ktorý bola táto udalosť zaznamenaná.

eventBeginTime je dátum a čas začiatku udalosti.

eventEndTime je dátum a čas skončenia udalosti.

maxSpeedValue je maximálna rýchlosť nameraná počas udalosti.

averageSpeedValue je aritmeticky priemerná rýchlosť nameraná počas udalosti.

cardNumberDriverSlotBegin identifikuje kartu vloženú v slote druhého vodiča na začiatku udalosti.

similarEventsNumber je počet podobných udalostí v tomto dni.

2.142 **VuPartNumber**

Číslo časti jednotky vozidla.

VuPartNumber ::= IA5String(SIZE(16))

Priradenie hodnoty: špecifické podľa výrobcu JV.

2.143 **VuPlaceDailyWorkPeriodData**

Informácie uložené v jednotke vozidla, vzťahujúce sa k miestam, kde vodiči začínajú a končia denný pracovný čas (požiadavka 087)

VuPlaceDailyWorkPeriodData ::= SEQUENCE {

noOfPlaceRecords	INTEGER(0..255),
vuPlaceDailyWorkPeriodRecords	SET SIZE(noOfPlaceRecords) OF VuPlaceDailyWorkPeriodRecord

}

noOfPlaceRecords je počet záznamov uvedených v súbore vuPlaceDailyWorkPeriodRecords.

vuPlaceDailyWorkPeriodRecords je súbor záznamov vzťahujúcich sa k miestu.

2.144 **VuPlaceDailyWorkPeriodRecord**

Informácie uložené v jednotke vozidla, vzťahujúce sa k miestu, kde vodič začína a končí denný pracovný čas (požiadavka 087).

VuPlaceDailyWorkPeriodRecord ::= SEQUENCE {

fullCardNumber	FullCardNumber,
placeRecord	PlaceRecord

}

fullCardNumber je typ karty vodiča, členský štát, ktorý kartu vydal a číslo karty.

placeRecord obsahuje informácie vzťahujúce sa k zapísaným miestam.

2.145 **VuPrivateKey**

Súkromný kľúč jednotky vozidla.

VuPrivateKey ::= RSAKeyPrivateExponent

2.146 **VuPublicKey**

Verejný kľúč jednotky vozidla.

VuPublicKey ::= PublicKey

2.147 **VuSerialNumber**

Sériové číslo jednotky vozidla (požiadavka 075).

VuSerialNumber ::= ExtendedSerialNumber

2.148 **VuSoftInstallationDate**

Dátum inštalovania softwarovej verzie jednotky vozidla.

VuSoftInstallationDate ::= TimeReal

Priradenie hodnoty: nešpecifikované.

2.149 **VuSoftwareIdentification**

Informácie uložené v jednotke vozidla, vzťahujúce sa k inštalovanému softwaru.

VuSoftwareIdentification ::= SEQUENCE {

vuSoftwareVersion	VuSoftwareVersion,
vuSoftInstallationDate	VuSoftInstallationDate

}

vuSoftwareVersion číslo softwarovej verzie jednotky vozidla.

vuSoftInstallationDate je dátum inštalovania softwarovej verzie jednotky vozidla.

2.150 **VuSoftwareVersion**

Číslo softwarovej verzie jednotky vozidla.

VuSoftwareVersion ::= IA5String(SIZE(4))

Priradenie hodnoty: nešpecifikované.

2.151 **VuSpecificConditionData**

Informácie uložené v jednotke vozidla, ktoré sa vzťahujú k špecifickým podmienkam.

VuSpecificConditionData ::= SEQUENCE {

noOfSpecificConditionRecords	INTEGER(0..2^{16}–1)
specificConditionRecords	SET SIZE (noOfSpecificConditionRecords) OF SpecificConditionRecord

}

noOfSpecificConditionRecords je počet záznamov uvedených v súbore specificConditionRecords.

specificConditionRecords súbor záznamov vzťahujúcich sa k špecifickým podmienkam.

2.152 **VuTimeAdjustmentData**

Informácie uložené v jednotke vozidla, vzťahujúce sa k nastaveniam času, vykonaným mimo rámca pravidelnej kalibrácie (požiadavka 101).

VuTimeAdjustmentData ::= SEQUENCE {

noOfVuTimeAdjRecords	INTEGER(0..6),
vuTimeAdjustmentRecords	SET SIZE(noOfVuTimeAdjRecords) OF VuTimeAdjustmentRecords

}

noOfVuTimeAdjRecords je počet záznamov v vuTimeAdjustmentRecords.

vuTimeAdjustmentRecords je súbor záznamov nastavenia času.

2.153 **VuTimeAdjustmentRecord**

Informácie uložené v jednotke vozidla, vzťahujúce sa k nastaveniu času, vykonanému mimo rámca pravidelnej kalibrácie (požiadavka 101).

VuTimeAdjustmentRecord ::= SEQUENCE {

oldTimeValue	TimeReal,
oldTimeValue	TimeReal,
newTimeValue	TimeReal,
workshopName	Name,
workshopAddress	Address,
workshopCardNumber	FullCardNumber

}

oldTimeValue, **newTimeValue** sú staré a nové hodnoty dátumu a času.

workshopName, **workshopAddress** je názov a adresa podniku.

workshopCardNumber identifikuje dielenskú kartu použitú na vykonanie nastavenia času.

2.154 **W–VehicleCharacteristicConstant**

Charakteristický koeficient vozidla (definícia (k)).

W–VehicleCharacteristicConstant ::= INTEGER(0..2^{16}–1))

Priradenie hodnoty: Impulzy na kilometer v prevádzkovom rozsahu 0 až 64 255 impulzov/km.

2.155 **WorkshopCardApplicationIdentification**

Informácie uložené na dielenskej karte, vzťahujúce sa k identifikácii aplikácie karty (požiadavka 190).

WorkshopCardApplicationIdentification ::= SEQUENCE {

typeOfTachographCardId	EquipmentType,
cardStructureVersion	CardStructureVersion,
noOfEventsPerType	NoOfEventsPerType,
noOfFaultsPerType	NoOfFaultsPerType,
activityStructureLength	CardActivityLengthRange,
noOfCardVehicleRecords	NoOfCardVehicleRecords,
noOfCardPlaceRecords	NoOfCardPlaceRecords,
noOfCalibrationRecords	NoOfCalibrationRecords

}

typeOfTachographCardId špecifikuje implementovaný typ karty.

cardStructureVersion špecifikuje verziu štruktúry, ktorá je implementovaná v karte.

noOfEventsPerType je počet udalostí podľa typu udalosti, ktoré sa môžu na karte zaznamenať.

noOfFaultsPerType je počet porúch podľa typu poruchy, ktoré sa môžu na karte zaznamenať.

activityStructureLength udáva počet bajtov, ktoré sú k dispozícii na uloženie záznamov o činnosti.

noOfCardVehicleRecords je počet záznamov o vozidle, ktoré môže karta obsahovať.

noOfCardPlaceRecords je počet miest, ktoré sa môžu na karte zaznamenať.

noOfCalibrationRecords je počet záznamov o kalibrácii, ktoré sa môžu na karte uložiť.

2.156 **WorkshopCardCalibrationData**

Informácie uložené na dielenskej karte, ktoré sa vzťahujú k dielenskej činnosti vykonanej s kartou (požiadavky 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 kalibrácií vykonaných s kartou.

calibrationPointerNewestRecord je index naposledy aktualizovaného záznamu o kalibrácii.

Priradenie hodnoty: počet zodpovedajúci počítadlu záznamov o kalibrácii, začínajúci od „0“ pre prvý výskyt záznamov o kalibrácii v štruktúre.

calibrationRecords je súbor záznamov obsahujúcich informácie o kalibrácii a a/alebo nastavení času.

2.157 **WorkshopCardCalibrationRecord**

Informácie uložené na dielenskej karte, ktoré sa vzťahujú ku kalibrácii vykonanej s kartou (požiadavka 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 kalibrácie.

vehicleIdentificationNumber je VIN.

vehicleRegistration obsahuje VRN a registrujúci členský štát.

wVehicleCharacteristicConstant je charakteristický koeficient vozidla.

kConstantOfRecordingEquipment je konštanta záznamového zariadenia.

lTyreCircumference je účinný obvod pneumatík kolies.

tyreSize je označenie rozmerov pneumatík montovaných na vozidlo.

authorisedSpeed je maximálna povolená rýchlosť vozidla.

oldOdometerValue, **newOdometerValue** sú staré a nové hodnoty počítadla kilometrov.

oldTimeValue, **newTimeValue** sú staré a nové dátumu a času.

nextCalibrationDate je dátum budúcej kalibrácie typu špecifikovaného v CalibrationPurpose, ktorú má vykonať oprávnený kontrolný orgán.

vuPartNumber, **vuSerialNumber** and s**ensorSerialNumber** sú dáta prvkov na identifikáciu záznamového zariadenia.

2.158 **WorkshopCardHolderIdentification**

Informácie uložené na dielenskej karte, vzťahujúce sa k identifikácii držiteľa karty (požiadavka 216).

WorkshopCardHolderIdentification ::= SEQUENCE {

workshopName	Name,
workshopAddress	Address,
cardHolderName	HolderName,
cardHolderPreferredLanguage	Language

}

workshopName je názov dielne držiteľa karty.

workshopAddress je adresa dielne držiteľa karty.

cardHolderName je priezvisko a meno(á) držiteľa (napr. meno mechanika).

cardHolderPreferredLanguage je uprednostnený jazyk držiteľa karty.

2.159 **WorkshopCardPIN**

Osobné identifikačné číslo dielenskej karty (požiadavka 213).

WorkshopCardPIN ::= IA5String(SIZE(8))

Priradenie hodnoty: PIN kód známy držiteľovi karty, vyplnený doprava s „FF“ bajtami až do 8 bajtov.

3. DEFINÍCIE PRE ROZSAH HODNÔT A ROZMEROV

Definície premenných hodnôt použitých na definície v odseku 2.

TimeRealRange ::= 2^{32}–1

3.1 **Definície pre kartu vodiča**

Názov premennej hodnoty	Minimum	Maximum
CardActivityLengthRange	5 544 bajtov (28 dní 93 zmien činnosti za deň)	13 776 bajtov (28 dní 240 zmien činnosti za deň)
NoOfCardPlaceRecords	84	112
NoOfCardVehicleRecords	84	200
NoOfEventsPerType	6	12
NoOfFaultsPerType	12	24

3.2 **Definície pre dielenskú kartu**

Názov premennej hodnoty	Minimum	Maximum
CardActivityLengthRange	198 bajtov (1 deň 93 zmien činnosti)	492 bajtov (1 deň 240 zmien činnosti)
NoOfCardPlaceRecords	6	8
NoOfCardVehicleRecords	4	8
NoOfEventsPerType	3	3
NoOfFaultsPerType	6	6
NoOfCalibrationRecords	88	255

3.3 **Definície pre kontrolnú kartu**

Názov premennej hodnoty	Minimum	Maximum
NoOfControlActivityRecords	230	520

3.2 **Definície pre podnikovú kartu**

Názov premennej hodnoty	Minimum	Maximum
NoOfCompanyActivityRecords	230	520

4. SÚBORY ZNAKOV

V IA5Strings sú použité znaky ASCII definované v ISO/IEC 8824–1. Z dôvodov čitateľnosti a odkazov je priradenie hodnoty uvedené nižšie. V prípade nezhody s týmito, na informačné účely uvedenými informáciami, platí vždy ISO/IEC 8824–1.

! " # $ % & ' ( ) * + , – . / 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 { | } ~

Iné reťazce znakov (adresa, meno, registračné číslo vozidla) používajú okrem toho znaky definované kódmi 192 až 255 ISO/IEC 8859–1 (Latinský súbor znakov) alebo ISO/IEC 8859–7 (Grécky súbor znakov).

5. KÓDOVANIE

Pri kódovaní podľa kódovacích pravidiel ASN.1, všetky definované typy dát sa kódujú podľa ISO/IEC 8825–2, usporiadaný variant.

Doplnok 2

ŠPECIFIKÁCIA TACHOGRAFOVÝCH KARIET

Obsah

1. ÚVOD

1.1 **Skratky**

Na účely tohto doplnku platia tieto skratky:

AC	access conditions (prístupové podmienky)
AID	application identifier (identifikátor aplikácie)
ALW	always (vždy)
APDU	application protocol data unit (structure of a command) (štruktúra príkazov)
ATR	answer to reset (odpoveď na resetovanie)
AUT	authenticated (overené)
C6, C7	kontakty č. 6 a 7 karty popísané v ISO/IEC 7816–2
cc	clock cycles (cykly hodinových impulzov)
CHV	card holder verification information (informácie overujúce držiteľa karty)
CLA	bajty triedy APDU príkazov
DF	vyhradený súbor. DF môže obsahovať iné súbory (EF or DF)
EF	elementary file (elementárny súbor)
ENC	zakódované: prístup je možný len cez kódovacie dáta
etu	elementary time unit (elementárna časová jednotka)
IC	integrated circuit (integrovaný obvod)
ICC	integrated circuit card (karta s integrovaným obvodom)
ID	identifier (identifikátor)
IFD	interface device (prepojovacie zariadenie)
IFS	information field size (veľkosť informačného poľa)
IFSC	information field size for the card (veľkosť informačného poľa karty)
IFSD	information field size device (for the terminal) (veľkosť informačného poľa zariadenia) (pre koncové zariadenie)
INS	instruction byte of an APDU command (príkazový bajt pre príkaz APDU)
Lc	length of the input data for a APDU command (dĺžka vstupných dát pre príkaz APDU)
Le	length of the expected data (output data for a command) (dĺžka predpokladaných dát) (výstupné dáta pre príkaz)
MF	master file (root DF) (koreň DF)
P1–P2	parameter bytes (parametrické bajty)
NAD	node address used in T=1 protocol (uzlová adresa používaná v T=1)
NEV	never (nikdy)
PIN	personal identification number (osobné identifikačné číslo)
PRO SM	protected with secure messaging (chránené s secure messaging)
PTS	protocol transmission selection (voľba prenosu protokolu)
RFU	reserved for future use (vyhradené pre budúce použitie)
RST	reset (of the card) (resetovanie (karty))

SM	secure messaging
SW1–SW2	status bytes (stavové bajty)
TS	initial ATR character (počiatočný znak ATR)
VPP	programming voltage (programové napätie)
XXh	value XX in hexadecimal notation (hodnota XX v hexadecimálnej notácii)
||	concatenation symbol 03||04=0304 (symbol zreťazenia 03||04=0304).

1.2 **Referenčné dokumenty**

V tomto doplnku sú použité tieto referenčné dokumenty::

EN 726–3	Identification cards systems – Telecommunications integrated circuit(s) cards and terminals – Part 3: Application independent card requirements. December 1994 (Systémy identifikačných kariet – telekomunikačné karty s integrovanými obvodmi a koncové zariadenia – Časť 3 – Požiadavky na karty nezávislé na aplikácii. December 1994)
ISO/IEC 7816–2	Information technology – Identification cards – Integrated circuit(s) cards with contacts – Part 2: Dimensions and location of the contacts. First edition: 1999 (Informačné technológie – Identifikačné karty – Karty s integrovanými obvodmi a s kontaktmi – Časť 2: Rozmery a umiestnenie kontaktov. Prvé vydanie: 1999).
ISO/IEC 7816–3	Information technology – Identification cards – Integrated circuit(s) cards with contacts – Part 3: Electronic signals and transmission protocol. Edition 2: 1997 (Informačné technológie – Identifikačné karty – Karty s integrovanými obvodmi a s kontaktmi – Časť 3: Elektronické signály a protokoly procesu. Vydanie 2: 1997).
ISO/IEC 7816–4	Information technology – Identification cards – Integrated circuit(s) cards with contacts – Part 4: Interindustry commands for interexchange. First edition: 1995 + Amendment 1: 1997 (Informačné technológie – Identifikačné karty – Karty s integrovanými obvodmi a s kontaktmi – Časť 4: Medziodborové príkazy pre výmenu. Prvé vydanie: 1995 + zmeny 1:1997).
ISO/IEC 7816–6	Information technology – Identification cards – Integrated circuit(s) cards with contacts – Part 6: Interindustry data elements. First Edition: 1996 + Cor 1: 1998 (Informačné technológie – Identifikačné karty – Karty s integrovanými obvodmi a s kontaktmi – Časť 6: Medziodborové dátové prvky. Prvé vydanie: 1996 + cor. 1:1998).
ISO/IEC 7816–8	Information technology – Identification cards – Integrated circuit(s) cards with contacts – Part 8: Security related interindustry commands. First Edition: 1999 (Informačné technológie – Identifikačné karty – Karty s integrovanými obvodmi a s kontaktmi – Časť 8: Medziodborové príkazy vzťahujúce sa k bezpečnosti. Prvé vydanie: 1999).
ISO/IEC 9797	Information technology – Security techniques – Data integrity mechanism using a cryptographic check function employing a block cipher algorithm. Edition 2: 1994 (Informačné technológie. Bezpečnostné techniky. Mechanizmus na zachovanie integrity dát s kryptovacou kontrolnou funkciou pracujúcou s blokovým šifrovacím algoritmom).

2. ELEKTRICKÉ A FYZIKÁLNE CHARAKTERISTIKY

TCS_200	Všetky elektronické signály musia byť v súlade s normou ISO/IEC 7816–3, pokiaľ nie je špecifikované inak.
TCS_201	Umiestnenie a rozmery kontaktov karty musia spĺňať požiadavky normy ISO/IEC 7816–2.

2.1 **Napájanie a spotreba prúdu**

TCS_202	Karta pracuje v súlade so špecifikáciami v rámci limitov spotreby špecifikovaných v ISO/IEC 7816–3.

TCS_203 Karta pracuje s V_{cc} = 3 V (+/– 0,3 V) alebo V_{cc} = 5 V (+/– 0,5 V).

Voľba napätia sa vykoná podľa ISO/IEC 7816–3.

2.2 **Programovacie napätie V_{pp}**

TCS_204 Karta nepotrebuje programovacie napätie pri kontakte C6. Predpokladá sa, že kontakt C6 nie je pripojený k prepojovaciemu zariadeniu (IFD). Kontakt C6 môže byť pripojený k V_{cc} v karte, ale nesmie byť pripojený na kostru. Toto napätie nesmie byť v žiadnom prípade interpretované.

2.3 **Generovanie a frekvencia hodinových impulzov**

TCS_205 Karta pracuje vo frekvenčnom rozsahu 1 až 5 Mhz. V rámci jednej relácie karty sa frekvencia taktu môže kolísať v rozsahu ±2%. Frekvencia hodinových impulzov je generovaná jednotkou vozidla a nie samotnou kartou. Pracovný cyklus sa môže meniť od 40 do 60%.

TCS_206 Za podmienok obsiahnutých v kartovom súbore EF_{ICC} sa môžu vonkajšie hodiny zastaviť. Prvý bajt hlavnej časti súboru EF_{ICC} kóduje podmienky pre režim Clockstop (pre bližšie údaje pozri EN 726–3):

Úroveň nízka	Úroveň vysoká		
Bit 3	Bit 2	Bit 1	
0	0	1	Clockstop povolené, žiadna preferenčná úroveň
0	1	1	Clockstop povolené, vysoká preferenčná úroveň
1	0	1	Clockstop povolené, nízka preferenčná úroveň
0	0	0	Clockstop nepovolené
0	1	0	Clockstop povolené len na vysokej úrovni
1	0	0	Clockstop povolené len na nízkej úrovni

Nie sú použité bity 4 až 8.

2.4 **I/O kontakt**

TCS_207 I/O kontakt C7 sa použije na príjem dát z IFD a vysielanie dát na IFD. Počas prevádzky sa nachádza karta alebo prepojovacie zariadenie vo vysielacom režime. Ak by vo vysielacom režime boli obe jednotky, karta sa nesmie poškodiť. Pokiaľ karta nie je vo vysielacom režime, nachádza sa v prijímacom režime.

2.5 **Stavy karty**

TCS_208 Pri uplatňovanom napájacom napätí pracuje karta v dvoch stavoch:

– stav prevádzky počas vykonávania príkazov alebo počas spojenia s digitálnou jednotkou,

– stav pokoja počas všetkých ostatných časov; v tomto stave sa všetky dáta uchovávajú na karte.

3. HARDWARE A VÝMENA DÁT

3.1 **Úvod**

Tento odsek popisuje minimálnu funkčnosť vyžadovanú tachografovými kartami alebo jednotkami vozidla, potrebnú na zabezpečenie správnej činnosti a interoperability.

Tachografové karty majú byť v čo možno najväčšej miere zhodné s aplikovateľnými normami ISO/IEC (hlavne s ISO/IEC 7816). Avšak príkazy a protokoly musia byť podrobne popísané aby bolo špecifikované prípadné určité obmedzené použitie alebo niektoré rozdiely. Špecifikované príkazy musia plne zodpovedať daným normám, pokiaľ nie je stanovené inak.

3.2 **Protokol procesu**

TCS_300 Protokol procesu musí spĺňať normu ISO/IEC 7816–3. JV musí rozoznať najmä predĺženia čakacej doby vysielané kartou.

3.2.1 ***Protokoly***

TCS_301 Karta podporuje protokol T=0 ako aj protokol T=1.

TCS_302 T=0 je štandardný protokol; k zmene na protokol T=1 je potrebný príkaz PTS.

TCS_303 Zariadenia podporujú „direct convention“ v oboch protokoloch; direct convention je tým pre kartu povinná.

TCS_304 Bajt pre veľkosť informačného poľa karty sa v ATR prezentuje v znaku TA3. Táto hodnota je minimálne ‘F0h’ (= 240 bajtov).

Pre protokoly platia tieto obmedzenia:

TCS_305 <u>T=0</u>

– Prepojovacie zariadenie podporuje odpoveď na I/O po stúpajúcej hrane signálu na RST od 400 cc.

– Prepojovacie zariadenie musí byť schopné čítať znaky s rozostupom 12 etu.

– Prepojovacie zariadenie musí prečítať chybný znak a jeho opakovanie, ak rozostup činí 13 etu. Ak sa zistí chybný signál, chybný signál na I/O môže nastať medzi 1 etu a 2 etu. Zariadenie podporuje oneskorenie 1 etu.

– Prepojovacie zariadenie akceptuje 33 bajtové ATR (TS+32).

– Ak je TCI prezentované v ATR, Extra Guard Time sa prezentuje pre znaky vysielané prepojovacím zariadením, hoci znaky vysielané kartou sú naďalej oddelené s rozostupom 12 etu. Toto platí aj pre znaky ACK vysielané kartou po znaku P3 vyslanom prepojovacím zariadením.

– Prepojovacie zariadenie berie do úvahy znak NUL vyslaný kartou.

– Prepojovacie zariadenie akceptuje doplnkový režim pre ACK.

– Príkaz GET RESPONSE sa nemôže použiť v režime reťazenia za účelom získania dát, ktorých dĺžka presahuje 255 bajtov.

TCS_306 T=1

– NAD byte: nepoužitý (NAD sa nastaví na ‘00’).

– S–blok ABORT: nepoužitý.

– S–blok VPP chyba stavu: nepoužitý.

– Celková dĺžka reťazenia pre dátové pole nepresiahne 255 bajtov (zabezpečené prostredníctvom IFD).

– Veľkosť informačného poľa zariadenia (IFSD) IFD ukáže ihneď po ATR; IFD prenesie S–blok IFS požiadavku po ATR a karta vyšle späť S–blok IFS. Odporúčaná hodnota pre IFSD je 254 bajtov.

– Karta nebude vyžadovať dodatočné nastavenie IFS.

3.2.2 **ATR**

TCS_307 Zariadenie kontroluje ATR bajty podľa ISO/IEC 7816–3. Na ATR historických znakoch sa nerobí žiadne overovanie.

Príklad základného biprotokolu ATR podľa ISO/IEC 7816–3

Znak	Hodnota	Poznámky
TS	‘3Bh‘	Udáva „direct convention“
T0	‘85h‘	TD1 prítomné; je prítomných 5 histo–rických bajtov
TD1	‘80h‘	TD2 prítomné; použité T=0
TD2	‘11h‘	TA3 prítomné; použité T=1
TA3	‘XXh‘ (mind. ‘F0h‘)	Veľkosť informačného poľa karty (IFSC)
TH1 bis TH5	‘XXh‘	Historické znaky
TCK	‘XXh‘	Kontrolný znak (bez OR)

TCS_308 Po odpovedi na resetovanie (znovu nastavenie) (ATR) sa implicitne zvolí hlavný súbor (MF) a stáva sa aktuálnym adresárom.

3.2.3 **PTS**

TCS_309 Štandardný protokol je T=0 Na nastavenie na protokol T=1, PTS (známy aj ako PPS) musí zariadenie poslať na kartu.

TCS_310 Oba protokoly T=0 ako aj T=1 sú pre kartu povinné, základný PTS pre prepnutie protokolu je povinný pre kartu.

PTS sa môže použiť, ako je uvedené v norme ISO/IEC 7816–3 na prepnutie na vyššie prenosové rýchlosti než prípadné štandardné rýchlosti navrhované kartou v ATR (TA3(1) bajty).

TCS_311 Ak nie je podporovaná žiadna iná rýchlosť prenosu než štandardná (alebo ak nie je zvolená rýchlosť prenosu podporovaná), karta odpovedá na PTS správne podľa ISO/IEC 7816–3 tak, že vynechá bajty PPS1.

Príklady základného PTS pre voľbu protokolu sú tieto:

Znak	Hodnota	Poznámky

PPSS	‘FFh‘	Úvodný znak	
PPSO	‘00h‘ alebo ‘01h‘	PPS1 až PPS3 nie sú prítomné; ‘00h‘ na voľbu T0, ‘01h‘ na voľbu T1	
PK	‘XXh‘	Kontrolný znak:	‘XXh‘ = ‘FFh‘ ak PPS0 = ‘00h‘ ‘XXh‘ = ‘FEh‘ ak PPS0 = ‘01h‘

3.3 **Prístupové podmienky (AC)**

Prístupové podmienky (AC) pre príkazy UPDATE_BINARY a READ_BINARY sú definované pre každý elementárny súbor.

TCS_312 pred prístupom k aktuálnemu súboru prostredníctvom týchto príkazov musia byť splnené AC aktuálneho súboru.

Definície dostupných prístupových podmienok sú tieto:

- ALW: činnosť je vždy možná a môže sa vykonať bez akýchkoľvek obmedzení.
- NEV: činnosť nie je možná nikdy.
- AUT: musí sa otvoriť právo zodpovedajúce úspešnému externému overeniu (vykoná sa príkazom EXTERNAL_AUTHENTICATE).
- PO SM: príkaz sa musí preniesť s kryptografickým kontrolným súčtom použitím secure messaging (pozri doplnok 11).
- AUT a PRO SM (kombinované)

Príkazmi na spracovanie (UPDATE_BINARY and READ_BINARY) sa môžu v karte nastaviť tieto prístupové podmienky:

	UPDATE_BINARY	READ_BINARY
ALW	Áno	Áno
NEV	Áno	Áno
AUT	Áno	Áno
PRO SM	Áno	Nie
AUT a PRO SM	Áno	Nie

Prístupové podmienky PRO SM nie sú k dispozícii pre príkaz READ_BINARY. To znamená, že prítomnosť kryptografického kontrolného súčtu pre príkaz READ nikdy nie je povinná. Avšak s použitím hodnoty ‘OC’ pre triedu je možné použiť príkaz READ_BINARY so secure messaging, ako je popísané v odseku 3.6.2.

3.4 **Kódovanie dát**

Keď musí byť chránená dôvernosť dát čítaných zo súboru, súbor sa označí ako „kódovaný“. Kódovanie sa vykoná s použitím secure messaging (pozri doplnok 11)

3.5 **Prehľad príkazových a chybových kódov**

Organizácia príkazov a súborov sa odvodí z normy ISO/IEC 7816–4, ktorej požiadavky musia byť splnené.

TCS_313 Tento odsek popisuje nasledovné APDU páry príkazov a odpovedí:

Príkaz	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 Stavové slová SW1 SW2 sa vrátia v každej odpovedi na správu a označujú stav spracovania príkazu.

SW1	SW2	Význam
90	00	Normálne spracovanie
61	XX	Normálne spracovanie. XX = počet dostupných bajtov odpovedí
62	81	Spracovanie s výstrahou. Časť vrátených dát môže byť poškodená.
63	CX	Chybné CHV (PIN). Počítadlo zostávajúcich pokusov 'X'
64	00	Vykonávacia chyba – stav energeticky nezávislej pamäte nezmenený. Chyba integrity
65	00	Vykonávacia chyba – stav energeticky nezávislej pamäte zmenený.
65	81	Vykonávacia chyba – stav energeticky nezávislej pamäte zmenený. Chyba pamäte
66	88	Bezpečnostná chyba: chybný kryptografický kontrolný súčet (počas secure messaging) alebo chybné osvedčenie (počas overovania osvedčenia) alebo chybný kryptogram chybný podpis (počas overovania podpisu)
67	00	Chybná dĺžka (chybná Lc alebo Le)
69	00	Zakázaný príkaz (žiadna odpoveď dostupná v T=0)
69	82	Bezpečnostný stav neuspokojivý
69	83	Blokovaný postup overovania
69	85	Nesplnené podmienky používania
69	86	Príkaz nie je prípustný (žiadny aktuálny EF)
69	87	Chýbajú očakávané secure messaging dátové objekty
69	88	Nesprávne secure messaging dátové objekty
6A	82	Nenašiel sa súbor
6A	86	Chybné parametre P1–P2
6A	88	Nenašli sa referenčné dáta
6B	00	Chybné parametre (posun mimo EF)
6C	XX	Chybná dĺžka, SW2 udáva presnú dĺžku. Nevrátilo sa žiadne dátové pole
6D	00	Nepodporovaný alebo neplatný príkazový kód
6E	00	Nepodporovaná trieda
6F	00	Iné kontrolné chyby

3.6 **Popis príkazov**

V tejto kapitole sú popísané povinné príkazy pre tachografové karty.

Ďalšie relevantné podrobnosti, vzťahujúce sa ku kryptografickým operáciám sú uvedené v doplnku 11 Spoločné bezpečnostné mechanizmy.

Všetky príkazy sú popísané nezávisle na použitom protokole (T=0 alebo T=1). Vždy sú udané ADPU bajty CLA, INS, P1, P2, Lc a Le. Ak pre popísané príkazy nie sú potrebné Lc alebo Le, príslušná dĺžka, hodnota a popis sú prázdne.

TCS_315 Ak sa vyžadujú obe dĺžky bajtov (Lc aj Le), popísané príkazy musia byť rozdelené do dvoch častí ak IFD použije protokol T=0: IFD vysiela príkaz popísaný s P3=Lc + dáta a potom posiela príkaz GET_RESPONSE (pozri odsek 3.6.6) s P3=Le.

TCS_316 Ak sa vyžadujú obe dĺžky bajtov a ak Le=0 (secure messaging):

– keď sa použije protokol T=1, karta odpovedá na Le=0 vyslaním všetkých disponibilných výstupných dát;

– keď sa použije protokol T=0, IFD vyšle prvý príkaz s P3=Lc + dáta, karta odpovie (na túto implicitnú Le=0) stavom bajtov ‘61La’, pričom La je počet dostupných odpoveďových bajtov. IFD potom generuje príkaz GET RESPONSE s P3=La na čítanie dát.

3.6.1 **Select file**

Tento príkaz zodpovedá norme ISO/IEC 7816–4, no má obmedzené použitie v porovnaní s príkazom definovaným v norme.

Príkaz SELECT FILE sa používa:

– na voľbu aplikácie DF (musí sa použiť voľba podľa mena)

– na voľbu elementárneho súboru zodpovedajúceho predloženému súboru ID

3.6.1.1 *Výber podľa mena (AID)*

Tento príkaz umožňuje voľbu aplikácie DF v karte.

TCS_317 Tento príkaz sa môže vykonať z ktorejkoľvek štruktúry súboru (po ATR alebo kedykoľvek).

TCS_318 Voľba aplikácie vynuluje súčasné bezpečnostné prostredie. Po vykonaní voľby aplikácie, sa nezvolí žiadny aktuálny verejný kľúč a predchádzajúci relačný kľúč nie je pre secure messaging viac dostupný. Prístupová podmienka AUT sa teda stratí.

TCS_319 Príkazová správa

Bajty	Dĺžka	Hodnota	Popis
CLA	1	‘00h’	
INS	1	‘A4h‘	
P1	1	‘04h‘	Voľba podľa mena
P2	1	‘0Ch‘	Neočakáva sa žiadna odpoveď
Lc	1	‘NNh‘	Počet bajtov poslaných na kartu (dĺžka AID): ‘06h‘ pre tachografovú aplikáciu
#6–#(5+NN)	NN	‘XX..XXh‘	AID: ‘FF 54 41 43 48 4F‘pre tachografovú aplikáciu

Nie je potrebná žiadna odpoveď na príkaz SELECT FILE (Le chýba v T=1, alebo nevyžaduje sa žiadna odpoveď v T=0).

TCS_320 Odpovedacia správa (nevyžaduje sa žiadna odpoveď)

Bajty	Dĺžka	Hodnota	Popis
SW	2	‘XXXXh’	Stavové slová (SW1, SW2)

– Ak je príkaz úspešný, karta vráti ‘9000’,

– ak sa nenašla aplikácia zodpovedajúca AID, vrátený stav spracovania je ‘6A82’,

– v T=1, ak je prítomný bajt Le, vrátený stav je ‘6700’,

– v T=0, ak sa po príkaze SELECT FILE vyžaduje odpoveď, vrátený stav je ‘6900’,

– ak sa zvolená aplikácia považuje za chybnú (zistila sa chyba integrity v atribútoch súboru), vrátený stav spracovania je ‘6400‘ alebo ‘6581’.

3.6.1.2 *Výber elementárneho súboru s použitím jeho identifikátora*

TCS_321 Príkazová správa

Bajty	Dĺžka	Hodnota	Popis
CLA	1	‘00h’	
INS	1	‘A4h‘	
P1	1	‘02h‘	Voľba EF podľa aktuálneho DF
P2	1	‘0Ch‘	Neočakáva sa žiadna odpoveď
Lc	1	‘02h‘	Počet bajtov poslaných na kartu
#6–#7	2	‘XXXXh‘	Identifikátor súboru

Nie je potrebná žiadna odpoveď na príkaz SELECT FILE (Le chýba v T=1, alebo nevyžaduje sa žiadna odpoveď v T=0).

TCS_322 Odpovedacia správa (nevyžaduje sa žiadna odpoveď)

Bajty	Dĺžka	Hodnota	Popis
SW	2	‘XXXXh’	Stavové slová (SW1, SW2)

– Ak je príkaz úspešný, karta vráti ‘9000’,

– ak sa nenašiel súbor zodpovedajúci identifikátoru súboru, vrátený stav spracovania je ‘6A82’,

– v T=1, ak je prítomný bajt Le, vrátený stav je ‘6700’,

– v T=0, ak sa po príkaze SELECT FILE vyžaduje odpoveď, vrátený stav je ‘6900’,

– ak sa zvolený súbor považuje za chybný (zistila sa chyba integrity v atribútoch súboru), vrátený stav spracovania je ‘6400‘ alebo ‘6581’.

3.6.2 **Read Binary**

Tento príkaz zodpovedá norme ISO/IEC 7816–4, no má obmedzené použitie v porovnaní s príkazom definovaným v norme.

Príkaz Read Binary sa používa na čítanie dát z transparentného súboru.

Odpoveď karty pozostáva z vrátených prečítaných dát, ktoré sú nepovinne uzavreté v štruktúre secure messaging.

TCS_323 Príkaz sa môže vykonať len ak bezpečnostný stav spĺňa bezpečnostné atribúty definované pre EF pre funkciu READ.

3.6.2.1 *Príkaz bez Secure Messaging*

Tento príkaz umožňuje IFD čítanie dát z aktuálne zvoleného EF, bez secure messaging.

TCS_324 Týmto príkazom nie je možné čítanie dát zo súboru označeného ako „kódovaný“.

TCS_325 Príkazová správa

Bajty	Dĺžka	Hodnota	Popis
CLA	1	‘00h’	Nevyžaduje sa žiadne secure messaging
INS	1	‘B0h‘	
P1	1	‘XXh‘	Posun v bajtoch od začiatku súboru: bajt najvyššieho rádu
P2	1	‘XXh‘	Posun v bajtoch od začiatku súboru: bajty najnižšieho rádu
Le	1	‘XXh‘	Dĺžka očakávaných dát: počet čítaných bajtov

Poznámka: bit 8 P1 musí byť nastavený na 0.

TCS_326 Odpovedacia správa

Bajty	Dĺžka	Hodnota	Popis
#1–#X	X	‘XX..XXh‘	Čítané dáta
SW	2	‘XXXXh‘	Stavové slová (SW1, SW2)

– Ak je príkaz úspešný, karta vráti ‘9000’,

– nie je zvolený žiadny EF, vrátený stav spracovania je ‘6986’,

– ak nie je splnená prístupová podmienka zvoleného súboru, príkaz sa preruší s ‘6982’

– ak nie je posun kompatibilný s veľkosťou EF (Offset > veľkosť EF), vrátený stav spracovania je ‘6B00’,

– ak nie je veľkosť čítaných dát kompatibilná s veľkosťou EF (Offset + Le > veľkosť EF), vrátený stav spracovania je ‘6700’ alebo ‘6Cxx’, pričom ‘xx’ znamená presnú dĺžku,

– ak sa zistila chyba integrity v atribútoch súboru, karta považuje súbor za chybný a neopraviteľný, vrátený stav spracovania je ‘6400’ alebo ‘6581’,

– ak sa zistila chyba integrity v uložených dátach, karta vráti požadované dáta a vrátený stav spracovania je ‘6281’,

3.6.2.2 *Príkaz so Secure Messaging*

Tento príkaz umožňuje IFD čítanie dát z aktuálne zvoleného EF so secure messaging, aby sa overila integrita prijatých dát a chránila dôvernosť dát v prípade, že EF je označený ako „kódovaný“.

TCS_327 Príkazová správa

Bajty	Dĺžka	Hodnota	Popis
CLA	1	‘0Ch’	Vyžaduje sa secure messaging
INS	1	‘B0h‘	INS
P1	1	‘XXh‘	P1 (posun v bajtoch od začiatku súboru): bajt najvyššieho rádu
P2	1	‘XXh‘	P2 (posun v bajtoch od začiatku súboru): bajt najnižšieho rádu
Lc	1	‘09h‘	Dĺžka vstupných dát: pre secure messaging
#6	1	‘97h‘	T_{LE}: tag pre špecifikácie očakávanej dĺžky
#7	1	‘01h‘	L_{LE}: očakávaná dĺžka

#8	1	‘NNh‘	Špecifikácia očakávanej dĺžky (pôvodná Le): počet čítaných bajtov
#9	1	‘8Eh‘	T_{CC}: tag pre kryptografický kontrolný súčet
#10	1	‘04h‘	L_{CC}: dĺžka nasledujúceho kryptografického kontrolného súčtu
#11–#114	4	‘XX..XXh‘	Kryptografický kontrolný súčet (4 bajty najvyššieho rádu)
Le	1	‘00h‘	Špecifikované v ISO/IEC 7816–4

TCS_328 Odpovedacia správa ak EF nie je označený ako „kódovaný“ a ak je vstupný formát secure messaging správny.

Bajt	Dĺžka	Hodnota	Popis
#1	1	‘81h‘	T_{PV}: tag pre čitateľné hodnotové dáta
#2	L	‘NNh‘ alebo ‘81NNh ‘	L_{PV}: dĺžka vrátených dát (= pôvodná Le) L je dvojbajtová ak L_{PV} > 127 bajtov
#(2+L)–#(1+L+NN)	NN	‘XX..XXh‘	Hodnota čitateľných dát
#(2+L+NN)	1	‘8Eh‘	T_{CC}: tag pre kryptografický kontrolný súčet
#(3+L+NN)	1	‘04h‘	L_{CC}: dĺžka nasledujúceho kryptografického kontrolného súčtu
#(4+L+NN)–#(7+L+NN)	4	‘XX..XXh‘	Kryptografický kontrolný súčet (4 bajty najvyššieho rádu)
SW	2	‘XXXXh‘	Stavové slová (SW1, SW2)

TCS_329 Odpovedacia správa ak EF je označený ako „kódovaný“ a ak je vstupný formát secure messaging správny.

Bajt	Dĺžka	Hodnota	Popis
#1	1	‘87h‘	$T_{PI\ CG}$: tag pre kódované dáta (kryptogram)
#2	L	‘MMh‘ alebo ‘81MMh ‘	$L_{PI\ CG}$: dĺžka vrátených kódovaných dát (kvôli vyplneniu iná ako pôvodná dĺžka Le príkazu) L je dvojbajtová ak $L_{PI\ CG}$ > 127 bajtov
#(2+L)–#(1+L+MM)	MM	‘01XX..XXh‘	Kódované dáta: indikátor vyplnenia a kryptogram
#(2+L+MM)	1	‘8Eh‘	T_{CC}: tag pre kryptografický kontrolný súčet
#(3+L+MM)	1	‘04h‘	L_{CC}: dĺžka nasledujúceho kryptografického kontrolného súčtu
#(4+L+MM)–#(7+L+MM)	4	‘XX..XXh‘	Kryptografický kontrolný súčet (4 bajty najvyššieho rádu)
SW	2	‘XXXXh‘	Stavové slová (SW1, SW2)

Vrátené kódované dáta obsahujú prvý bajt udávajúci použitý režim vyplňovania. Pre tachografovú aplikáciu indikátor vyplňovania má vždy hodnotu ‘01h’ udávajúc, že použitý režim vyplňovania je jedným z režimov špecifikovaných v ISO/IEC 7816–4 (jeden bajt s hodnotou ‘80h’, za ktorým nasledujú niektoré nulové bajty: ISO/IEC 9797 metóda 2).

„Pravidelné“ stavy spracovania popísané pre príkaz READ BINARY bez secure messaging (pozri odsek 3.6.2.1), môžu byť vrátené s použitím štruktúr správ popísaných vyššie, pod označením ‘99h’. (popísané v TCS 335).

Okrem toho sa môžu vyskytnúť niektoré chyby špecificky vztiahnuté k secure messaging. V takom prípade sa stav spracovania jednoducho vráti bez štruktúry secure messaging:

TCS_330 Odpovedacia správa pri nesprávnom vstupnom formáte Secure Messaging

Bajt	Dĺžka	Hodnota	Popis
SW	2	‘XXXXh‘	Stavové slová (SW1, SW2)

– Ak nie je dostupný aktuálny kľúč relácie, vrátený stav spracovania je ‘6A88’. To sa uskutoční buď vtedy keď kľúč relácie nebol ešte generovaný alebo keď skončila platnosť kľúča relácie (v tomto prípade IFD musí obnoviť vzájomný overovací proces aby sa nastavil nový kľúč relácie.

– Ak vo formáte secure messaging chýbajú niektoré očakávané dátové objekty (ako je špecifikované vyššie), vrátený stav spracovania je ‘6987’; táto chyba nastáva vtedy, keď chýba očakávaný tag alebo keď telo príkazu nie je vhodne konštruované.

– Ak sú niektoré dátové objekty nesprávne, vrátený stav spracovania je ‘6988’; táto chyba nastáva vtedy, keď sú prítomné všetky požadované označenia, no niektoré dĺžky sa líšia od očakávaných dĺžok.

– Ak overenie kryptografického kontrolného súčtu chýba, vrátený stav spracovania je ‘6688’.

3.6.3 **Update Binary**

Tento príkaz zodpovedá norme ISO/IEC 7816–4, no má obmedzené použitie v porovnaní s príkazom definovaným v norme.

Príkazová správa UPDATE BINARY iniciuje aktualizáciu (erase + write) bitov, ktoré sú už k dispozícii v EF binary bitmi danými v príkaze APDU.

TCS_331 Príkaz sa môže vykonať len ak bezpečnostný stav spĺňa atribúty bezpečnosti definované v EF pre funkciu UPDATE (ak kontrola prístupu funkcie UPDATE zahŕňa PRO SM, musí sa v príkaze doplniť secure messaging).

3.6.3.1 *Príkaz bez Secure Messaging*

Tento príkaz umožňuje IFD písať dáta do aktuálne zvoleného EF bez toho, aby karta overila integritu prijímaných dát. Tento jednoduchý model je povolený len vtedy, keď nie je príslušný súbor označený ako „kódovaný“.

TCS_332 Príkazová správa

Bajt	Dĺžka	Hodnota	Popis
CLA	1	‘00h’	Nevyžaduje sa secure messaging
INS	1	‘D6h‘	Posun v bajtoch od začiatku súboru: bajt najvyššieho rádu
P1	1	‘XXh‘	
P2	1	‘XXh‘	Posun v bajtoch od začiatku súboru: bajt najnižšieho rádu
Lc	1	‘NNh‘	Lc dĺžka aktualizovaných dát. Počet napísaných bajtov
#6–# (5+NN)	NN	‘XX..XXh‘	Napísané dáta

Poznámka: bit 8 P1 musí byť nastavený na 0.

TCS_333 Odpovedacia správa

Bajt	Dĺžka	Hodnota	Popis
SW	2	‘XXXXh‘	Stavové slová (SW1, SW2)

– Ak je príkaz úspešný, karta vráti ‘9000’,

– nie je zvolený žiadny EF, vrátený stav spracovania je ‘6986’,

– ak nie je splnená prístupová podmienka zvoleného súboru, príkaz sa preruší s ‘6982’

– ak nie je posun kompatibilný s veľkosťou EF (Offset > veľkosť EF), príkaz sa preruší s ‘6B00’,

– ak nie je veľkosť čítaných dát kompatibilná s veľkosťou EF (Offset + Lc > veľkosť EF), vrátený stav spracovania je ‘6700’,

– ak sa zistila chyba integrity v atribútoch súboru, karta považuje súbor za chybný a neopraviteľný, vrátený stav spracovania je ‘6400’ alebo ‘6500’,

– ak je písanie neúspešné, vrátený stav spracovania je ‘6581’.

3.6.3.2 *Príkaz so Secure Messaging*

Tento príkaz umožňuje IFD písať dáta do aktuálne zvoleného EF s kartou overujúcou integritu prijímaných dát. Pretože sa nevyžaduje dôvernosť dát, dáta nie sú kódované.

TCS_334 Príkazová správa

Bajt	Dĺžka	Hodnota	Popis
CLA	1	‘0Ch’	Vyžaduje sa secure messaging
INS	1	‘D6h‘	INS
P1	1	‘XXh‘	Posun v bajtoch od začiatku súboru: bajt najvyššieho rádu
P2	1	‘XXh‘	Posun v bajtoch od začiatku súboru: bajt najnižšieho rádu
Lc	1	‘XXh‘	Dĺžka poľa zabezpečeného dátového poľa
#6	1	‘81h‘	T_{PV}: tag pre čitateľné hodnotové dáta
#7	L	‘NNh‘ alebo ‘81NNh ‘	L_{PV}: dĺžka prenesených dát L je dvojbajtová ak L_{PV} > 127 bajtov
#(7+L)–#(6+L+NN)	NN	‘XX..XXh‘	Čitateľné hodnotové dáta (písané dáta)
#(7+L+NN)	1	‘8Eh‘	T_{CC}: tag pre kryptografický kontrolný súčet
#(8+L+NN)	1	‘04h‘	L_{CC}: dĺžka nasledujúceho kryptografického kontrolného súčtu
#(9+L+NN)–#(12+L+NN)	4	‘XX..XXh‘	Kryptografický kontrolný súčet (4 bajty najvyššieho rádu)
Le	1	‘00h‘	Špecifikované v ISO/IEC 7816–4

TCS_335 Odpovedacia správa ak je vstupný formát secure messaging správny.

Bajt	Dĺžka	Hodnota	Popis
#1	1	‘99h‘	T_{SW}: tag pre stavové slová (chránené CC)
#2	1	‘02h‘	L_{SW}: dĺžka vrátených stavových slov
#3–#4	2	‘XXXXh‘	Stavové slová (SW1, SW2)
#5	1	‘8Eh‘	T_{CC}: tag pre kryptografický kontrolný súčet
#6	1	‘04h‘	L_{CC}: dĺžka nasledujúceho kryptografického kontrolného súčtu
#7–#10	4	‘XX..XXh‘	Kryptografický kontrolný súčet (4 bajty najvyššieho rádu)
SW	2	‘XXXXh‘	Stavové slová (SW1, SW2)

„Pravidelné“ stavy spracovania popísané pre príkaz UPDATE BINARY bez secure messaging (pozri odsek 3.6.3.1), môžu byť vrátené s použitím štruktúry odpovedacej správy popísanej vyššie.

Okrem toho sa môžu vyskytnúť niektoré chyby špecificky vztiahnuté k secure messaging. V takom prípade sa stav spracovania jednoducho vráti bez štruktúry secure messaging:

TCS_336 Odpovedacia správa pri nesprávnom vstupnom formáte Secure Messaging

Bajt	Dĺžka	Hodnota	Popis
SW	2	‘XXXXh‘	Stavové slová (SW1, SW2)

– Ak nie je dostupný aktuálny kľúč relácie, vrátený stav spracovania je ‘6A88’ .

– Ak vo formáte secure messaging chýbajú niektoré očakávané dátové objekty (ako je špecifikované vyššie), vrátený stav spracovania je ‘6987’; táto chyba nastáva vtedy, keď chýba očakávaný tag alebo keď telo príkazu nie je vhodne konštruované.

– Ak sú niektoré dátové objekty nesprávne, vrátený stav spracovania je ‘6988’; táto chyba nastáva vtedy, keď sú prítomné všetky požadované označenia, no niektoré dĺžky sa líšia od očakávaných dĺžok.

– Ak overenie kryptografického kontrolného súčtu chýba, vrátený stav spracovania je ‘6688’.

3.6.4 ***Get challenge***

Tento príkaz zodpovedá norme ISO/IEC 7816–4, no má obmedzené použitie v porovnaní s príkazom definovaným v norme.

Príkaz GET CHALLENGE vyžaduje, aby karta vydala výzvu na jeho použitie v bezpečnostnom postupe, ktorým sa kryptogram alebo šifrované dáta posielajú na kartu.

TCS_337 Výzva vydaná kartou je platná len pre nasledujúci príkaz, ktorý použije výzvu odoslanú na kartu.

TCS_338 Príkazová správa

Bajt	Dĺžka	Hodnota	Popis
CLA	1	‘00h’	CLA
INS	1	‘84h‘	INS
P1	1	‘00h‘	P1
P2	1	‘00h‘	P2
Le	1	‘08h‘	Le (dĺžka očakávanej výzvy)

TCS_339 Odpovedacia správa

Bajt	Dĺžka	Hodnota	Popis
#1–#8	8	‘XX..XXh‘	Výzva
SW	2	‘XXXXh‘	Stavové slová (SW1, SW2)

– Ak je príkaz úspešný, karta vráti ‘9000’,

– ak sa Le líši od ‘08h’, stav spracovania je ‘6700’,

– ak sú parametre P1–P2 nesprávne, stav spracovania je ‘6A86’.

3.6.5 ***Verify***

Tento príkaz zodpovedá norme ISO/IEC 7816–4, no má obmedzené použitie v porovnaní s príkazom definovaným v norme.

Príkaz Verify iniciuje na karte porovnanie dát CHV (PIN) posielaných príkazom s odkazom CHV uloženým na karte.

Poznámka: PIN zapísané užívateľom musí IFD vyplniť s bajtmi ‘FFh’ doprava až do dĺžky 8 bajtov

TCS_340 Ak je príkaz úspešný, uvoľnia sa práva zodpovedajúce prezentácii CHV a počítadlo pre zostávajúce pokusy sa musí znovu iniciovať.

TCS_341 Neúspešné porovnanie sa zaznamená na karte, aby sa obmedzil počet ďalších pokusov použitia odkazu CHV.

TCS_342 Príkazová správa

Bajt	Dĺžka	Hodnota	Popis
CLA	1	‘00h’	CLA
INS	1	‘20h‘	INS
P1	1	‘00h‘	P1
P2	1	‘00h‘	P2 (Overované CHV je implicitne známe)
Lc	1	‘08h‘	Dĺžka prenášaného kódu CHV
#6–#13	8	‘XX..Xh‘	CHV

TCS_343 Odpovedacia správa

Bajt	Dĺžka	Hodnota	Popis
SW	2	‘XXXXh’	Stavové slová (SW1, SW2)

– Ak je príkaz úspešný, karta vráti ‘9000’,

– ak sa nenašiel odkaz na CHV, vrátený stav spracovania je ‘6A88’,

– ak je CHV blokované, (počítadlo zostávajúcich pokusov je na nule), vrátený stav spracovania je ‘6983’. Keď sa dosiahne tento stav, nesmie byť CHV nikdy opäť úspešne prezentované,

– ak je porovnanie neúspešné, počítač zostávajúcich pokusov sa zníži a vráti sa stav ‘63CX’ (X > 0 a X sa rovná počítadlu zostávajúcich pokusov. X = ‘F’, počítadlo zostávajúcich pokusov je väčšie než ‘F’),

– ak sa odkaz CHV považuje za chybný, vrátený stav spracovania je ‘6400’ alebo ‘6581’.

3.6.6 ***Get response***

Tento príkaz zodpovedá norme ISO/IEC 7816–4.

Tento príkaz (potrebný a dostupný len pre protokol T=0) sa používa na prenos pripravených dát, inak sú dáta stratené. Po vykonaní príkazu GET_RESPONSE (okrem prípadu, keď nastane chyba ‘61xx’ alebo ‘6Cxx’, pozri nižšie), predchádzajúce pripravené dáta nie sú naďalej dostupné.

TCS_344 Príkazová správa

Bajt	Dĺžka	Hodnota	Popis
CLA	1	‘00h’	
INS	1	‘C0h‘	
P1	1	‘00h‘	
P2	1	‘00h‘	
Le	1	‘XXh‘	Počet očakávaných bajtov

TCS_345 Odpovedacia správa

Bajt	Dĺžka	Hodnota	Popis
#1–#X	X	‘XX..XXh‘	Dáta
SW	2	‘XXXXh‘	Stavové slová (SW1, SW2)

– Ak je príkaz úspešný, karta vráti ‘9000’.

– Ak neboli kartou pripravené žiadne dáta, vrátený stav spracovania je ‘6900’ alebo ‘6F00’.

– Ak Le presiahne počet dostupných bajtov alebo ak je Le nulová, vrátený stav spracovania je ‘6Cxx’, kde ‘xx’ označuje presný počet dostupných bajtov. V uvedenom prípade sú pripravené dáta stále dostupné pre nasledujúci príkaz GET_RESPONSE.

– Ak Le nie je nulová a je menšia než počet dostupných bajtov, požadované dáta budú odosielané kartou normálne a vrátený stav spracovania je ‘61xx’, kde ‘xx’ označuje počet dodatočných bajtov, ktoré sú ešte stále dostupné pre nasledujúci príkaz GET_RESPONSE.

– Ak príkaz nie je podporovaný (protokol T=1), karta vráti ‘6D00’.

3.6.7 ***PSO: verify Certificate***

Tento príkaz zodpovedá norme ISO/IEC 7816–8, no má obmedzené použitie v porovnaní s príkazom definovaným v norme.

Príkaz VERIFY CERTIFICATE karta použije na získanie verejného kľúča zvonku a na kontrolu jej platnosti.

TCS_346 Keď je príkaz VERIFY CERTIFICATE úspešný, verejný kľúč sa uloží pre budúce použitie v zabezpečenom prostredí. Tento kľúč sa explicitne nastaví na použitie v príkazoch vzťahujúcich sa k bezpečnosti (INTERNAL AUTHENICATE, EXTERNAL AUTHENICATE, AUTHENICATE alebo VERIFY AUTHENICATE) prostredníctvom príkazu MSE (pozri odsek 3.6.10) s použitím svojho identifikátora kľúča.

TCS_347 V každom prípade príkaz VERIFY CERTIFICATE používa verejný kľúč, ktorý bol predtým zvolený príkazom MSE na otvorenie osvedčenia. Musí ísť o verejný kľúč jedného z členských štátov alebo európskeho štátu.

TCS_348 Príkazová správa

Bajt	Dĺžka	Hodnota	Popis
CLA	1	‘00h’	CLA
INS	1	‘2Ah‘	Perform Security Operation
P1	1	‘00h‘	P1
P2	1	‘AEh‘	P2: nie BER–TLV kódované dáta (zreťazenie dátových prvkov)
Lc	1	‘C2h‘	Lc: dĺžka osvedčenia, 194 bajtov
#6–#199	194	‘XX..XXh’	Osvedčenie: zreťazenie dátových prvkov (popísané v doplnku 11)

TCS_349 Odpovedacia správa

Bajt	Dĺžka	Hodnota	Popis
SW	2	‘XXXXh‘	Stavové slová (SW1, SW2)

– Ak je príkaz úspešný, karta vráti ‘9000’,

– je overenie osvedčenia chybné, vrátený stav spracovania je ‘6688’. Proces overenia a rozbalenia osvedčenia je popísaný v doplnku 11,

– ak nie je v bezpečnostnom prostredí prítomný žiadny verejný kľúč, vráti sa ‘6A88’,

– ak zvolený verejný kľúč (použitý na rozbalenie osvedčenia) sa považuje za chybný, vrátený stav spracovania je ‘6400’ alebo ‘6581’,

– ak zvolený verejný kľúč (použitý na rozbalenie osvedčenia) má CHA.LSB (CertificateHolderAuthorisation.equipmentType) s inou hodnotou než ‘00’ (t. j. nie je to kľúč členského štátu alebo európskeho štátu), vrátený stav spracovania je ‘6985’.

3.6.8 ***Internal authenticate***

Tento príkaz zodpovedá norme ISO/IEC 7816–4.

Pomocou príkazu INTERNAL AUTHENTICATE môže IFD overiť autenticitu karty.

Proces overenia je popísaný v doplnku 11. Obsahuje tieto konštatovania:

TCS_350 Príkaz INTERNAL AUTHENTICATE používa súkromný kľúč karty (zvolený implicitne) na označenie autentifikačných dát vrátane K1 (prvý prvok pre dohodnutý kľúč relácie) a RND1 a používa aktuálne zvolený verejný kľúč (pomocou posledného príkazu MSE), na kódovanie podpisu a vytvorenie overovacieho znaku (bližšie údaje v doplnku 11)

TCS_351 Príkazová správa

Bajt	Dĺžka	Hodnota	Popis
CLA	1	‘00h’	CLA
INS	1	‘88h‘	INS
P1	1	‘00h‘	P1
P2	1	‘00h‘	P2
Lc	1	‘10h‘	Dĺžka dát posielaných na kartu
#6–#13	8	‘XX..XXh‘	Výzva použitá na overenie karty
#14–#21	8	‘XX..XXh‘	VU.CHR (pozri doplnok 11)
Le	1	‘80h‘	Dĺžka z karty očakávaných dát

TCS_352 Odpovedacia správa

Bajt	Dĺžka	Hodnota	Popis
#1–#128	128	‘XX..XXh‘	Overovací znak karty (pozri doplnok 11)
SW	2	‘XXXXh‘	Stavové slová (SW1, SW2)

– Ak je príkaz úspešný, karta vráti ‘9000’,

– ak nie je v bezpečnostnom prostredí prítomný žiadny verejný kľúč, vrátený stav spracovanie je ‘6A88’,

– ak nie je v bezpečnostnom prostredí prítomný žiadny súkromný kľúč, vrátený stav spracovania je ‘6A88’,

– ak sa VU.CHR nezhoduje s aktuálnym identifikátorom verejného kľúča, vrátený stav spracovanie je ‘6A88’,

– ak sa zvolený súkromný kľúč považuje za chybný, vrátený stav spracovania je ‘6400’ alebo ‘6581’.

TCS_353 Ak je príkaz INTERNAL_AUTHENTICATE úspešný, aktuálny kľúč relácie, ak existuje, sa vymaže a nie je naďalej dostupný. Aby bol k dispozícii nový kľúč relácie, musí sa úspešne vykonať príkaz EXTERNAL_AUTHENTICATE.

3.6.9 ***External authenticate***

Tento príkaz zodpovedá norme ISO/IEC 7816–4.

Pomocou príkazu EXTERNAL AUTHENTICATE môže IFD overiť autenticitu karty.

Proces overenia je popísaný v doplnku 11. Obsahuje tieto konštatovania:

TCS_354 Príkaz GET CHALLENGE musí bezprostredne predchádzať príkazu EXTERNAL_AUTHENTICATE. Karta vydá výzvu von (RND3).

TCS_355 Overenie kryptogramu používa RND3 (výzva vydaná kartou), súkromný kľúč karty (implicitne zvolený) a predtým príkazom MSE zvolený verejný kľúč.

TCS_356 Karta overí kryptogram a ak je správny, otvorí sa prístupová podmienka AUT.

TCS_357 Vstupný kryptogram prenáša druhý prvok dohodnutého kľúča relácie K2.

TCS_358 Príkazová správa

Bajt	Dĺžka	Hodnota	Popis
CLA	1	‘00h’	CLA
INS	1	‘82h‘	INS
P1	1	‘00h‘	P1
P2	1	‘00h‘	P2 (použitý verejný kľúč je implicitne známy a bol predtým nastavený príkazom MSE)
Lc	1	‘80h‘	Lc (dĺžka dát posielaných na kartu)
#6–#133	128	‘XX..XXh‘	Kryptogram (pozri doplnok 11)

TCS_359 Odpovedacia správa

Bajt	Dĺžka	Hodnota	Popis
SW	2	‘XXXXh‘	Stavové slová (SW1, SW2)

– Ak je príkaz úspešný, karta vráti ‘9000’,

– ak nie je v bezpečnostnom prostredí prítomný žiadny verejný kľúč, vráti sa ‘6A88’,

– ak CHA aktuálne nastaveného verejného kľúča nie je zreťazením tachografovej aplikácie AID a zariadenia JV, vrátený stav spracovania je ‘6F00’ (pozri doplnok 11),

– ak nie je v bezpečnostnom prostredí prítomný žiadny súkromný kľúč, vrátený stav spracovania je ‘6A88’,

– ak je overenie kryptogramu chybné, vrátený stav spracovania je ‘6688’,

– ak pred príkazom nie je bezprostredne príkaz GET CHALLENGE, vrátený stav spracovania je ‘6985’,

– ak sa zvolený súkromný kľúč považuje za chybný, vrátený stav spracovanie je ‘6400’ alebo ‘6581’.

TCS_360 Ak je príkaz EXTERNAL_AUTHENTICATE úspešný a ak je prvá časť kľúča relácie dostupná z úspešného príkazu INTERNAL_AUTHENTICATE vykonaného predtým, kľúč relácie sa nastaví na budúce príkazy pomocou secure messaging.

TCS_361 Ak prvá časť kľúča relácie nie je dostupná z predtým vykonaného príkazu INTERNAL_AUTHENTICATE, druhá časť kľúča relácie, odoslaná IFD sa neuloží na karte. Tento mechanizmus zabezpečí, že vzájomný proces overovania autenticity prebieha v slede špecifikovanom v doplnku 11.

3.6.10 ***Manage security environment***

Tento príkaz sa používa na nastavenie verejného kľúča na účely autentifikácie.

Tento príkaz zodpovedá norme ISO/IEC 7816–8. Použitie tohto príkazu je obmedzené v porovnaní s príslušnou normou.

TCS_362 Kľúč na ktorý sa odkazuje v dátovom poli MSE je platný pre každý súbor DF tachografu.

TCS_363 Kľúč na ktorý sa odkazuje v dátovom poli MSE zostáva aktuálnym verejným kľúčom až do nasledovného správneho príkazu MSE.

TCS_364 Ak kľúč na ktorý sa odkazuje nie je (už) na karte k dispozícii, bezpečnostné prostredie zostáva nezmenené.

TCS_365 Príkazová správa

Bajt	Dĺžka	Hodnota	Popis
CLA	1	‘00h’	CLA

INS	1	‘22h‘	INS
P1	1	‘C1h‘	P1: kľúč, na ktorý sa odkazuje, platný pre všetky kryptografické operácie
P2	1	‘B6h‘	P2: (dáta opatrené odkazom týkajúce sa digitálneho podpisu)
Lc	1	‘0Ah‘	Lc: dĺžka následného dátového poľa
#6	1	‘83h’	Tag pre odkaz na verejný kľúč v asymetrických prípadoch
#7	1	‘08h’	Dĺžka odkazu na kľúč (identifikátor kľúča)
#8–#15	08h	‘XX..XXh‘	Identifikátor kľúča špecifikovaný v doplnku 11

TCS_366 Odpovedacia správa

Bajt	Dĺžka	Hodnota	Popis
SW	2	‘XXXXh‘	Stavové slová (SW1, SW2)

- Ak je príkaz úspešný, karta vráti ‘9000’,
- ak nie na karte prítomný kľúč, na ktorý sa odkazuje, vrátený stav spracovanie je ‘6A88’,
- ak niektoré očakávané dátové objekty chýbajú vo formácii secure messaging, vrátený stav spracovania je ‘6987’. To môže nastať ak chýba tag ‘83h’,
- ak sú niektoré dátové objekty nesprávne, vrátený stav spracovanie je ‘6988’. To môže nastať ak dĺžka identifikátora kľúča nie je ‘08h’,
- ak sa zvolený kľúč považuje za chybný, vrátený stav spracovania je ‘6400’ alebo ‘6581’.

3.6.11 ***PSO: hash***

Tento príkaz sa používa na prenos výsledkov hash výpočtu niektorých dát na kartu. Tento príkaz sa používa na overenie digitálnych podpisov. Hash hodnota sa uloží v EEPROM pre následný príkaz na overenie digitálneho podpisu.

Tento príkaz zodpovedá norme ISO/IEC 7816–8. Použitie tohto príkazu je obmedzené v porovnaní s príslušnou normou.

TCS_367 Príkazová správa

Bajt	Dĺžka	Hodnota	Popis
CLA	1	‘00h’	CLA
INS	1	‘2Ah‘	Perform security operation
P1	1	‘90h‘	Vrátený hash kód
P2	1	‘A0h‘	Tag: dátové pole obsahuje DO relevantné pre použitie hash kódu
Lc	1	‘16h‘	Lc: dĺžka následného dátového poľa
#6	1	‘90h’	Tag hash kódu
#7	1	‘14h’	Dĺžka hash kódu
#8–#27	20	‘XX..XXh‘	Hash kód

TCS_368 Odpovedacia správa

Bajt	Dĺžka	Hodnota	Popis
SW	2	‘XXXXh‘	Stavové slová (SW1, SW2)

– Ak je príkaz úspešný, karta vráti ‘9000’,

– ak niektoré očakávané dátové objekty (špecifikované vyššie) chýbajú, vrátený stav spracovania je ‘6987’. To môže nastať ak chýba tag ‘90‘,

– ak sú niektoré dátové objekty nesprávne, vrátený stav spracovanie je ‘6988’. Táto chyba môže nastať ak je prítomné požadovaný tag no s dĺžkou inou než ‘14h’.

3.6.12 **Perform hash of file**

Tento príkaz nezodpovedá norme ISO/IEC 7816–8. CLA bajt tohto príkazu udáva, že sa výhradne použije PERFORM SECURITY OPERATION/HASH.

TCS_369 Príkaz PERFORM HASH sa používa na hash výpočet dátovej oblasti aktuálne zvoleného transparentného EF.

TCS_370 Výsledok operácie hash je uložený na karte. Môže sa potom použiť na získanie digitálneho podpisu súboru, s použitím príkazu PSO–COMPUTE_DIGITAL_SIGNATURE . Tento výsledok zostáva k dispozícii pre príkaz COMPUTE DIGITAL SIGNATURE až do nasledovného úspešného príkazu PERFORM HASH of FILE.

TCS_371 Príkazová správa

Bajt	Dĺžka	Hodnota	Popis
CLA	1	‘80h’	CLA
INS	1	‘2Ah‘	Perform security operation
P1	1	‘90h‘	Tag: hash
P2	1	‘00h‘	P2: hash výpočet dát aktuálne zvoleného transparentného súboru

TCS_372 Odpovedacia správa

Bajt	Dĺžka	Hodnota	Popis
SW	2	‘XXXXh‘	Stavové slová (SW1, SW2)

– Ak je príkaz úspešný, karta vráti ‘9000’,

– ak nebola zvolená žiadna aplikácia, vrátený stav spracovania je ‘6985’,

– ak sa zvolený EF považuje za chybný (chyby atribútov súboru alebo integrity uložených dát), vrátený stav spracovania je ‘6400’ alebo ‘6581’,

– ak zvolený súbor nie je transparentným súborom, vrátený stav spracovania je ‘6986’.

3.6.13 ***PSO: compute digital signature***

Príkaz sa používa na výpočet digitálneho podpisu predtým vypočítaného hash kódu (pozri PERFORM HASH of FILE, odsek 3.6.12).

Tento príkaz zodpovedá norme ISO/IEC 7816–8. Použitie tohto príkazu je obmedzené v porovnaní s príslušnou normou.

TCS_373 Kľúč súkromnej karty sa používa na výpočet digitálneho podpisu a je pre kartu implicitne známy.

TCS_374 Karta vykoná digitálny podpis s použitím vyplňovacej metódy zodpovedajúcej PKCS1 (podrobnosti pozri v doplnku 11).

TCS_375 Príkazová správa

Bajt	Dĺžka	Hodnota	Popis
CLA	1	‘00h’	CLA
INS	1	‘2Ah‘	Perform security operation
P1	1	‘9Eh‘	Vrátený digitálny podpis
P2	1	‘9Ah‘	Tag: dátové pole obsahuje dáta, ktoré majú byť podpísané. Pretože nie je zahrnuté žiadne dátové pole vychádza sa z toho, že na karte sú už dáta prítomné (hash of file)
Le	1	‘80h‘	Dĺžka očakávaného podpisu

TCS_376 Odpovedacia správa

Bajt	Dĺžka	Hodnota	Popis
#1–#128	128	‘XX..XXh‘	Podpis predtým vypočítaného hash
SW	2	‘XXXXh‘	Stavové slová (SW1, SW2)

– Ak je príkaz úspešný, karta vráti ‘9000’,

– ak sa implicitne zvolený súkromný kľúč považuje za chybný, vrátený stav spracovania je ‘6400’ alebo ‘6581’.

3.6.14 ***PSO: verify digital signature***

Tento príkaz sa používa na overenie digitálneho podpisu poskytnutého v súlade s PKCS1 ako vstup správy, ktorej hash je karte implicitne známy.

Tento príkaz zodpovedá norme ISO/IEC 7816–8. Použitie tohto príkazu je obmedzené v porovnaní s príslušnou normou.

TCS_377 Príkaz VERIFY DIGITAL SIGNATURE vždy používa verejný kľúč zvolený predchádzajúcim príkazom MANAGE SECURITY ENVIRONMENT a predchádzajúci hash kód zapísaný PSO: hash príkaz

TCS_378 Príkazová správa

Bajt	Dĺžka	Hodnota	Popis
CLA	1	‘00h’	CLA
INS	1	‘2Ah‘	Perform security operation
P1	1	‘00h‘	
P2	1	‘A8h‘	Tag: dátové pole obsahuje DO relevantné pre overenie
Lc	1	‘83h‘	Dĺžka Lc následného dátového poľa
#28	1	‘9Eh’	Tag digitálneho podpisu
#29–#30	2	‘8180h‘	Dĺžka digitálneho podpisu (128 bajtov, kódované v súlade s ISO/IEC 7816–6)
#31–#158	128	‘XX..XXh’	Obsah digitálneho podpisu

TCS_379 Odpovedacia správa

Bajt	Dĺžka	Hodnota	Popis
SW	2	‘XXXXh‘	Stavové slová (SW1, SW2)

– Ak je príkaz úspešný, karta vráti ‘9000’,

– ak je overenie podpisu chybné, vrátený stav spracovania je ‘6688’. Proces overenia je popísaný v doplnku 11,

– ak nie je zvolený žiadny verejný kľúč, vrátený stav spracovania je ‘6A88’,

– ak niektoré očakávané dátové objekty (špecifikované vyššie) chýbajú, vrátený stav spracovania je ‘6987’. To môže nastať ak chýba jedno z požadovaných označení,

– ak nie je k dispozícii žiadny hash kód na spracovanie príkazu (ako výsledok predchádzajúceho PSO: hash príkaz), vrátený stav spracovania je ‘6985’,

– ak sú niektoré dátové objekty nesprávne, vrátený stav spracovania je ‘6988’. Toto môže nastať ak je dĺžka jedného z požadovaných dátových objektov nesprávna,

– ak sa zvolený verejný kľúč považuje za chybný, vrátený stav spracovania je ‘6400’ alebo ‘6581’.

4. ŠTRUKTÚRA TACHOGRAFOVEJ KARTY

Tento odsek špecifikuje štruktúry súborov tachografovej karty, ktoré slúžia na uloženie dostupných dát.

Nešpecifikuje vnútorné štruktúry závisiace na výrobcovi karty ako sú napr. záhlavia súborov, ani ukladanie a spracovávanie dátových prvkov potrebných len na vnútorné použitie ako sú EuropeanPublicKey, CardPrivateKey, TDesSessionKey or WorkshopCardPin.

Užitočná kapacita pamäte tachografových kariet musí byť minimálne 11 Kbajtov. Môžu sa používať vyššie kapacity. V takom prípade štruktúra karty zostáva rovnaká, ale počet záznamov niektorých prvkov štruktúry je zvýšený. Tento odsek špecifikuje minimálne a maximálne hodnoty týchto počtov záznamov.

4.1 **Štruktúra karty vodiča**

TCS_400 Po personalizácii musí mať karta vodiča nasledovnú stálu štruktúru súboru a prístupové podmienky k súborom:

Prístupové podmienky

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

TCS_401 Štruktúry všetkých EF sú transparentné.

TCS_402 Čítanie so secure messaging je možné pre všetky súbory pod DF tachograf.

TCS_403 Karta vodiča má túto dátovú štruktúru:

Súborový/dátový prvok	Počet záznamov	Veľkosť (v bajtoch) Min.	Max.	Štandardné hodnoty
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 Nasledovné hodnoty uvedené v tabuľke a používané na údaje o veľkosti, sú minimálnymi a maximálnymi hodnotami, ktoré musí používať dátová štruktúra karty vodiča:

		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 bajtov (28 dní * 93 zmien činnosti)	13 776 bajtov (28 dní * 240 zmien činnosti)

4.2 **Štruktúra dielenskej karty**

TCS_405 Po personalizácii musí mať dielenská karta nasledovnú stálu štruktúru súboru a prístupové podmienky k súborom:

File	File ID	Prístupové podmienky		
		Read	Update	Encrypted
MF	3F00			
├─EF ICC	0002	ALW	NEV	No
├─EF IC	0005	ALW	NEV	No
└─DF Tachograph	0500			
├─EF Application_Identification	0501	ALW	NEV	No
├─EF Card_Certificate	C100	ALW	NEV	No
├─EF CA_Certificate	C108	ALW	NEV	No
├─EF Identification	0520	ALW	NEV	No
├─EF Card_Download	0509	ALW	ALW	No
├─EF Calibration	050A	ALW	PRO SM / AUT	No
├─EF Sensor_Installation_Data	050B	ALW	NEV	Yes
├─EF Events_Data	0502	ALW	PRO SM / AUT	No
├─EF Faults_Data	0503	ALW	PRO SM / AUT	No
├─EF Driver_Activity_Data	0504	ALW	PRO SM / AUT	No
├─EF Vehicles_Used	0505	ALW	PRO SM / AUT	No
├─EF Places	0506	ALW	PRO SM / AUT	No
├─EF Current_Usage	0507	ALW	PRO SM / AUT	No
├─EF Control_Activity_Data	0508	ALW	PRO SM / AUT	No
└─EF Specific_Conditions	0522	ALW	PRO SM / AUT	No

TCS_406 Štruktúry všetkých EF sú transparentné.

TCS_407 Čítanie so secure messaging je možné pre všetky súbory pod DF tachograf.

TCS_408 Dielenská karta má túto dátovú štruktúru:

Súborový/dátový prvok	Počet záznamov	Veľkosť (v bajtoch) Min.	Max.	Štandardné 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 Nasledovné hodnoty uvedené v tabuľke a používané na údaje o veľkosti, sú minimálnymi a maximálnymi hodnotami, ktoré musí používať dátová štruktúra dielenskej karty:

		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 bajtov (1 deň * 93 zmien činnosti)	492 bajtov (1 deň * 240 zmien činnosti)

4.3 **Štruktúra kontrolnej karty**

TCS_410 Po personalizácii musí mať kontrolná karta nasledovnú stálu štruktúru súboru a prístupové podmienky k súborom:

		Prístupové podmienky		
File	File ID	Read	Update	Encrypted
MF	3F00			
EF ICC	0002	ALW	NEV	No
EF IC	0005	ALW	NEV	No
DF Tachograph	0500			
EF Application_Identification	0501	ALW	NEV	No
EF Card_Certificate	C100	ALW	NEV	No
EF CA_Certificate	C108	ALW	NEV	No
EF Identification	0520	AUT	NEV	No
EF Controller_Activity_Data	050C	ALW	PRO SM / AUT	No

TCS_411 Štruktúry všetkých EF sú transparentné.

TCS_412 Čítanie so secure messaging je možné pre všetky súbory pod DF tachograf.

TCS_413 Kontrolná karta má túto dátovú štruktúru:

Súborový/dátový prvok	Počet záznamov	Veľkosť (v bajtoch) Min.	Max.	Štandardné 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 Nasledovné hodnoty uvedené v tabuľke a používané na údaje o veľkosti, sú minimálnymi a maximálnymi hodnotami, ktoré musí používať dátová štruktúra kontrolnej karty:

		Min.	Max.
n_7	NoOfControlActivityRecords	230	520

4.4 **Štruktúra podnikovej karty**

TCS_415 Po personalizácii musí mať podniková karta nasledovnú stálu štruktúru súboru a prístupové podmienky k súborom:

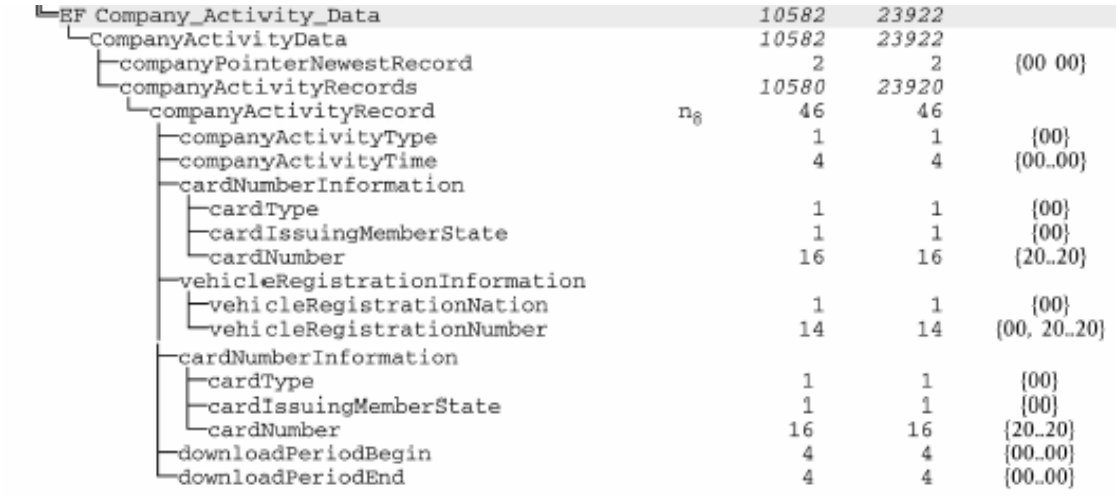
File	File ID	Prístupové podmienky		
		Read	Update	Encrypted
MF	3F00			
├─EF ICC	0002	ALW	NEV	No
├─EF IC	0005	ALW	NEV	No
└─DF Tachograph	0500			
├─EF Application_Identification	0501	ALW	NEV	No
├─EF Card_Certificate	C100	ALW	NEV	No
├─EF CA_Certificate	C108	ALW	NEV	No
├─EF Identification	0520	AUT	NEV	No
└─EF Company_Activity_Data	050D	ALW	PRO SM / AUT	No

TCS_416 Štruktúry všetkých EF sú transparentné.

TCS_417 Čítanie so secure messaging je možné pre všetky súbory pod DF tachograf.

TCS_418 Podniková karta má túto dátovú štruktúru:

Súborový/dátový prvok	Počet záznamov	Veľkosť (v bajtoch)		Štandardné hodnoty
		Min.	Max.	
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 Nasledovné hodnoty uvedené v tabuľke a používané na údaje o veľkosti, sú minimálnymi a maximálnymi hodnotami, ktoré musí používať dátová štruktúra podnikovej karty:

		Min.	Max.
n_8	NoOfCompanyActivityRecords	230	520

Doplnok 3.

PIKTOGRAMY

PIC_001 Záznamové zariadenie môže používať tieto piktogramy a ich kombinácie:

1. ZÁKLADNÉ PIKTOGRAMY

	Osoby	**Činnosť**	**Prevádzkové režimy**
	Podnik		Režim podniku
	Kontrolór	Kontrola	Režim kontroly
	Vodič	Vedenie	Režim prevádzky
	Dielňa/skúšobňa	Prehliadka/kalibrácia	Režim kalibrácie
	Výrobca		

	Činnosti	**Trvanie**
	Pohotovosť	Súčasný čas pohotovosti
	Vedenie	Nepretržitý čas vedenia
	Odpočinok	Súčasný čas odpočinku
	Práca	Súčasný čas práce
	Prestávka	Kumulovaný čas prestávok
	Neznáme	

	Zariadenie	**Funkcie**
	Slot vodiča	
	Slot druhého vodiča	
	Karta	
	Hodiny	
	Displej	Zobrazovanie
	Vonkajšia pamäť	Sťahovanie
	Napájanie	
	Tlačiareň/výpisy	Tlač
	Snímač	
	Rozmer pneumatiky	
	Vozidlo/jednotka vozidla	

	Špecifické podmienky
	Zariadenie sa nevyžaduje
	Prevoz prevoznou loďou/vlakom

Rôzne

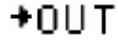
	Udalosti		Poruchy
	Začiatok denného pracovného času		Koniec denného pracovného času
	Miesto		Manuálny zápis činností vodiča
	Bezpečnosť		Rýchlosť
	Čas		Celkom/súhrn

Kvalifikátory

	Denne
	Týždenne
	Dvojtýždenne
	Od do

2. KOMBINÁCIE PIKTOGRAMOV

Rôzne

	Miesto kontroly		
	Miesto začiatku pracovného času		Miesto skončenia pracovného času
	Čas začiatku		Čas skončenia
	Od vozidla		
	Zariadenie sa nevyžaduje – začiatok		Zariadenie sa nevyžaduje – koniec

Karty

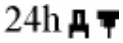
	Karta vodiča
	Podniková karta
	Kontrolná karta
	Dielenská karta
	Žiadna karta

Vedenie

	Posádka
	Čas vedenia počas jedného týždňa
	Čas vedenia počas dvoch týždňov

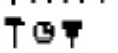
Výpisy


Denný výpis činností vodiča z karty


Denný výpis činností vodiča z JV


Výpis udalostí a porúch z karty


Výpis udalostí a porúch z JV


Výpis technických dát


Výpis prekročenia rýchlosti

Udalosti


Vloženie neplatnej karty


Sporná karta


Časové prekrývanie


Vedenie bez príslušnej karty


Vloženie karty počas vedenia


Nesprávne uzavretá posledná relácia karty


Prekročenie rýchlosti


Prerušenie napájania


Pohybová dátová chyba


Narušenie bezpečnosti


Nastavenie času (dielňou)


Kontrola prekročenia rýchlosti

Poruchy


Chybná funkcia karty (slot vodiča)


Chybná funkcia karty (slot druhého vodiča)


Porucha displeja


Porucha sťahovania


Porucha tlačiarne


Porucha snímača


Vnútorná porucha JV

Postup pri manuálnom zápise

 Ešte ten istý pracovný čas?

 Koniec predchádzajúceho pracovného času?

 Potvrdenie alebo zápis miesta skončenia pracovného času

 Zápis času začiatku

 Zápis miesta začiatku pracovného času

Poznámka: Ďalšie kombinácie piktogramov ako identifikátorov blokov alebo záznamov pri výpisoch, sú definované v doplnku 4.

Doplnok 4

VÝPISY

OBSAH

1. VŠEOBECNE

Každý výpis pozostáva z reťazcov rôznych dátových blokov, ktoré môžu byť identifikované identifikátorom bloku.

Dátový blok obsahuje jeden alebo viac záznamov, ktoré môžu byť identifikované identifikátorom záznamu.

PRT_001 Keď stojí identifikátor bloku bezprostredne pred identifikátorom záznamu, identifikátor záznamu sa nevypíše.

PRT_002 V prípade, že je dátový údaj neznámy alebo sa nesmie vypísať z dôvodov týkajúcich sa prístupových práv k dátam, vypíšu sa namiesto neho prázdne riadky.

PRT_003 Ak je obsah celého riadku neznámy alebo sa nemusí vypísať, celý riadok sa vynechá.

PRT_004 Numerické dátové polia sa vypíšu zarovnané sprava s medzerou pre tisíce a milióny a bez úvodných núl.

PRT_005 Reťazcové dátové polia sa vypíšu zarovnané zľava a podľa potreby vyplnené prázdnymi riadkami pre dĺžku dátového prvku alebo skrátené na dĺžku dátového prvku (mená a adresy).

2. ŠPECIFIKÁCIE DÁTOVÝCH BLOKOV

V tejto kapitole sa použila táto dohoda o formátovej notácii:

– znaky vytlačené tučne znamenajú nešifrovaný text, ktorý sa má vytlačiť (tlačia sa normálne znaky),

– normálne znaky znamenajú premenné (piktogramy alebo dáta), ktoré majú byť pri tlači nahradené ich hodnotami,

– označenia premenných boli doplnené znakom podčiarknutia, aby sa zviditeľnila dĺžka dátového prvku, ktorá je k dispozícii pre premenné,

– dátumy sú vo formáte „dd/mm/rrrr“ (deň, mesiac, rok). Môže sa použiť aj formát „dd.mm.rrrr“.

– pojem „identifikácia karty“ znamená zoskupenie týchto prvkov: typ karty prostredníctvom kombinácie piktogramov, kód členského štátu, ktorý kartu vydáva, šikmej čiary (lomítka) a čísla karty s náhradným indexom a indexom obnovy, oddelených medzerou:

P		x	x	x	/	x	x	x	x	x	x	x	x	x	x	x	x–	x	x		x		x
Kombinácia piktogramu karty		Kód členského štátu, ktorý kartu vydáva				Prvých 14 znakov čísla karty (možné s poradovým indexom)															Index náhrady		Index obnovy

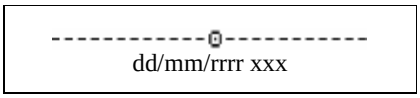
PRT_006 Výpisy používajú nasledovné dátové bloky a/alebo dátové záznamy, v súlade s týmto významom a formátmi:

Číslo bloku alebo záznamu Význam	Dátový formát
1. **Dátum a čas výpisu**	dd/mm/rrrr: mm **(UTC)**
2. **Typ výpisu** Identifikátor bloku Kombinácia piktogramu výpisu (pozri doplnok 3), zariadenie na obmedzenie rýchlosti (len pri výpise prekročenia rýchlosti)	---------- Picto xxx **km/h**
3. **Identifikácia držiteľa karty** Identifikátor bloku. P = piktogram osoby Priezvisko držiteľa karty Prípadne meno(á) držiteľa karty Identifikácia karty Dátum skončenia platnosti karty (ak je) V prípade, že ide o neosobnú kartu, bez mena priezviska držiteľa karty, vytlačí sa namiesto toho názov podniku, dielne alebo kontrolného orgánu.	----------P---------- P Last_Name _____ First_Name _____ Card_Identification _____ dd/mm/rrrr
4. **Identifikácia vozidla** Identifikátor bloku (VIN) Registrujúci členský štát a registračné číslo vozidla	----------A---------- A VIN _____ Nat/VRN _____
5. **Identifikácia JV** Identifikátor bloku Meno výrobcu JV Číslo časti JV	----------B---------- B VU_Manufacturer _____ VU_Part_Number _____
6. **Posledná kalibrácia záznamového zariadenia** Identifikátor bloku Názov dielne Identifikácia dielenskej karty Dátum kalibrácie	----------T---------- T Last_Name _____ Card_Identification _____ T dd/mm/rrrr
7. **Posledná kontrola (kontrolórom)** Identifikátor bloku Identifikácia kontrolnej karty Dátum, čas a druh kontroly Druh kontroly: až do štyroch piktogramov. Druh kontroly môže byť kombináciou: sťahovania z karty, sťahovania z JV, tlače, zobrazovania	----------C---------- Card_Identification _____ C dd/mm/rrrr hh:mm pppp

8. **Činnosti vodiča uložené na karte v poradí v akom sa vykonávajú**

Identifikátor bloku

Dátum dopytu (kalendárny deň výpisu) + počítadlo dennej prítomnosti



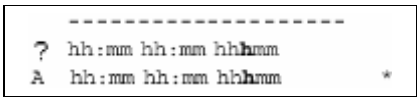
8.1 *Perióda, počas ktorej nebola karta vložená*

8.1a Identifikátor záznamu (začiatok časového úseku)

8.1b *Neznámy čas. úsek.* Čas začiatku a konca, trvanie

8.1c *Manuálne zapísané činnosti*

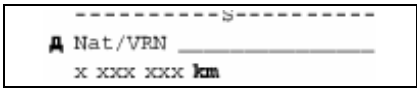
Piktogram činnosti, čas začiatku a konca (vrátane), trvanie, odpočinkové časy v trvaní minimálne jednej hodiny sú označené hviezdičkou.



8.2 *Vloženie karty do slotu S*

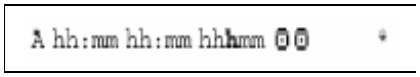
Členský štát registrujúci vozidlo a registračné číslo vozidla

Stav kilometrov pri vložení karty.

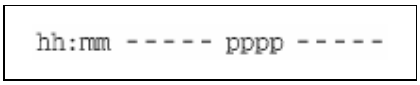


8.3 *Činnosť (zatiaľčo je karta vložená)*

Piktogram činnosti, čas začiatku a konca (vrátane), trvanie, stav vedenia vozidla (piktogram posádky ak ide o POSÁDKA, prázdne pri JEDEN VODIČ), odpočinkové časy v trvaní minimálne jednej hodiny sú označené hviezdičkou.

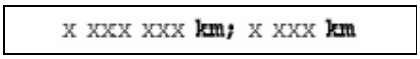


8.3a *Špecifická podmienka.* Čas zápisu, piktogram špeci–fickej podmienky (alebo kombinácia piktogramu)



8.4 *Vytiahnutie karty*

Stav kilometrov a ubehnutá vzdialenosť od posledného vloženia, pri ktorom je známy stav kilometrov.



9. **Činnosti vodiča uložené v JV podľa slotu v chronologickom poradí**

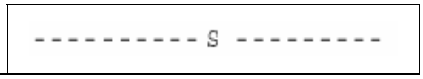
Identifikátor bloku

Čas dopytu (kalendárny deň výpisu)

Stav kilometrov vozidla pri 00.00 a 24.00

10. **Činnosti v slote S**

Identifikátor bloku

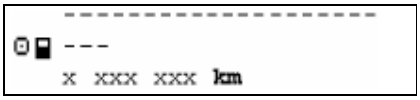


10.1 *Perióda, počas ktorej nie je vložená v slote S žiadna karta*

Identifikátor záznamu

Nie je vložená žiadna karta

Stav kilometrov na začiatku časového úseku



10.2 *Vloženie karty*

Identifikátor záznamu vloženia karty

Priezvisko vodiča

Meno vodiča

Identifikácia karty vodiča

Dátum skončenia platnosti karty vodiča

Členský štát registrujúci vozidlo a registračné číslo predchádzajúceho vozidla

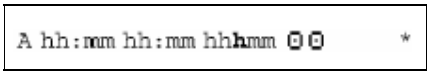
Dátum a čas vytiahnutia karty z prechádzajúceho vozidla

Prázdny riadok

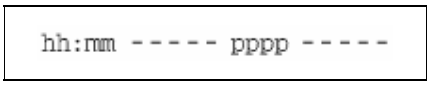
Stav kilometrov pri vložení karty, manuálny zápis znaku činností vodiča (M ak áno, prázdne ak nie).

10.3 *Činnosť*

Piktogram činnosti, čas začiatku a konca (vrátane), trvanie, stav vedenia vozidla (piktogram posádky ak ide o POSÁDKA, prázdne pri JEDEN VODIČ), odpočinkové časy v trvaní minimálne jednej hodiny sú označené hviezdičkou.

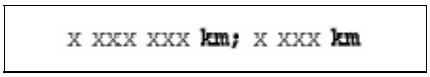


10.3a *Špecifická podmienka*. Čas zápisu, piktogram špe–cifickej podmienky (alebo kombinácia piktogramu).



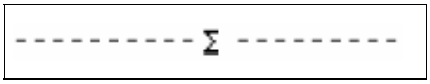
10.4 *Vytiahnutie karty alebo koniec časového úseku „Žiadna karta“*

Stav kilometrov pri vytiahnutí karty alebo na konci časového úseku „Žiadna karta“ a ubehnutá vzdialenosť od vloženia, alebo od začiatku časového úseku „Žiadna karta“.



11. **Denný súhrn**

Identifikátor bloku.



11.1 *Súčet časových úsekov JV bez karty v slote vodiča*

Identifikátor bloku.

11.2 *Súčet časových úsekov JV bez karty v slote druhého vodiča*

Identifikátor bloku.

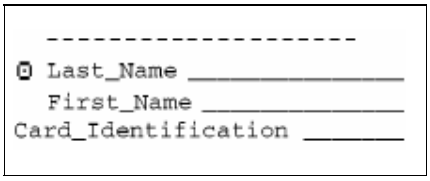
11.3 *Denný súhrn JV na vodiča*

Identifikátor záznamu

Priezvisko vodiča

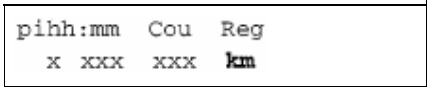
Meno vodiča

Identifikácia karty vodiča.



11.4 *Zápis miesta, kde denný pracovný čas začína a/alebo končí*

pi = piktogram miesta začiatku/skončenia, čas, štát, región, stav kilometrov.



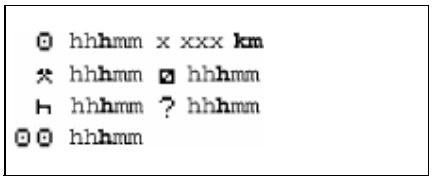
11.5 *Činnosti celkom (z karty)*

Celkový čas vedenia, ubehnutá vzdialenosť

Celkový čas práce a pohotovosti

Celkový čas odpočinku a neznámy čas

Celkový čas činností posádky.

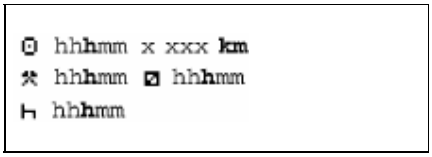


11.6 *Činnosti celkom (časové úseky bez karty v slote vodiča)*

Celkový čas vedenia, ubehnutá vzdialenosť

Celkový čas práce a pohotovosti

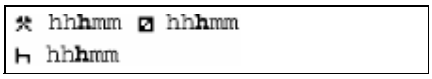
Celkový čas odpočinku.



11.7 *Činnosti celkom (časové úseky bez karty v slote druhého vodiča)*

Celkový čas práce a pohotovosti

Celkový čas odpočinku.



11.8 *Činnosti celkom (na vodiča, oba sloty)*

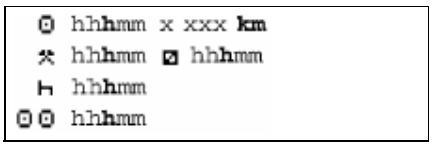
Celkový čas vedenia, ubehnutá vzdialenosť

Celkový čas práce a pohotovosti

Celkový čas odpočinku

Celkový čas činností posádky

Keď sa vyžaduje výpis za aktuálny deň, denné súhrnné informácie sa vypočítajú s dátami dostupnými v dobe výpisu.

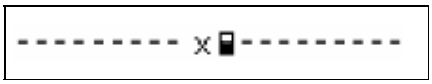


12. **Udalosti a/alebo poruchy uložené na karte**

12.1 Identifikátor bloku posledných 5 udalostí a porúch na karte

12.2 Identifikátor bloku všetkých zaznamenaných udalostí na karte

12.3 Identifikátor bloku všetkých zaznamenaných porúch na karte



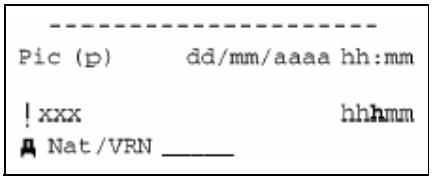
12.4 *Záznamy udalostí a/alebo porúch*

Identifikátor záznamu

Piktogram udalosti/poruchy, účel záznamu, dátum a čas začiatku,

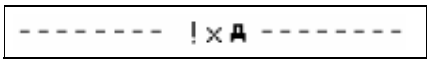
Ďalší kód udalosti/poruchy (ak je), trvanie

Členský štát registrujúci vozidlo a registračné číslo vozidla, u ktorého udalosť alebo porucha nastala.

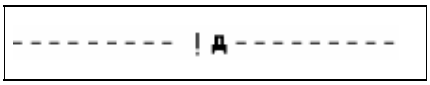


13. **Udalosti a/alebo poruchy uložené alebo prebiehajúce v JV**

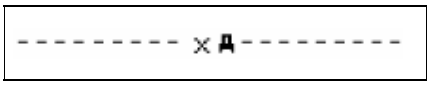
13.1 Identifikátor bloku posledných 5 udalostí a porúch v JV.



13.2 Identifikátor bloku všetkých zaznamenaných alebo prebiehajúcich udalostí v JV.



13.3 Identifikátor bloku všetkých zaznamenaných alebo prebiehajúcich porúch v JV.



13.4 *Záznamy udalostí a/alebo porúch*

Identifikátor záznamu

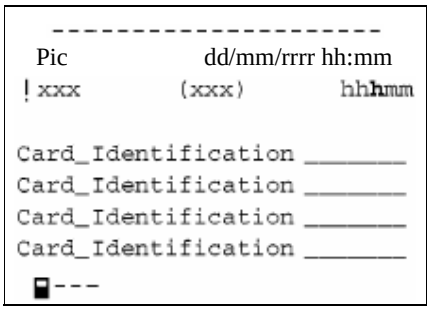
Piktogram udalosti/poruchy, účel záznamu, dátum a čas začiatku,

Ďalší kód udalosti/poruchy (ak je), Žiadna podobná udalosť v tomto dni, trvanie

Identifikácia karty vloženej na začiatku alebo konci udalosti alebo poruchy (až do 4 riadkov bez opakovania tohto istého čísla karty)

Prípad keď nebola vložená žiadna karta

Účel záznamu (p) je numerický kód vysvetľujúci, prečo bola udalosť alebo porucha zaznamenaná, kódovanie v súlade s dátovým prvkom EventFaultRecordPurpose



14. **Identifikácia vozidla**

Identifikátor bloku

Meno výrobcu JV

Adresa výrobcu JV

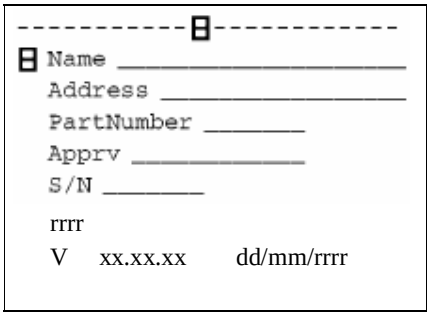
Číslo časti JV

Schvaľovacie číslo JV

Sériové číslo JV

Rok výroby JV

Verzia a dátum inštalácie softwaru JV



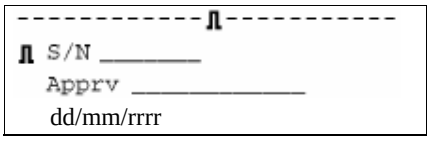
15. **Identifikácia snímača**

Identifikátor bloku

Sériové číslo snímača

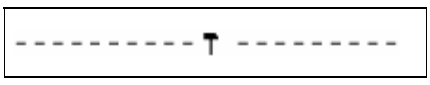
Schvaľovacie číslo snímača

Dátum prvej inštalácie snímača



16. **Kalibračné dáta**

Identifikátor bloku

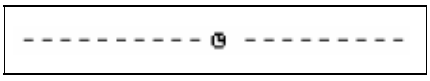


16.1 *Kalibračný záznam*

Identifikátor záznamu
Dielňa, ktorá má kalibráciu vykonať
Adresa dielne
Identifikácia dielenskej karty
Dátum skončenia platnosti dielenskej karty
Prázdny riadok
Dátum kalibrácie – účel kalibrácie
VIN
Registrujúci členský štát a registračné číslo vozidla
Charakteristický koeficient vozidla
Konštanta záznamového zariadenia
Účinný obvod pneumatík kolesa
Rozmer montovaných pneumatík
Nastavenie zariadenia obmedzujúceho rýchlosť
Staré a nové hodnoty počítadla kilometrov
Účel kalibrácie (p) je numerický kód vysvetľujúci, prečo boli tieto kalibračné parametre zaznamenané, kódovanie v súlade s dátovým prvkom CalibrationPurpose

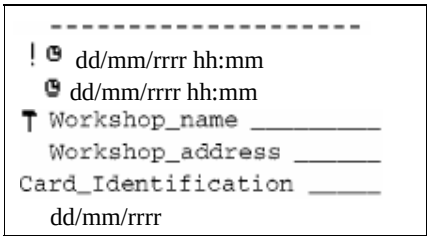
17. **Nastavenie času**

Identifikátor bloku



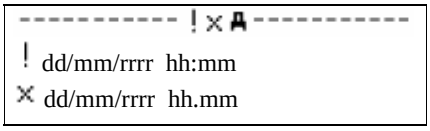
17.1 *Záznam nastavenia času*

Identifikátor záznamu
Starý dátum a čas
Nový dátum a čas
Dielňa, ktorá má nastavenie času vykonať
Adresa dielne
Identifikácia dielenskej karty
Dátum skončenia platnosti dielenskej karty



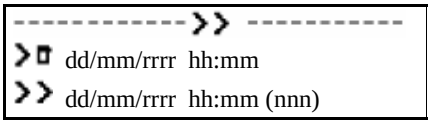
18. **Najnovšia udalosť a porucha zaznamenaná v JV**

Identifikátor bloku
Dátum a čas najnovšej udalosti
Dátum a čas najnovšej poruchy



19. **Informácie ku kontrole prekročenia rýchlosti**

Identifikátor bloku
Dátum a čas poslednej KONTROLY PREKROČENIA RÝCHLOSTI
Dátum/čas prvého prekročenia rýchlosti a počet ďalších udalostí prekročenia rýchlosti



20. **Záznam o prekročení rýchlosti**

20.1 Identifikátor bloku „Prvé prekročenie rýchlosti po poslednej kalibrácii“.

```
-------- >>T --------
```

20.2 Identifikátor bloku „5 najvážnejších prekročení za posledných 365 dní“.

```
------- >>(365) -------
```

20.3 Identifikátor bloku „Najvážnejšie prekročenie rýchlosti za každý z posledných 10 dní výskytu“.

```
------- >>(10) -------
```

20.4 Identifikátor záznamu
Dátum, čas a trvanie
Maximálna a priemerná rýchlosť, Žiadne podobné udalosti v tomto dni
Priezvisko vodiča
Meno(á) vodiča
Identifikácia karty vodiča

```
-----------------
>> dd/mm/rrrr hh:mm hhhmm
   xxx km/h xxx km/h (xxx)
   Last_Name _____________
   First_Name _____________
Card_Identification _______
```

20.5 Ak nie je v bloku žiadny záznam o prekročení rýchlosti

```
>> - - -
```

21. **Rukou písané informácie**
Identifikátor bloku
21.1 Miesto kontroly
21.2 Podpis kontrolóra
21.3 Čas začiatku
21.4 Čas skončenia
21.5 Podpis vodiča
„Rukou písané informácie“: Vložiť dostatočný počet prázdnych riadkov nad rukou písaný záznam, aby bol dostatok miesta pre požadované informácie alebo podpis.

```
-------------------------
                .....
                .....
                .....
                .....
                .....
```

3. ŠPECIFIKÁCIE VÝPISOV

V tejto kapitole sa použila nasledovná dohoda o notácii:

N	Číslo N bloku tlače alebo záznamu
N	Číslo bloku tlače alebo záznamu opakované podľa potreby
X/Y	Bloky tlače alebo záznamy X a/alebo Y podľa požiadavky, opakovanie podľa potreby

3.1 **Denný výpis činností vodiča z karty**

PRT_007 Denný výpis činností vodiča z JV musí byť v súlade s týmto formátom:

1	Dátum a čas tlače dokumentu
2	Typ výpisu
3	Identifikácia kontrolóra (ak je kontrolná karta vložená v JV)
3	Identifikácia vodiča (z karty, ktorej sa výpis berie)
4	Identifikácia vozidla (vozidlo, z ktorého sa výpis berie)
5	Identifikácia JV (JV, z ktorej sa výpis berie)
6	Posledná kalibrácia tejto JV
7	Posledná kontrola, ktorej sa tento kontrolovaný vodič podrobil
8	Oddeľovač činností vodiča
8.1a / 8.1b / 8.1c / 8.2 / 8.3 / 8.3a / 8.4	Činnosti vodiča v poradí, akom sa vykonávali
11	Oddeľovač denného súhrnu
11.4	Miesta zapísané v chronologickom poradí
11.5	Činnosti celkom
12.1	Oddeľovač udalostí alebo porúch z karty
12.4	Záznamy udalosť/porucha (posledných 5 udalostí alebo porúch uložených na karte)
13.1	Oddeľovač udalostí alebo porúch z JV
13.4	Záznamy udalosť/porucha (posledných 5 udalostí alebo porúch uložených alebo prebiehajúcich v JV)
21.1	Miesto kontroly
21.2	Podpis kontrolóra
21.5	Podpis vodiča

3.2 Denný výpis činností vodiča z JV

PRT_008 Denný výpis činností vodiča z JV musí byť v súlade s týmto formátom:

1	Dátum a čas tlače dokumentu
2	Typ výpisu
3	Identifikácia držiteľa karty (pre všetky karty vložené v JV)
4	Identifikácia vozidla (vozidlo, z ktorého sa výpis berie)
5	Identifikácia JV (JV, z ktorej sa výpis berie)
6	Posledná kalibrácia tejto JV
7	Posledná kontrola tohto záznamového zariadenia
9	Oddeľovač činností vodiča
10	Oddeľovač drážky vodiča (drážka 1)
10.1 / 10.2 / 10.3 /10.3a / 10.4	Činnosti v chronologickom poradí (drážka vodiča)
10	Oddeľovač drážky druhého vodiča (drážka 2)
10.1 / 10.2 / 10.3 /10.3a / 10.4	Činnosti v chronologickom poradí (drážka druhého vodiča)
11	Oddeľovač denného súhrnu
11.1	Súčet období bez karty v drážke vodiča
11.4	Miesta zapísané v chronologickom poradí
11.6	Činnosti celkom

11.2	Súčet období bez karty v drážke druhého vodiča	
11.4	Miesta zapísané v chronologickom poradí	
11.7	Činnosti celkom	
11.3	Súhrn činností vodiča, obe drážky	
11.4	Miesta zapísané týmto vodičom v chronologickom poradí	
11.7	Činnosti celkom pre tohto vodiča	
13.1	Oddeľovač udalostí alebo porúch	
13.4	Záznamy udalosť/porucha (posledných 5 udalostí alebo porúch uložených alebo prebiehajúcich v JV)	
21.1	Miesto kontroly	
21.2	Podpis kontrolóra	(miesto, v ktorom vodič bez karty môže uviesť, ktoré periódy sa naňho vzťahujú)
21.3	Čas začiatku	
21.4	Čas skončenia	
21.5	Podpis vodiča	

3.3 **Výpis udalostí a porúch z karty**

PRT_009 Výpis udalostí a porúch z karty musí byť v súlade s týmto formátom:

1	Dátum a čas tlače dokumentu
2	Typ výpisu
3	Identifikácia kontrolóra (ak je kontrolná karta vložená v JV)
3	Identifikácia vodiča (z karty, z ktorej sa výpis berie)
4	Identifikácia vozidla (vozidlo, z ktorého sa výpis berie)
12.2	Oddeľovač udalostí
12.4	Záznamy udalostí (všetky udalosti uložené na karte)
12.3	Oddeľovač porúch
12.4	Záznamy porúch (všetky poruchy uložené na karte)
21.1	Miesto kontroly
21.2	Podpis kontrolóra
21.5	Podpis vodiča

3.4 **Výpis udalostí a porúch z JV**

PRT_010 Výpis udalostí a porúch z JV musí byť v súlade s týmto formátom:

1	Dátum a čas tlače dokumentu
2	Typ výpisu
3	Identifikácia držiteľa karty (pre všetky karty vložené v JV)
4	Identifikácia vozidla (vozidlo, z ktorého sa výpis berie)
13.2	Oddeľovač udalostí
13.4	Záznamy udalostí (všetky udalosti uložené alebo prebiehajúce v JV)
13.3	Oddeľovač porúch
13.4	Záznamy porúch (všetky poruchy uložené alebo prebiehajúce v JV)
21.1	Miesto kontroly
21.2	Podpis kontrolóra
21.5	Podpis vodiča

3.5 **Výpis technických dát**

PRT_011 Výpis technických dát musí byť v súlade s týmto formátom:

1	Dátum a čas tlače dokumentu
2	Typ výpisu
3	Identifikácia držiteľa karty (pre všetky karty vložené v JV)
4	Identifikácia vozidla (vozidlo, z ktorého sa výpis berie)
14	Identifikácia JV
15	Identifikácia snímača
16	Oddeľovač kalibračných dát
16.1	Kalibračné záznamy (všetky dostupné záznamy v chronologickom poradí)
17	Oddeľovač nastavenia času
17.1	Záznamy o nastavení času (všetky záznamy dostupné zo záznamov o nastavení času a kalibrácii)
18	Najnovšia udalosť a porucha zaznamenaná v JV

3.6 **Výpis prekročenia rýchlosti**

PRT_012 Výpis prekročenia rýchlosti musí byť v súlade s týmto formátom:

1	Dátum a čas tlače dokumentu
2	Typ výpisu
3	Identifikácia držiteľa karty (pre všetky karty vložené v JV)
4	Identifikácia vozidla (vozidlo, z ktorého sa výpis berie)
19	Informácie o kontrole prekročenia rýchlosti
20.1	Identifikátor dát o prekročení rýchlosti
20.4 / 20.5	Prvé prekročenie rýchlosti po poslednej kalibrácii
20.2	Identifikátor dát o prekročení rýchlosti
20.4 / 20.5	5 najvážnejších udalostí prekročenia rýchlosti za posledných 365 dní
20.3	Identifikátor dát o prekročení rýchlosti
20.4 / 20.5	Najvážnejšie prekročenie rýchlosti za každý z posledných 10 dní výskytu
21.1	Miesto kontroly
21.2	Podpis kontrolóra
21.5	Podpis vodiča

Doplnok 5

DISPLEJ

V tomto doplnku sa použila táto dohoda o formátovej notácii:

– znaky vytlačené tučne znamenajú nešifrovaný text, ktorý sa má zobraziť (zobrazia sa normálne znaky),

– normálne znaky znamenajú premenné (piktogramy alebo dáta), ktoré majú byť pri zobrazení nahradené ich hodnotami:

dd mm rrrr:	deň mesiac rok,
hh:	hodiny,
mm:	minúty
D:	piktogram trvania,
EF:	kombinácia piktogramov udalostí alebo porúch
O:	piktogram prevádzkového režimu

DIS_001 Záznamové zariadenie musí zobraziť dáta v týchto formátoch:

Dáta	Formato
Štandardný displej	
Miestny čas	hh:mm
Prevádzkový režim	O
Informácie týkajúce sa vodiča	1Dhh**h**mm ▮▮hh**h**mm
Informácie týkajúce sa druhého vodiča	2Dhh**h**mm
Otvorená podmienka „zariadenie sa nevyžaduje“	OUT
Výstražný displej	
Prekročenie nepretržitého času vedenia	10hhhmm ▮▮hhhmm
Udalosť alebo porucha	EF
Iné displeje	
UTC dátum čas	UTC dd/mm/aaaa o bien UTC dd.mm.aaaa hh:mm
Nepretržitý čas vedenia a kumulovaný čas prestávok vodiča	10hhhmm ▮▮hhhmm
Nepretržitý čas vedenia a kumulovaný čas prestávok druhého vodiča	20hhhmm ▮▮hhhmm
Kumulovaný nepretržitý čas vedenia vodiča za predchádzajúci a prebiehajúci týždeň	10▮hhhhmm
Kumulovaný nepretržitý čas vedenia druhého vodiča za predchádzajúci a prebiehajúci týždeň	20▮hhhhmm

Doplnok 6

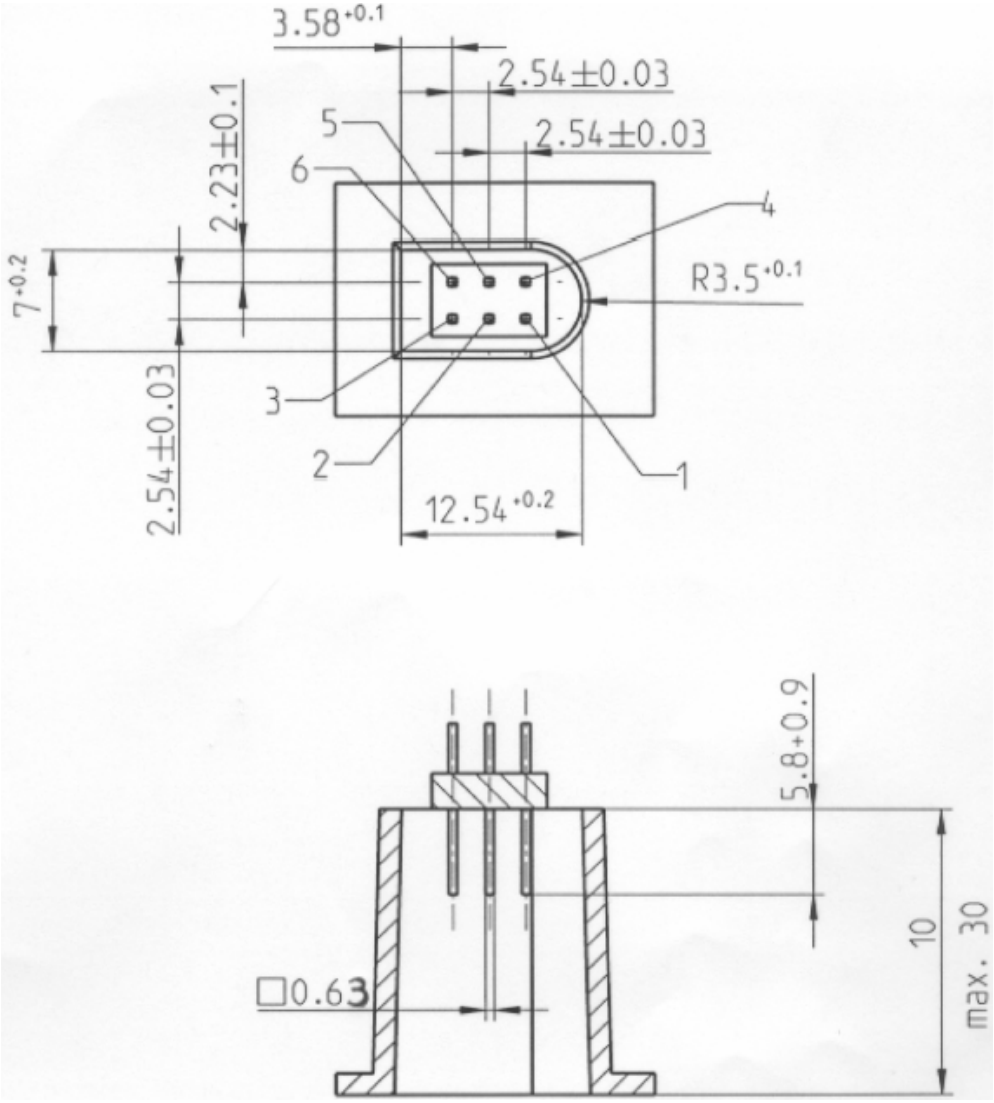
VONKAJŠIE ROZHRANIA

OBSAH

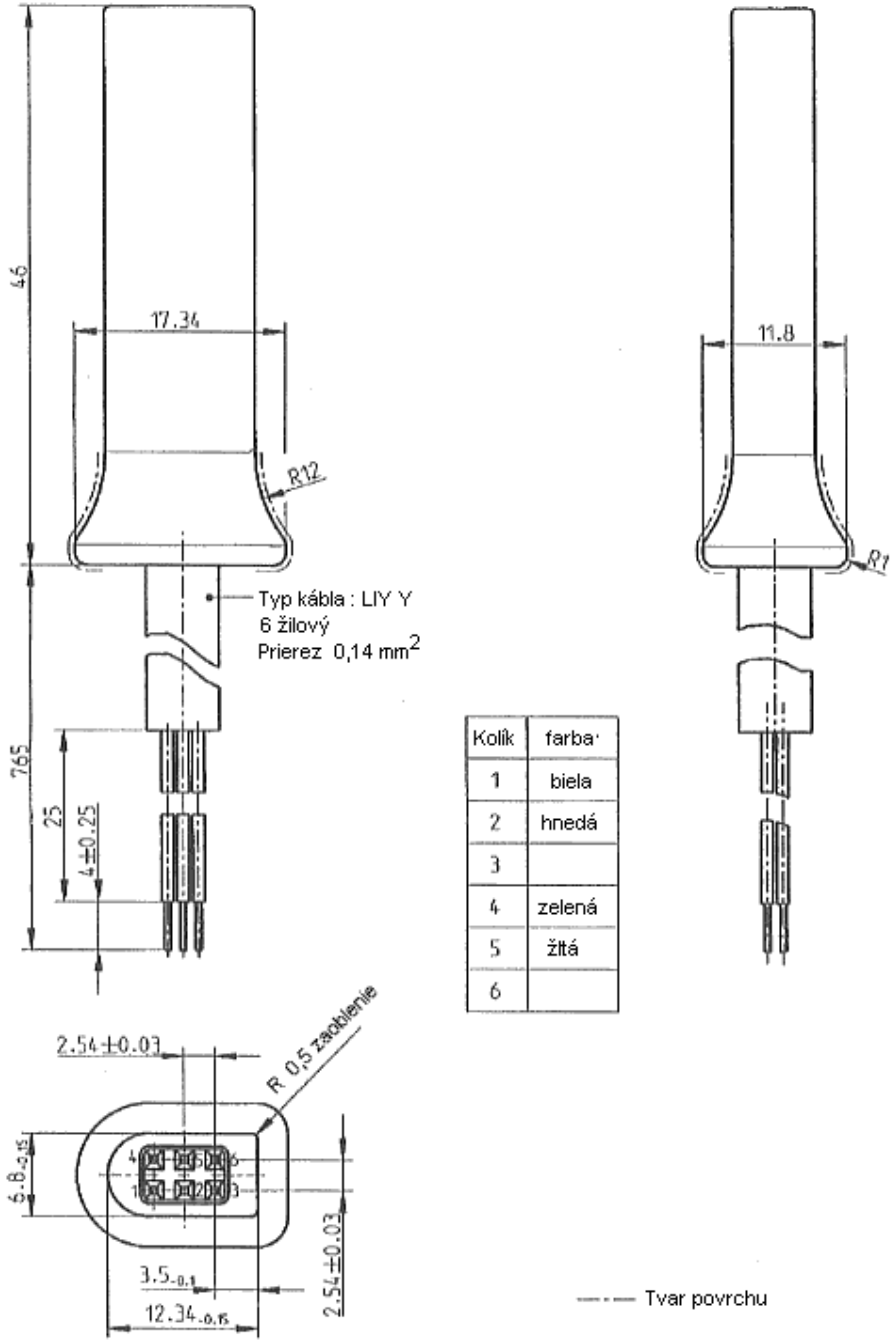
1. Hardware

1.1 **Konektor**

INT_001 Konektor sťahovania/kalibrácie musí byť šesťkolíkový, prístupný z predného panelu bez potreby odpojenia akejkoľvek časti záznamového zariadenia a musí zodpovedať nasledovným náčrtom (všetky rozmery v milimetroch):



Nasledovný náčrt ukazuje typickú šesťkolíkovú zástrčku:



Kolík	farba
1	biela
2	hnedá
3	
4	zelená
5	žltá
6	

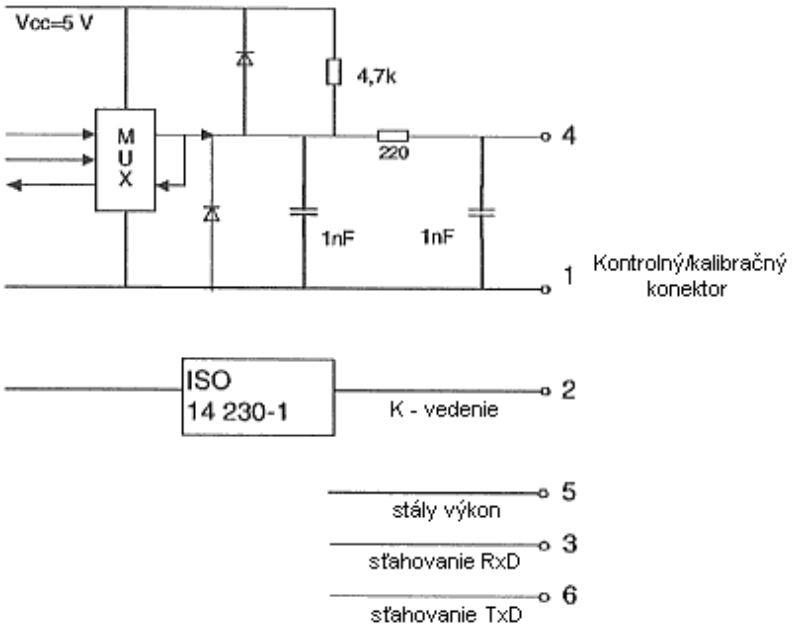
1.2 **Rozloženie kontaktov**

INT_002 Kontakty musia byť rozložené v súlade s touto tabuľkou:

Kolík	Popis	Poznámka
1	Záporný pól batérie	Pripojený k zápornému pólu batérie vozidla
2	Dátová komunikácia	K vedenie (ISO 14 230–1)
3	RxD – sťahovanie	Dátový vstup do záznamového zariadenia
4	Vstupný/výstupný signál	Kalibrácia
5	Stály výstupný prúd	Rozsah napätia je špecifikovaný ako rozsah napätia vozidla mínus 3V, aby bol možný pokles napätia v ochrannom prúdovom obvode Výkon: 40 mA
6	TxD – sťahovanie	Dátový výstup zo záznamového zariadenia

1.3 **Blokový diagram**

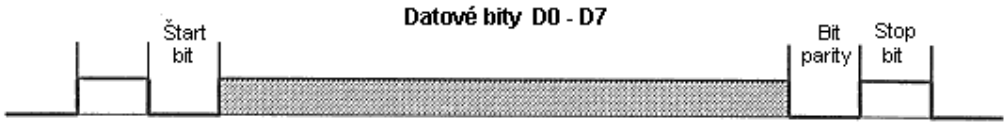
INT_003 Blokový diagram musí byť zhodný s týmto:



2. ROZHRANIE PRE SŤAHOVANIE

INT_004 Rozhranie pre sťahovanie musí zodpovedať špecifikáciám RS232.

INT_005 Rozhranie pre sťahovanie používa jeden štart bit, 8 dátových bitov s bitom najnižšieho rádu na prvom mieste, jeden bit párnej parity a jeden stop bit.



Organizácia dátového bajtu

Štart bit: jeden bit s logickou úrovňou 0

Dátové bity: na prvom mieste bit najnižšieho rádu

Paritný bit: párna parita

Stop bit: jeden bit s logickou úrovňou 1

Keď sa prenášajú numerické dáta zložené z viac než jedného bajtu, bajt najvyššieho rádu sa prenáša prvý a bajt najnižšieho rádu posledný.

INT_006 Prenosová rýchlosť musí byť nastaviteľná od 9 600 bps do 115 200 bps. Prenos sa uskutoční pri najvyššej možnej prenosovej rýchlosti, pričom počiatočná prenosová rýchlosť po začiatku komunikácie sa nastaví na 9 600 bps.

3. ROZHRANIE PRE KALIBRÁCIU

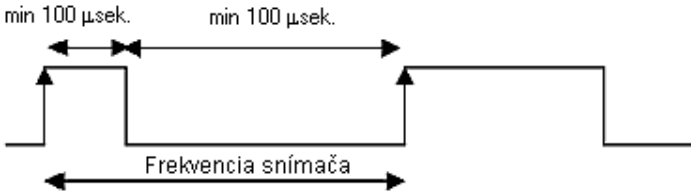
INT_007 Dátová komunikácia musí zodpovedať norme ISO 14 230–1 – Diagnostické systémy – Protokol Kľúčového slova 2000 – Časť 1: Fyzikálna vrstva, prvé vydanie: 1999.

INT_008 Vstupný/výstupný signál musí zodpovedať nasledovným elektrickým špecifikáciám:

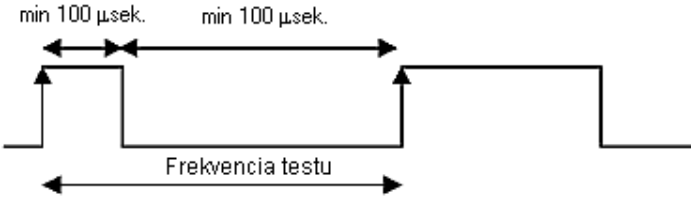
Parameter	Minimum	Typický	Maximum	Poznámka
U_{low}(vstup)			1,0 V	I = 750 μA
U_{high}(vstup)	4 V			I = 200 μA
Frekvencia			4 kHz	
U_{low}(výstup)			1,0 V	I = 1mA
U_{high}(výstup)	4 V		1,0 V	I = 1mA

INT_008 Vstupný/výstupný signál musí zodpovedať nasledovným časovým diagramom:

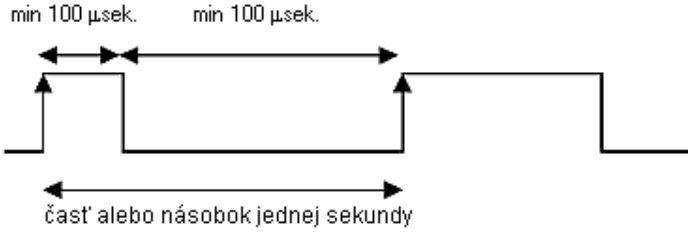
Signál snímača (odchádzajúci)



Testovací signál prichádzajúci)



UTC signál hodinových impulzov (odchádzajúci)



Doplnok 7

PROTOKOLY O SŤAHOVANÍ DÁT

OBSAH

1 ÚVOD

Tento doplnok špecifikuje postup pre rôzne druhy prenosu dát z karty na vonkajšie pamäťové médium spolu s protokolmi, ktoré musia byť zavedené preto, aby bol zaručený správny prenos dát a úplná kompatibilita formátu sťahovaných dát tak, aby kontrolór mohol overiť tieto dáta a mohol pred ich analýzou skontrolovať ich autenticitu a integritu.

1.1 **Rozsah pôsobnosti**

Sťahovanie dát na ESM sa môže uskutočniť:

– z jednotky vozidla pomocou „intelligent dedicated equipment (IDE)“ pripojeným k JV,

– z tachografovej karty pomocou IDE vybaveného prepojovacím zariadením karty (IFD),

– z tachografovej karty cez jednotku vozidla pomocou IDE pripojeného k JV.

Aby bolo možné overiť autenticitu a integritu sťahovaných dát uložených na ESM, dáta sa sťahujú s pripojeným podpisom v súlade s doplnkom 11 Spoločných bezpečnostných mechanizmov. Sťahujú sa aj údaje o identifikácii zdrojového zariadenia (JV alebo karty) a jeho bezpečnostných osvedčení (členský štát a zariadenie). Overovateľ dát musí vlastniť nezávislý a spoľahlivý európsky verejný kľúč.

DDP_001 Dáta sťahované počas relácie sťahovania musia byť uložené v ESM v jednom súbore.

1.2 **Akronymy a notácie**

V tomto doplnku sa používajú tieto akronymy a notácie

AID	application identifier (identifikátor aplikácie)
ATR	answer to reset (odpoveď na resetovanie)
CS	checksum byte (bajt kontrolného súčtu)
DF	dedicated file (vyhradený súbor)
DS_	diagnostic session (diagnostická relácia)
EF	elementary file (elementárny súbor)
ESM	external storage medium (vonkajšie pamäťové médium)
FID	file identifier (File ID, identifikátor súboru)
FMT	formátový bajt (prvý bajt záhlavia správy)
ICC	integrated circuit card (karta s integrovaným obvodom)
IDE	intelligent dedicated equipment: prístroj používaný na sťahovanie dát na ESM (napr. osobný počítač)
IFD	interface device (prepojovacie zariadenie)
KWP	keyword protocol 2000
LEN	length byte (posledný bajt záhlavia správy)
PPS	protocol parameter selection (voľba parametra protokolu)
PSO	perform security operation (vykonanie bezpečnostnej operácie)
SID	service identifier (identifikátor služby)
SRC	source byte (zdrojový bajt)
TGT	target byte (cieľový bajt)
TLV	tag length value (hodnota dĺžky tagu)

TREP transfer response parameter (parameter prenosu odpovede)

TRTP transfer request (prenos požiadavky)

VU vehicle unit (jednotka vozidla – JV)

2. SŤAHOVANIE DÁT Z JEDNOTKY VOZIDLA

2.1 **Postup sťahovania**

Za účelom sťahovania dát z JV, musí operátor vykonať nasledovné operácie:

– vložiť svoju tachografovú kartu do slotu JV[(1)],

– pripojiť IDE ku konektoru sťahovania JV,

– vytvoriť spojenie medzi IDE a JV,

– zvoliť na IDE dáta, ktoré treba sťahovať a odoslať požiadavku na JV,

– uzavrieť reláciu sťahovania dát.

2.2 **Protokol sťahovania dát**

Protokol je štruktúrovaný na master–slave základe, s IDE v úlohe master a s JV v úlohe slave.

Štruktúra správy, typy a tok spočívajú v zásade na Keyword Protokol 2000 (KWP) (ISO 14230–2 Cestné vozidlá – Diagnostické systémy – Kľúčový protokol 2000 – Časť 2: Vrstva riadenia dátových spojov).

Aplikačná vrstva spočíva v zásade na súčasnom návrhu normy ISO 14229–1 (Cestné vozidlá – Diagnostické systémy – Časť 1: Diagnostické služby, verzia 6 z 22. februára 2001).

2.2.1 ***Štruktúra správy***

DDP_002 Všetky správy vymieňané medzi IDE a JV sú formátované so štruktúrou pozostávajúcou z troch častí:

– záhlavie pozostávajúce z formátového bajtu (FMT), cieľového bajtu (TGT) a zdrojového bajtu (SRC) a možno dĺžkového bajtu (LEN),

– dátové pole pozostávajúce z bajtu identifikátora služby (SID) a variabilného počtu dátových bajtov, ktoré môžu zahŕňať voliteľný bajt diagnostickej relácie (DS_) alebo voliteľný bajt parametra prenosu (TRTP alebo TREP).

– kontrolný súčet pozostávajúci z bajtu kontrolného súčtu (CS).

(1) Vložená karta spustí požadované prístupové práva k funkcii sťahovania a k dátam.

Záhlavie				Dátové pole					Kontrolný súčet
FMT	TGT	SRC	LEN	SID	DATA	…	…	…	CS
4 bajty				Maximálne 225 bajtov					1 bajt

Bajt TGT a SRC predstavuje fyzickú adresu príjemcu a pôvodcu správy. Hodnoty sú F0 Hex pre IDE a EE Hex pre JV.

Bajt LEN je dĺžka časti dátového poľa.

Bajt kontrolného súčtu je 8 bitový súčet modulo 256 všetkých bajtov správy, okrem samotného CS.

Bajty FMT, SID, DS_, TRTP a TREP sú definované na inom mieste tohto dokumentu.

DDP_003 V prípade keď sú dáta prenášané v správe dlhšie než disponibilné miesto v časti dátového poľa, správa sa odošle v niekoľkých čiastkových správach. Každá čiastková správa musí mať záhlavie, rovnaký SID, TREP a 2–bajtové počítadlo čiastkovej správy udávajúce číslo čiastkovej správy v rámci celej správy. Aby bola možná kontrola chýb a zrušenie, IDE potvrdzuje každú čiastkovú správu. IDE môže prijať čiastkovú správu, požiadať o nový prenos ako aj požadovať od JV aby znovu zahájila alebo zrušila prenos.

DDP_004 Ak posledná čiastková správa obsahuje presne 255 bajtov v dátovom poli, musí byť pripojená konečná čiastková správa s prázdnym (okrem počítadla čiastkovej správy SID TREP) dátovým poľom, aby bol zrejmý koniec správy.

Príklad:

Záhlavie	SID	TREP	Správa	CS
4 bajty	Dlhšia než 255 bajtov			

bude sa prenášať ako:

Záhlavie	SID	TREP	00	01	Čiastková správa 1	CS
4 bajty	255 bajtov					

Záhlavie	SID	TREP	00	01	Čiastková správa 2	CS
4 bajty	255 bajtov					

Záhlavie	SID	TREP	xx	yy	Čiastková správa n	CS
4 bajty	Menej než 255 bajtov					

alebo ako:

Záhlavie	SID	TREP	00	01	Čiastková správa 1	CS
4 bajty	255 bajtov					

Záhlavie	SID	TREP	00	02	Čiastková správa 2	CS
4 bajty	255 bajtov					

Záhlavie	SID	TREP	xx	yy	Čiastková správa n	CS
4 bajty	255 bajtov					

Záhlavie	SID	TREP	xx	yy+1	CS
4 bajty	4 bajty				

2.2.2 ***Typy správy***

Komunikačný protokol pre dáta sťahované medzi JV a IDE si vyžaduje výmenu ôsmich rôznych typov správ.

V nasledovnej tabuľke sú tieto správy zhrnuté.

Štruktúra správy	Záhlavie maximálne 4 bajty				Dáta maximálne 225 bajtov			1 bajtový kontrolný súčet
IDE → / ← JV	FMT	TGT	SRC	LEN	SID	DS_/TRIP	DATA	CS
Start communication request	81	EE	F0		81			E0
Positive response start communication	80	F0	EE	03	C1		8F,EA	9B
Start diagnostic session request	80	EE	F0	02	10	81		F1
Positive response start diagnostic	80	F0	EE	02	50	81		31
Link control service								
Verify Baud rate (stage 1)								
9 600 Bd	80	EE	F0	04	87		01,01,01	EC
19 200 Bd	80	EE	F0	04	87		01,01,02	ED
38 400 Bd	80	EE	F0	04	87		01,01,03	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
Positive response verify Baud rate	80	F0	EE	02	C7		01	28
Transition baud rate (stage 2)	80	EE	F0	03	87		02,03	ED
Request Upload	80	EE	F0	0A	35		00,00,00, 00,00,FF,FF, FF,FF	99
Positive response request upload	80	F0	EE	03	75		00,FF	D5
Transfer data request								
Overview	80	EE	F0	02	36	01		97
Activities	80	EE	F0	06	36	02	Date	CS
Events and faults	80	EE	F0	02	36	03		99
Detailed speed	80	EE	F0	02	36	04		9A
Technical data	80	EE	F0	02	36	05		9B
Card download	80	EE	F0	02	36	06		9C
Positive response transfer data	80	F0	EE	Len	76	TREP	Data	CS
Request transfer exit	80	EE	F0	01	37			96
Positive response request transfer exit	80	F0	EE	01	77			D6
Stop communication request	80	EE	F0	01	82			E1
Positive response stop communication	80	F0	EE	01	C2			21
Acknowledge sub message	80	EE	F0	Len	83		Data	CS
Negative responses								
General reject	80	F0	EE	03	7F	Sid Req	10	CS
Service not supported	80	F0	EE	03	7F	Sid Req	11	CS
Subfunction not supported	80	F0	EE	03	7F	Sid Req	12	CS
Incorrect message length	80	F0	EE	03	7F	Sid Req	13	CS
Conditions not correct or request sequence error	80	F0	EE	03	7F	Sid Req	22	CS
Request out of range	80	F0	EE	03	7F	Sid Req	31	CS
Upload not accepted	80	F0	EE	03	7F	Sid Req	50	CS
Response pending	80	F0	EE	03	7F	Sid Req	78	CS
Data not available	80	F0	EE	03	7F	Sid Req	FA	CS

Poznámky:
– Sid Req = Sid zodpovedajúcej požiadavky.
– TREP = TRTP zodpovedajúcej požiadavky.
– Tmavé okienka znamenajú, že sa nič neprenáša.

– Výraz „Upload“ (z IDE) sa používa vzhľadom na kompatibilitu s ISO 14229. Znamená, to isté ako „download (z JV).

– Možné 2 bajtové počítadlo čiastkovej správy nie je v tejto tabuľke uvedené.

2.2.2.1 *Start communication request (SID 81)*

DDP_005 Túto správu vydáva IDE za účelom vytvorenia komunikačného spojenia s JV. Počiatočné komunikácie sa vždy vykonávajú prenosovou rýchlosťou 9600 baud (pokým sa prenosová rýchlosť eventuálne nezmení s použitím vhodnej Link control service (riadiacej spojovacej služby).

2.2.2.2 *Positive response start communication (SID C1)*

DDP_006 Túto správu vydáva IDE ako kladnú odpoveď na Start communication request. Obsahuje 2 kľúčové bajty 'EA' '8F' udávajúce, že jednotka podporuje protokol so záhlavím, vrátane cieľových, zdrojových a dĺžkových informácií.

2.2.2.3 *Start diagnostic session request (SID 10)*

DDP_007 Správu Start diagnostic session request vydáva IDE, aby začala nová diagnostická relácia s JV. Subfunkcia 'default session' (81 Hex) udáva, že sa zaviedla štandardná diagnostická relácia.

2.2.2.4 *Positive response start diagnostic (SID 50)*

DDP_008 Správu Positive response start diagnostic posiela JV ako kladnú odpoveď na Diagnostic session request.

2.2.2.5 *Link control service (SID 87)*

DDP_052 Link control service používa IDE na zahájenie zmeny prenosovej rýchlosti. Uskutočňuje sa v dvoch krokoch. V prvom kroku IDE navrhne zmenu prenosovej rýchlosti a uvedie novú rýchlosť. Po prijatí kladnej odpovede z JV, IDE odošle potvrdenie zmeny prenosovej rýchlosti na JV (2. krok). IDE potom zmení prenosovú rýchlosť. Po prijatí potvrdenia JV prejde na novú prenosovú rýchlosť.

2.2.2.6 *Link control positive response (SID C7)*

DDP_053 Správu Link control positive response vydáva JV ako kladnú odpoveď na Link control service request (1. krok). Na potvrdzovaciu správu sa nedáva žiadna odpoveď (2. krok).

2.2.2.7 *Request upload* (SID 35)

DDP_009 Správa Request upload vydáva IDE ako oznámenie pre JV, že sa požaduje download operation. V zhode s normou ISO 14229 obsahuje táto požiadavka vždy údaje o adrese, veľkosti a formáte požadovaných dát. Pretože tieto údaje nie sú pre IDE známe pred sťahovaním, adresa pamäte sa nastaví na 0, formát sa dekóduje a dekomprimuje a veľkosť pamäti sa nastaví na maximum.

2.2.2.8 *Positive response request upload (SID 75)*

DDP_010 Správu Positive response request upload posiela JV aby IDE oznámila, že JV je pripravená na sťahovanie dát. V zhode s normou ISO 14229 obsahuje táto správa aj dáta, pomocou ktorých IDE oznamuje, že ďalšie správy Positive response transfer data budú obsahovať maximálne 00FF hex bytes.

2.2.2.9 *Transfer data request (SID 36)*

DDP_011 Správu Transfer data request posiela IDE, aby pre JV špecifikovalo typ sťahovaných dát. Jeden bajt transfer request parameter (TRTP) udáva typ prenosu.

Existuje šesť typov prenosu dát:

– prehľad (TRTP 01),

– činnosti určitého dňa (TRTP 02),

– udalosti a poruchy (TRTP 03),

– presné údaje o rýchlosti (TRTP 04),

– technické dáta (TRTP 05),

– download karty (TRTP 06).

DDP_054 IDE musí požiadať o prehľad prenosu dát (TRTP 01) počas relácie sťahovania, pretože len to zabezpečí, že osvedčenia JV sa zaznamenajú v rámci sťahovaného súboru (a bude možné overiť digitálny podpis).

V druhom prípade (TRTP 02) správa Transfer data request obsahuje údaje sťahovaného kalendárneho dňa (formát TimeReal).

2.2.2.10 *Positive response transfer data (SID 76)*

DDP_012 Správu Positive response transfer data posiela JV ako odpoveď na transfer data request. Správa obsahuje požadované dáta s transfer response parameter (TREP), ktorý zodpovedá TRTP požiadavke.

DDP_055 V prvom prípade (TREP 01) JV posiela dáta, ktoré pomáhajú operátorovi IDE pri výbere dát, ktoré chce stiahnuť. Informácie obsiahnuté v tejto správe sú tieto:

– bezpečnostné osvedčenia,

– identifikácia vozidla,

– aktuálny dátum a čas JV,

– min. a max. sťahovateľný dátum (dáta JV),

– údaje o prítomnosti kariet v JV,

– predchádzajúci download pre podnik,

– podnikové zablokovanie,

– predchádzajúce kontroly.

2.2.2.11 *Transfer exit request (SID 37)*

DDP_013 Správu Transfer exit request posiela IDE aby bola JV informovaná, že sa skončila relácia download.

2.2.2.12 *Positive response request transfer exit (SID 77)*

DDP_014 Správu Positive response request transfer exit posiela JV ako potvrdenie request transfer exit.

2.2.2.13 *Stop communication request (SID 82)*

DDP_015 Správu Stop communication request posiela IDE aby sa prerušilo komunikačné spojenie s JV.

2.2.2.14 *Positive response stop communication (SID C2)*

DDP_016 Správu Positive response stop communication posiela JV ako potvrdenie Stop communication request.

2.2.2.15 *Acknowledge sub message (SID 83)*

DDP_017 Správu Acknowledge sub message posiela IDE aby sa potvrdilo prijatie jednotlivých častí správy, ktorá sa prenáša v niekoľkých čiastkových správach. Dátové pole obsahuje SID prijaté z JV a 2 bajtový kód takto:

– MsgC + 1 potvrdzuje správne prijatie čiastkovej správy číslo MsgC.

Požiadavku z IDE na JV, aby poslala ďalšiu čiastkovú správu.

– MsgC poukazuje na problém s prijatím čiastkovej správy číslo MsgC.

Požiadavku z IDE na JV, aby poslala znovu čiastkovú správu.

– FFFF žiada ukončenie správy.

Toto môže IDE použiť na skončenie prenosu správy JV z akéhokoľvek dôvodu.

Posledná čiastková správa správy (LEN bajt < 255) sa môže potvrdiť použitím ktoréhokoľvek z týchto kódov, alebo sa nemusí potvrdiť vôbec.

Odpoveď JV pozostávajúca z niekoľkých čiastkových správ:

– positive response transfer Data (SID 76)

2.2.2.16 *Negative response (SID 7F)*

DDP_018 Správu Negative response posiela JV ako odpoveď na vyššie uvedené požiadavky, keď JV nemôže túto požiadavku splniť. Dátové polia správy obsahujú SID odpovedi (7F), SID požiadavky a kód špecifikujúci dôvod zápornej odpovede. K dispozícii sú tieto kódy:

– 10 general reject

Činnosť sa nemôže vykonať, pretože sa neuviedol dôvod, uvedený nižšie.

– 11 service not supported

SID požiadavky nie je zrozumiteľný.

– 12 sub function not supported

DS_ alebo TRTP požiadavky nie sú zrozumiteľné, alebo nie je tu žiadna ďalšia čiastková správa, ktorá by sa mala prenášať.

– 13 incorrect message length

DÍžka prijatej správy nie je správna.

– 22 conditions not correct or request sequence error

Požadovaná služba nie je aktívna alebo nie je správny sled požiadavkových správ.

– 31 request out of range

Záznam o požiadavkovom parametri (dátové pole)nie je platný.

– 50 upload not accepted

Požiadavka sa nemôže splniť (JV v nevhodnom prevádzkovom režime alebo vnútorná porucha JV)

– 78 response pending

Požadovaná činnosť sa nemôže dokončiť načas a JV nie je pripravená na prijatie ďalšej požiadavky.

– FA data not available

Dátový objekt požiadavky na prenos dát nie sú v JV k dispozícii (napr. nie je vložená žiadna karta, ...)

2.2.3 ***Tok správ***

Typický tok správ počas normálneho postupu data download je nasledovný:

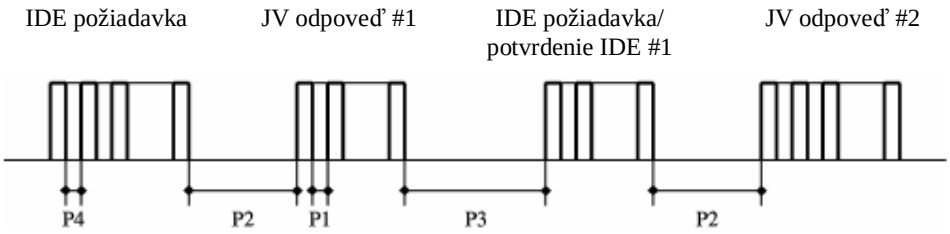
IDE		FE
Start communication request	⇨	
	⇦	Positive response
Start diagnostic service request	⇨	
	⇦	Positive response
Request upload	⇨	
	⇦	Positive response
Transfer data request overview	⇨	
	⇦	Positive response transfer
Data request #2	⇨	
	⇦	Positive response #1
Acknowledge submessage #1	⇨	
	⇦	Positive response #2
Acknowledge submessage #2	⇨	
	⇦	Positive response #m
Acknowledge submessage #m	⇨	
	⇦	Positive response (Data field < 255 Bytes)
Acknowledge submessage (optional)	⇨	
	...	
Transfer data request #n	⇨	
	⇦	Positive response
Request transfer exit	⇨	
	⇦	Positive response
Stop communication request	⇨	
	⇦	Positive response

2.2.4 ***Časovanie***

DDP_019 Počas normálnej prevádzky sú relevantné parametre časovania znázornené na nasledovnom obrázku:

Obrázok 1

Tok správ, časovanie



Kde:

P1 = čas medzi bajtmi pri JV odpovedi.

P2 = čas medzi IDE požiadavkou a začiatkom JV odpovede, alebo medzi IDE potvrdením a začiatkom ďalšej JV odpovede.

P3 = čas medzi koncom JV odpovede a začiatkom IDE požiadavky, alebo medzi koncom JV odpovede a začiatkom IDE potvrdenia, alebo medzi koncom IDE požiadavky a začiatkom novej IDE požiadavky ak JV neodpovedá.

P4 = čas medzi bajtmi pri IDE požiadavke.

P5 = Rozšírená hodnota P3 pre sťahovanie karty.

Povolené hodnoty pre časové parametre sú uvedené v nasledovnej tabuľke (KWP rozšírená sada časových parametrov, použitá v prípade fyzického adresovania pre rýchlejšie komunikácie).

Časové parametre	Hodnota dolného limitu (ms)	Hodnota horného limitu (ms)
P1	0	20
P2	20	1000(*)
P3	10	5000
P4	5	20
P5	10	20 minút

(*) Ak JV reaguje zápornou odpoveďou obsahujúcou kód, ktorý znamená „požiadavka správne prijatá, odpoveď nasleduje“, táto hodnota sa zväčší na rovnaký horný limit ako P3.

2.2.5 **Spracovanie chýb**

Ak počas výmeny správ nastane chyba, tok správy sa modifikuje v závislosti na zariadení, na ktorom sa chyba zistila a na správe, ktorý chybu vyvolala.

Na obrázku 2 a obrázku 3 sú znázornené postupy spracovania chýb pre JV a IDE.

2.2.5.1 *Start communication phase*

DDP_020 Ak IDE zistí chybu počas Start communication phase, buď časovaním alebo prúdom bitov, potom čaká po dobu P3 predtým, než znovu vydá požiadavku.

DDP_021 Ak JV zistí chybu v sekvencii prichádzajúcej z IDE, nepošle žiadnu odpoveď a čaká na ďalšiu správu Start communication request v rámci doby P3 max.

2.2.5.2 *Communication phase*

Môžu byť definované dve rôzne oblasti spracovania chýb:

1. JV zistí prenosovú chybu IDE

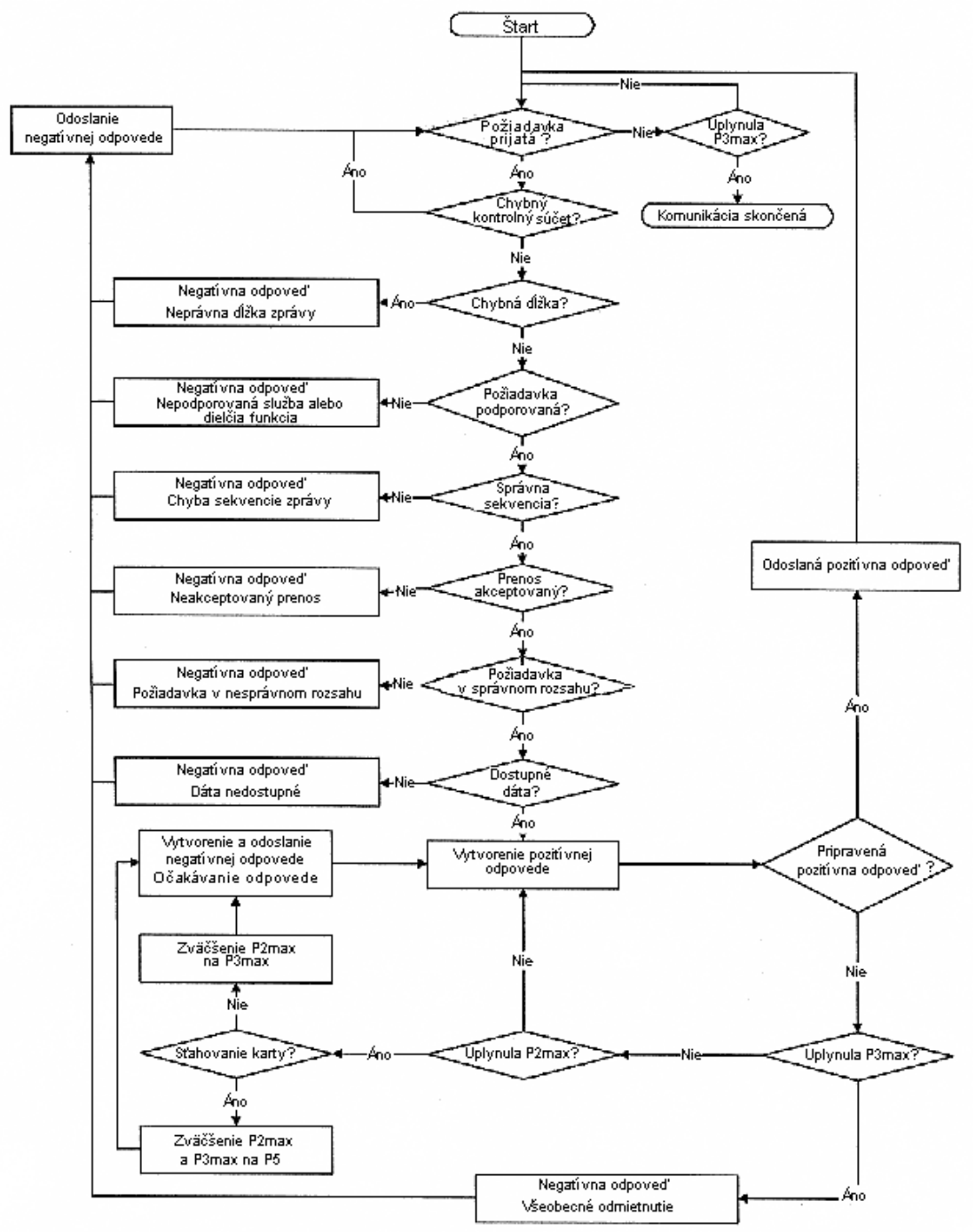
DDP_022 JV zisťuje u každej prijatej správy časové chyby, chyby bajtového formátu (napr. poškodenie start a stop bitu) a chyby dátového paketu (chybné číslo prijatých bajtov, chybný kontrolný súčet).

DDP_023 Ak JV zistí jednu z vyššie uvedených chýb, potom nepošle žiadnu odpoveď a ignoruje prijatú správu.

DDP_024 JV môže zistiť iné chyby vo formáte alebo obsahu prijatej správy (napr. nepodporovaná správa) dokonca aj vtedy, keď správa spĺňa požiadavky na dĺžku a kontrolný súčet; v takom prípade JV odpovedá IDE správou Negative Response, špecifikujúc druh chyby.

Obrázok 2

Spracovanie chyby cez JV



2. IDE zistí prenosovú chybu JV

DDP_025 IDE zisťuje u každej prijatej správy časové chyby, chyby bajtového formátu (napr. poškodenie start a stop bitu) a chyby dátového paketu (chybné číslo prijatých bajtov, chybný kontrolný súčet).

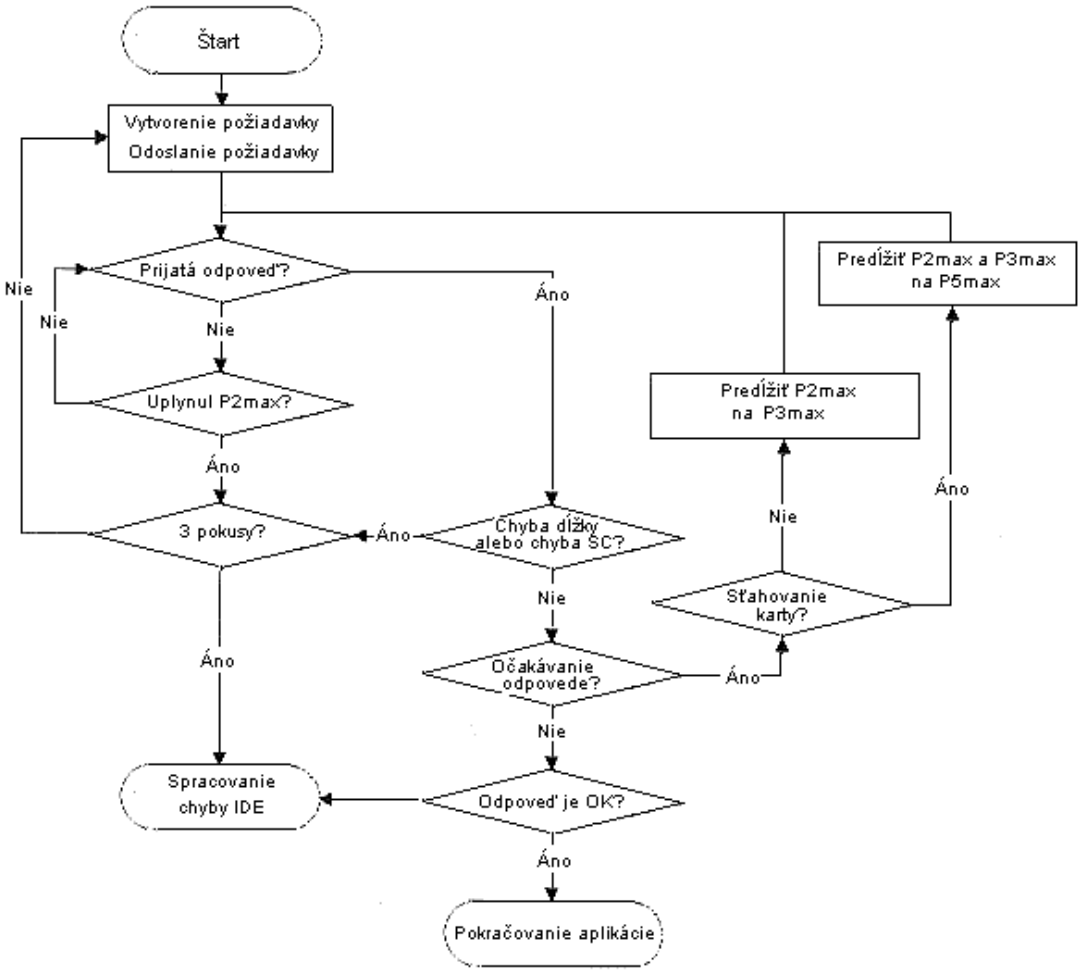
DDP_026 IDE zisťuje sekvenčné chyby, napr. nesprávne zvýšenie počítadla dielčej správy v postupne prijímaných správach.

DDP_027 Ak IDE zistí chybu alebo ak nie je žiadna odpoveď z JV v rámci doby P2max, požiadavková správa sa pošle znovu pre celkovo maximálne tri prenosy. Na účely tohto zisťovania chyby sa potvrdenie dielčej správy bude považovať za požiadavku na JV.

DDP_028 IDE čaká minimálne po dobu P3min pred začiatkom každého prenosu, čas čakania sa meria od posledného vypočítaného výskytu stop bitu po zistenej chybe.

Obrázok 2

Spracovanie chyby cez IDE



2.2.6 ***Obsah odpovedacej správy***

Tento odsek špecifikuje obsah dátových polí rôznych kladných odpovedacích správ.

Dátové prvky sú definované v doplnku 1, dátový slovník.

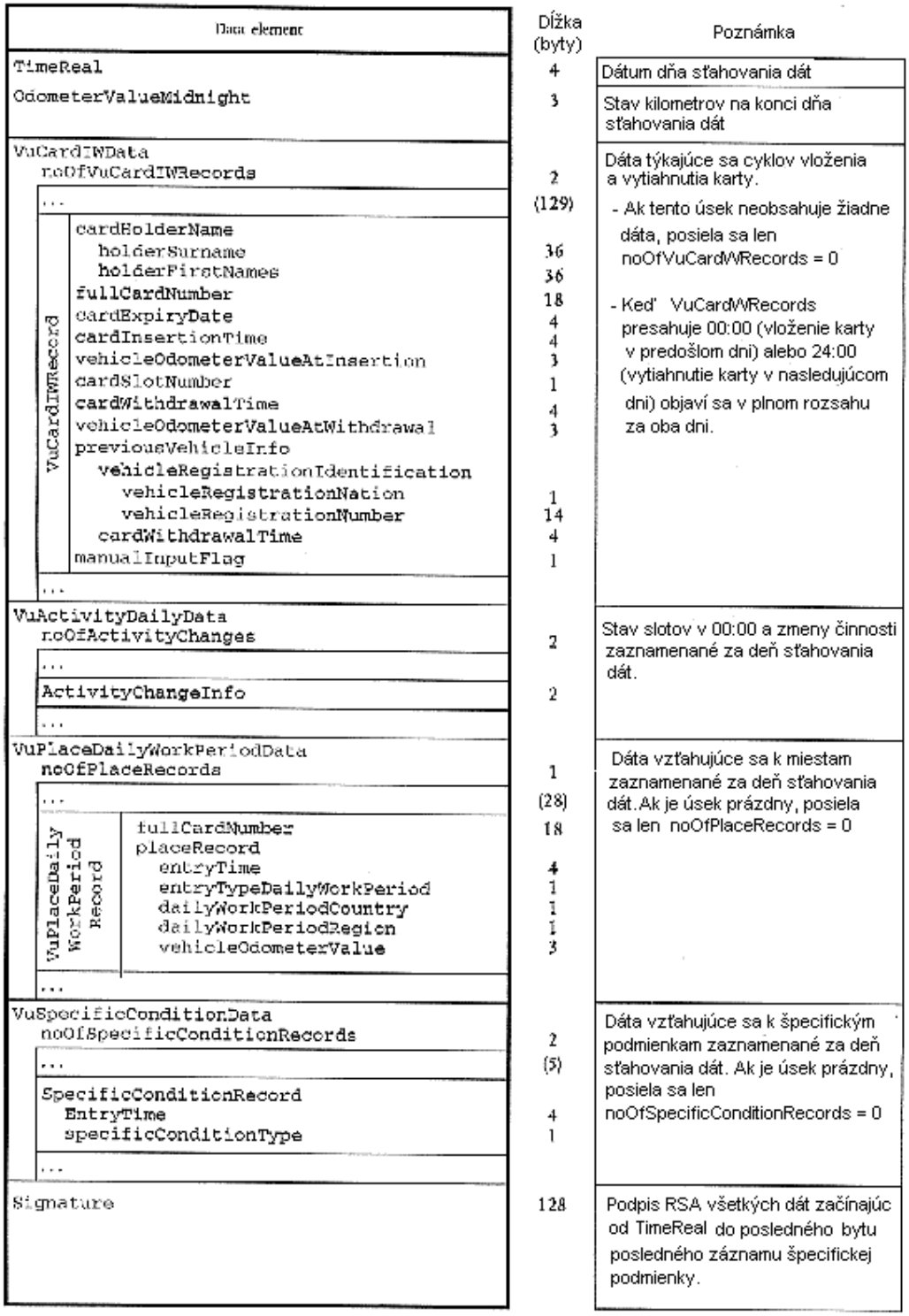
2.2.6.1 *Positive response transfer data overview*

DDP_029 Dátové pole správy „positive response transfer data overview“ poskytuje nasledovné dáta v tomto poradí podľa SID 76 Hex, TREP 01 Hex a primerané rozdelenie a sčítanie dielčích správ:

Data element		Dĺžka (byty)	Poznámka
MemberStateCertificate		194	Bezpečnostné osvedčenie JV
VUCertificate		194	
VehicleIdentificationNumber		17	Identifikátor vozidla
VehicleRegistrationIdentification			
vehicleRegistrationNation		1	
vehicleRegistrationNumber		14	
CurrentDateTime		4	Aktuálny dátum a čas JV
VuDownloadablePeriod			Čas sťahovania
minDownloadableTime		4	
maxDownloadableTime		4	
CardSlotsStatus		1	Typ karty vloženej do JV
VuDownloadActivityData			Predchádzajúce sťahovanie JV
downloadingTime		4	
fullCardNumber		18	
companyOrWorkshopName		36	
VuCompanyLocksData			Všetky uložené podnikové blokovania. Ak je úsek prázdny, len noOfLocks=0 je poslané.
noOfLocks		1	
...		(98)	
VuCompanyLocksRecord	lockInTime	4	
	lockOutTime	4	
	companyName	36	
	companyAddress	36	
	companyCardNumber	18	
...			
VuControlActivityData			Všetky uložené kontrolné záznamy v JV. Ak je úsek prázdny, len noOfControls=0 je poslané.
noOfControls		1	
...		(31)	
VuControlActivityRecord	controlType	1	
	controlTime	4	
	controlCardNumber	18	
	downloadPeriodBeginTime	4	
	downloadPeriodEndTime	4	
...			
Signature		128	RSA-podpis všetkých dát (okrem osvedčení), začínajúc od VehicleIdentificationNumber po posledný byte posledného VuControlActivitzRecord.

2.2.6.2 *Positive response transfer data activities*

DDP_030 Dátové pole správy „positive response transfer data activities“ poskytuje nasledovné dáta v tomto poradí podľa SID 76 Hex, TREP 02 Hex a primerané rozdelenie a sčítanie dielčich správ:



Data element	Dĺžka (byty)	Poznámka
TimeReal	4	Dátum dňa sťahovania dát
OdometerValueMidnight	3	Stav kilometrov na konci dňa sťahovania dát
VuCardIWData		Dáta týkajúce sa cyklov vloženia a vytiahnutia karty. - Ak tento úsek neobsahuje žiadne dáta, posiela sa len noOfVuCardIWRecords = 0 - Keď VuCardIWRecords presahuje 00:00 (vloženie karty v predošlom dni) alebo 24:00 (vytiahnutie karty v nasledujúcom dni) objaví sa v plnom rozsahu za oba dni.
noOfVuCardIWRecords	2	
...	(129)	
VuCardIWRecord: cardHolderName		
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 slotov v 00:00 a zmeny činnosti zaznamenané za deň sťahovania dát.
noOfActivityChanges	2	
...		
ActivityChangeInfo	2	
...		
VuPlaceDailyWorkPeriodData		Dáta vzťahujúce sa k miestam zaznamenané za deň sťahovania dát. Ak je úsek prázdny, posiela sa len noOfPlaceRecords = 0
noOfPlaceRecords	1	
...	(28)	
VuPlaceDailyWorkPeriodRecord: fullCardNumber	18	
placeRecord		
entryTime	4	
entryTypeDailyWorkPeriod	1	
dailyWorkPeriodCountry	1	
dailyWorkPeriodRegion	1	
vehicleOdometerValue	3	
...		
VuSpecificConditionData		Dáta vzťahujúce sa k špecifickým podmienkam zaznamenané za deň sťahovania dát. Ak je úsek prázdny, posiela sa len noOfSpecificConditionRecords = 0
noOfSpecificConditionRecords	2	
...	(5)	
SpecificConditionRecord		
EntryTime	4	
specificConditionType	1	
...		
Signature	128	Podpis RSA všetkých dát začínajúc od TimeReal do posledného bytu posledného záznamu špecifickej podmienky.

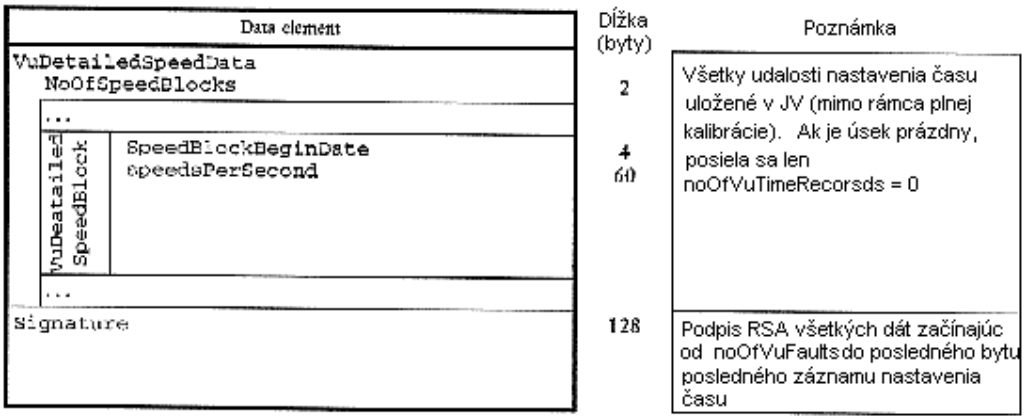
2.2.6.3 *Positive response transfer data events and faults*

DDP_031 Dátové pole správy „positive response transfer data events and faults“ poskytuje nasledovné dáta v tomto poradí podľa SID 76 Hex, TREP 03 Hex a primerané rozdelenie a sčítanie dielčich správ:

Data element	Dĺžka (byty)	Poznámka
VuFaultData		
NoOfVuFaults	1	Všetky poruchy uložené alebo prebiehajúce v JV. Ak je úsek prázdny, posiela sa len noOfVuFaults = 0
...	(82)	
VuFaultRecord: FaultType	1	
FaultRecordPurpose	1	
FaultBeginTime	4	
FaultEndTime	4	
CardNumberDriverSlotBegin	18	
cardNumberCodriverSlotBegin	18	
CardNumberDriverSlotEnd	18	
CardNumberCodriverSlotEnd	18	
...		
VuEventData		
NoOfVuEvents	1	Všetky udalosti (okrem prekročenia rýchlosti) uložené alebo prebiehajúce v JV. Ak je úsek prázdny, posiela sa len noOfVuEvents = 0
...	(83)	
VuEventRecord: EventType	1	
EventRecordPurpose	1	
EventBeginTime	4	
EventEndTime	4	
CardNumberDriverSlotBegin	18	
CardNumberCodriverSlotBegin	18	
CardNumberDriverSlotEnd	18	
CardNumberCodriverSlotEnd	18	
SimilarEventsNumber	1	
...		
VuOverSpeedingControlData		Dáta vzťahujúce sa k poslednému prekročeniu rýchlosti (štandardná hodnota ak nie sú žiadne dáta)
LastOverspeedControlTime	4	
FirstOverspeedSince	4	
NumberOfOverspeedSince	1	
VuOverSpeedingEventData		Všetky udalosti prekročenia rýchlosti uložené v JV. Ak je úsek prázdny, posiela sa len noOfVuOverSpeedingEvents = 0
NoOfVuOverSpeedingEvents	1	
...	(31)	
VuOverSpeedingEventRecord: EventType	1	
EventRecordPurpose	1	
EventBeginTime	4	
EventEndTime	4	
MaxSpeedValue	1	
AverageSpeedValue	1	
CardNumberDriverSlotBegin	18	
SimilarEventsNumber	1	
...		
VuTimeAdjustmentData		Všetky udalosti nastavenia času uložené v JV (mimo rámca úplnej kalibrácie). Ak je úsek prázdny, posiela sa len noOfVuTimeAdjRecords = 0
NoOfVuTimeAdjRecords	1	
...	(93)	
VuTimeAdjustmentRecord: OldTimeValue	4	
NewTimeValue	4	
WorkshopName	36	
WorkshopAddress	36	
WorkshopCardNumber	18	
...		
Signature	128	Podpis RSA všetkých dát začínajúc od noOfVuFaults do posledného bytu posledného záznamu nastavenia.času

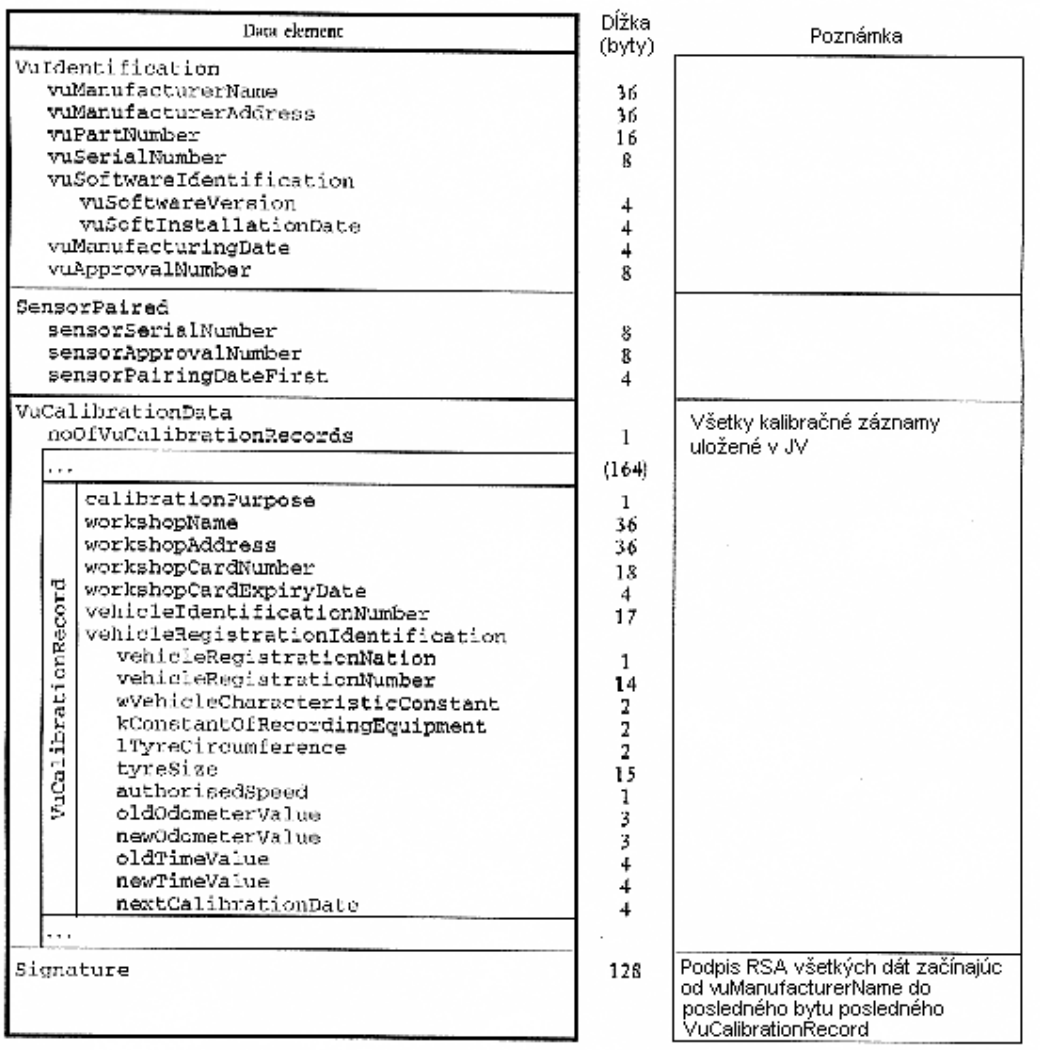
2.2.6.4 *Positive response transfer data detailed speed*

DDP_032 Dátové pole správy „positive response transfer data detailed speed“ poskytuje nasledovné dáta v tomto poradí podľa SID 76 Hex, TREP 04 Hex a primerané rozdelenie a sčítanie dielčich správ:



2.2.6.5 *Positive response transfer data technical data*

DDP_033 Dátové pole správy „positive response transfer data technical data“ poskytuje nasledovné dáta v tomto poradí podľa SID 76 Hex, TREP 05 Hex a primerané rozdelenie a sčítanie dielčich správ:



Data element	Dĺžka (byty)	Poznámka
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		
noOfVuCalibrationRecords	1	Všetky kalibračné záznamy uložené v JV
...	(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	Podpis RSA všetkých dát začínajúc od vuManufacturerName do posledného bytu posledného VuCalibrationRecord

2.3 **ESM pamäť**

DDP_034 Ak relácia download zahŕňa prenos dát JV, IDE uloží v rámci jedného fyzického súboru všetky dáta prijaté z JV počas relácie download v správach positive response transfer data. Pritom sa neukladajú záhlavia správ, počítadlá dielčich správ, prázdne dielčie správy a kontrolné súčty, no ukladá sa SID a TREP (prvej dielčej správy v prípade niekoľkých dielčich správ)

3. PROTOKOLY PRE SŤAHOVANIE DÁT Z TACHOGRAFOVÝCH KARIET

3.1 **Rozsah pôsobnosti**

Tento odsek popisuje priame sťahovanie kartových dát z tachografovej karty na IDE. IDE nie je časťou bezpečnostného prostredia, preto sa nevykonáva žiadna autentifikácia medzi kartou a IDE.

3.2 **Definície**

Download relácia: vykonanie každého download dát ICC. Relácia obsahuje úplný postup od resetovania ICC prostredníctvom IFD, až do deaktivovania ICC (vytiahnutie karty alebo ďalšie resetovanie).

Súbor s podpísanými dátami: súbor z ICC. Súbor sa prenáša na IFD v zrozumiteľnom texte. Na ICC sa súbor označí hash kódom, podpíše a podpis sa prenáša na IFD.

3.3 **Sťahovanie dát z karty**

DDP_035 Download tachografovej karty zahŕňa tieto kroky:

–download spoločných informácií karty v EFs ICC a IC. Tieto informácie nie sú povinné a nie sú zabezpečené digitálnym podpisom,

–download EFs Card_Certificate a CA_Certificate. Tieto informácie nie sú zabezpečené digitálnym podpisom.

Download týchto súborov je povinné pre každú download reláciu.

–download iných aplikačných dát EFs (v rámci Tachograph DF) okrem EF Card_Download. Tieto informácie sú zabezpečené digitálnym podpisom,

- je povinný download aspoň EFs Application_Identification a ID pre každú download reláciu,
- pri sťahovaní dát z karty vodiča je tiež povinný download týchto EFs:
  - Events_Data,
  - Faults_Data,
  - Driver_Activity_Data,
  - Vehicles_Used,
  - Places,
  - Control_Activity_Data,
  - Specific_Conditions.

– Pri sťahovaní dát z karty vodiča sa aktualizuje dátum LastCardDownload v EF Card_Download,

– Pri sťahovaní dát z dielenskej karty sa resetuje kalibračné počítadlo v EF Card_Download.

3.3.1 ***Inicializácia sekvencie***

DDP_036 IDE iniciuje túto sekvenciu:

Karta	Smer	IDE/IFD	Význam/Poznámky
	⇦	Reset hardwaru	
ATR	⇨		

S PPS sa môže zvoliť vyššia prenosová rýchlosť, pokiaľ to ICC podporuje.

3.3.2 ***Sekvencia pre nepodpísané dátové súbory***

DDP_037 Sekvencia pre sťahovanie ICC, IC, Card_Certificate a CA_ Certificate je nasledovná:

Karta	Smer	IDE/IFD	Význam/Poznámky
	⇦	Select file	Voľba podľa identifikátorov súboru
OK	⇨		
	⇦	Read Binary	Ak súbor obsahuje viac dát než je kapacita vyrovnávacej pamäti čítacieho zariadenia alebo karty, príkaz sa musí zopakovať až kým nie je načítaný celý súbor.
File data OK	⇨	Uloženie dát na ESM	Podľa 3.4, (formát dátovej pamäti)

Poznámka: Pred voľbou EF Card_Certificate, musí sa zvoliť tachografová aplikácia (výber prostredníctvom AID).

3.3.3 ***Sekvencia pre podpísané dátové súbory***

DDP_038 Nasledovná sekvencia sa používa pre každý z nasledovných súborov, ktoré sa musia sťahovať s ich podpisom:

Karta	Smer	IDE/IFD	Význam/Poznámky
	⇦	Select file	
OK	⇨		
	⇦	Perform hash of File	Vypočíta sa hodnota hash celého dátového obsahu zvoleného súboru s použitím predpísaného algoritmu hash v súlade s doplnkom 11. Tento príkaz nie je príkazom ISO.
Vypočíta sa hash of file a dočasne sa uloží hash hodnota			
OK	⇨		
	⇦	Real Binary	Ak súbor obsahuje viac dát než je kapacita vyrovnávacej pamäti čítacieho zariadenia alebo karty, príkaz sa musí zopakovať až kým nie je načítaný celý súbor.
File Data OK	⇨	Prijaté dáta uložené na ESM	Podľa 3.4, (formát dátovej pamäti)
	⇦	PSO: Compute Digital Signature	
Perform Security Operation „Compute Digital Signature“ s pomocou dočasne uloženej hash hodnoty			
Podpis OK	⇨	Pripojiť dáta k predchádzajúcim súborom	Podľa 3.4, (formát dátovej pamäti)

		uloženým na ESM	

3.3.4 ***Sekvencia pre resetovanie kalibračného počítadla***

DDP_039 Sekvencia pre resetovanie počítadla NoOfCalibrationsSinceDownload v EF Card_Download na dielenskej karte je nasledovná:

Karta	Smer	IDE/IFD	Význam/Poznámky
OK	⇦ ⇨	Select file EF Card_Download	Voľba podľa identifikátorov súboru
	⇦	Update Binary NoOfCalibrations–SinceDownload = ’00 00’	
Resetovanie počtu sťahovaní z karty			
OK	⇨		

3.4 **Formát dátovej pamäte**

3.4.1 ***Úvod***

DDP_040 Sťahované dáta sa musia uložiť podľa nasledovných podmienok:

– dáta sa musia ukladať transparentne. To znamená, že počas uloženia musí byť zachované poradie bajtov ako aj poradie bitov v rámci bajtu, ktoré sa prenášajú z karty,

– všetky súbory sťahované z karty počas download relácie, sú uložené v jednom súbore na ESM.

3.4.2 ***Formát súboru***

DDP_041 Formát súboru je zreťazením niekoľkých TLV objektov.

DDP_042 Tag pre EF je FID spolu s doplnkom „00“.

DDP_043 Tag podpisu EF je FID spolu s doplnkom „01“.

DDP_044 Dĺžka je dvojbajtová hodnota. Hodnota stanovuje počet bajtov v hodnotovom poli. Hodnota „FF FF“ v dĺžkovom poli je vyhradená pre budúce použitie.

DDP_045 Keď súbor nie je sťahovaný, nič z toho čo s vzťahuje k súboru sa nemusí ukladať (žiadny tag, žiadna nulová dĺžka).

DDP_046 Podpis sa ukladá ako ďalší TLV objekt bezprostredne za objektom, ktorý obsahuje dáta súboru.

Definícia	Význam	Dĺžka
FID (2 Bytes) || „00“	Tag pre EF (FID)	3 bajty
FID (2 Bytes) || „01“	Tag pre Signature EF(FID)	3 bajty
xx xx	Dĺžka hodnotového poľa	2 bajty

Príklad dát v sťahovanom súbore na ESM:

Definícia	Význam	Dĺžka
00 02 00	00 11	Dáta EF ICC
C1 00 00	00 C2	Dáta EF Card_Cerificate
		…
05 05 00	0A 2E	Dáta EF Vehicles_Used
05 05 01	00 80	Podpis EF Vehicles_Used

4. SŤAHOVANIE DÁT Z TACHOGRAFOVEJ KARTY CEZ JEDNOTKU VOZIDLA

DDP_047 JV musí umožniť stiahnutie obsahu karty vodiča vloženej do pripojeného IDE.

DDP_048 IDE pošle správu „transfer data request card download“ na JV, aby sa zahájil tento režim (pozri 2.2.2.9).

DDP_049 JV potom stiahne celú kartu súbor po súbore, v súlade s protokolom sťahovania karty definovaným v odseku 3, a odošle všetky dáta prijaté z karty na IDE v rámci vhodného TLV formátu súboru (pozri 3.4.2) a uzavrie ich v správe „positive response transfer data“.

DDP_050 IDE vyvolá dáta karty zo správy „positive response transfer data“ (s vynechaním všetkých záhlaví, SID, TREP, počítadiel dielčich správ a kontrolných súčtov) a uloží ich v jednom fyzickom súbore popísanom v odseku 2.3.

DDP_051 JV potom prípadne aktualizuje súbor Control_Activity_Data alebo Card_Download karty vodiča.

Doplnok 8

KALIBRAČNÝ PROTOKOL

OBSAH

1. ÚVOD

Tento doplnok popisuje výmenu dát medzi jednotkou vozidla a skúšobným zariadením cez K–vedenie, ktoré tvorí časť kalibračného rozhrania popísaného v doplnku 6. Popisuje aj riadenie vstupného/výstupného signalizačného vedenia na kalibračnom konektore.

Vytvorenie komunikácie na K–vedení je popísané v odseku 4 „Komunikačné služby“

Tento doplnok používa koncepciu diagnostických „relácií“ na stanovenie rozsahu riadenia K–vedenia v rôznych podmienkach. Štandardná relácia je „StandardDiagnosticSession“, keď môžu byť všetky dáta prečítané z jednotky vozidla, no žiadne dáta sa nemôžu v jednotke vozidla napísať.

Voľba diagnostickej relácie je popísané v odseku 5 „Riadiace služby“.

CPR_001 „ECUProgrammingSession“ umožňuje zápis dát do jednotky vozidla. V prípade zápisu kalibračných dát (požiadavky 097 a 098), jednotka vozidla musí byť navyše v režime prevádzky KALIBRÁCIA.

Prenos dát cez K–vedenie je popísaný v odseku 6 „Služby prenosu dát“. Formáty prenášaných dát sú podrobne popísané v odseku 8 „Formáty dataRecords“.

CPR_002 „ECUAdjustmentSession“ umožňuje voľbu vstupného/výstupného režimu kalibrácie vstupného/výstupného signalizačného vedenia cez rozhranie K–vedenia. Riadenie kalibrácie vstupného/výstupného signalizačného vedenia je popísané v odseku 7 „Riadenie skúšobných impulzov – Riadenie vstupu/výstupu funkčnej jednotky“.

CPR_003 V predloženom dokumente sa ako adresa skúšobného zariadenia používa ‘tt’. Bez ohľadu na to, že sa môžu používať prioritné adresy pre skúšobné zariadenia, JV správne odpovedá na každú adresu skúšobného zariadenia. Fyzická adresa JV je 0xEE.

2. POJMY, DEFINÍCIE A REFERENČNÉ DOKUMENTY

Protokoly, správy a chybové kódy sú v zásade založené na súčasnom návrhu normy ISO 14229–1 (Cestné vozidlá – Diagnostické systémy – Časť 1: Diagnostické služby, verzia 6 z 22. februára 2001).

Kódovanie bajtov a hexadecimálne hodnoty sa používajú pre identifikátory služby, požiadavky a odpovede vzťahujúce sa k službe a pre štandardné parametre.

Pojem „skúšobné zariadenie“ sa vzťahuje na zariadenie používané na zápis programovacích/kalibračných dát do JV.

Pojem „klient“ a „server“ sa vzťahuje na skúšobné zariadenie a JV.

Pojem ECU znamená „Elektronická riadiaca jednotka“ a vzťahuje sa na JV.

Referenčné dokumenty:

ISO 14230–2: Road Vehicles Diagnostics Systems Keyword Protocol 2000 - Part 2: Data Link Layer. First edition: 1999. Vehicles Diagnostic Systems (Cestné vozidlá – Diagnostické systémy – Kľúčový protokol 2000 – Časť 2: Vrstva riadenia dátových spojov. Prvé vydanie: 1999. Vozidlá – Diagnostické systémy.)

3. PREHĽAD SLUŽIEB

3.1 **Dostupné služby**

Nasledovná tabuľka poskytuje prehľad o službách, ktoré sú k dispozícii v záznamovom zariadení a sú definované v tomto dokumente.

CPR_004 V tabuľke sú uvedené služby, ktoré sú k dispozícii pri aktivovanej diagnostickej relácii.

– Prvý stĺpec obsahuje služby, ktoré sú k dispozícii,

– druhý stĺpec obsahuje číslo odseku v tomto doplnku, v ktorom sú služby popísané podrobnejšie,

– tretí stĺpec priraďuje hodnoty identifikátora služby požiadavkovým správam,

– štvrtý stĺpec špecifikuje služby „StandardDiagnosticSession“ (SD), ktoré sa musia zaviesť v každej JV,

– piaty stĺpec špecifikuje služby „ECUAdjustmentSession“ (ECUAS), ktoré sa musia zaviesť, aby bola možná kontrola vstupného/výstupného signalizačného vedenia v každej JV,

– šiesty stĺpec špecifikuje služby „ECUProgrammingSession“ (ECUPS), ktoré sa musia zaviesť, aby bolo možné programovanie parametrov v JV.

Tabuľka 1

Prehľad o hodnotách identifikátora služby

			Diagnostické relácie		
Názov diagnostickej služby	Odsek č.	Hodnota SID pož.	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 udáva, že v tejto diagnostickej relácii je služba povinná.
Žiadny symbol znamená, že v tejto diagnostickej relácii nie je služba povolená.

3.2 **Odpovedacie kódy**

Odpovedacie kódy sú definované pre každú službu.

4. KOMUNIKAČNÉ SLUŽBY

Niektoré služby, ktoré neležia na aplikačnej vrstve, sú nevyhnutné pre vytvorenie a udržanie komunikácie. Disponibilné služby sú uvedené v nasledovnej tabuľke:

Tabuľka 2

Komunikačné služby

Názov služby	Popis
StartCommunication	Klient žiada zahájenie komunikačnej relácie so serverom(mi).
StopCommunication	Klient žiada skončenie prebiehajúcej komunikačnej relácie.
TesterPresent	Klient oznamuje serveru, že spojenie je ešte stále aktívne.

CPR_005 Služba StartCommunication sa používa na zahájenie komunikácie. Na vykonanie služby sa musí zahájiť komunikácia a komunikačné parametre musia zodpovedať požadovanému režimu.

4.1 **Služba StartCommunication**

CPR_006 Po prijatí indikačného prvku StartCommunication JV skontroluje, či môže byť inicializované požadované komunikačné spojenie v súčasných podmienkach. Platné podmienky pre zahájenie komunikačného spojenia sú popísané v dokumente ISO 14230–2.

CPR_007 Potom JV vykoná všetky činnosti potrebné na inicializovanie komunikačného spojenia a pošle StartCommunication odpovedací prvok so zvolenými parametrami kladnej odpovede.

CPR_008 Ak JV, ktorá je už inicializovaná (a vstúpila do diagnostickej relácie) prijme novú požiadavku StartCommunication (napr. na základe opravy chyby v skúšobnom zariadení), požiadavka sa zaznamená a JV sa znovu inicializuje.

CPR_009 Ak komunikačné spojenie nemôže byť inicializované z akýchkoľvek dôvodov, JV pokračuje v činnosti, ktorá bezprostredne predchádzala pokusu o zahájenie komunikačného spojenia.

CPR_010 Požiadavková správa StartCommunication sa musí adresovať na fyzickú adresu.

CPR_011 Inicializácia JV pre služby sa vykoná pomocou metódy „rýchla inicializácia“:

– každej aktivite predchádza kľudový stav zbernice,

– skúšobné zariadenie potom odošle inicializačnú sekvenciu,

– všetky informácie, ktoré sú potrebné na vytvorenie komunikácie sú obsiahnuté v odpovedi JV.

CPR_012 Po dokončení inicializácie,

– všetky komunikačné parametre sa nastavia na hodnoty definované v tabuľke 4 podľa kľúčových bajtov,

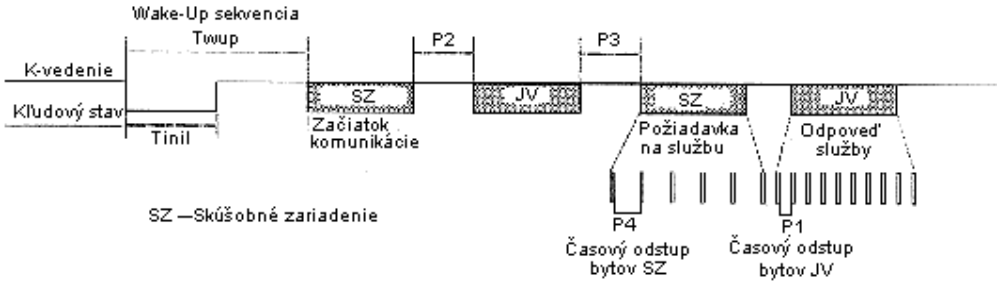
– JV čaká na prvú požiadavku skúšobného zariadenia,

– JV je v štandardnom diagnostickom režime, t. j. StandardDiagnosticSession,

– kalibračné vstupné/výstupné signalizačné vedenie je v štandardnom stave, t. j. v deaktivovanom stave.

CPR_014 Rýchlosť prenosu dát na K–vedení je 10 400 Baud.

CPR_016 Rýchlu inicializáciu zahájí skúšobné zariadenie prenášajúce Wake–Up–Sequence na K–vedení. Táto začína po kľudovom stave K–vedenia s krátkym časom Tinil. Skúšobné zariadenie prenáša prvý bit StartCommunicationService po čase Twup, ktorý začína po prvej klesajúcej hrane.



CPR_017 Časové hodnoty pre rýchlu inicializáciu a komunikácie sú všeobecne uvedené v tabuľke nižšie. Pre kľudový stav existujú rôzne možnosti:

– prvý prenos po zapnutí , $T_{kľud}$ = 300 ms,

– po dokončení služby StupCommunication, $T_{kľud}$ = P3 min.,

– po skončení komunikácie prekročením času P3 max, $T_{kľud}$ = 0.

Tabuľka 3

Časové hodnoty pre rýchlu inicializáciu

Parameter	minimálna hodnota	maximálna hodnota

Tinil	25 ± 1 ms	24 ms	26 ms
Twup	50 ± 1 ms	49 ms	51 ms

Tabuľka 4

Časové hodnoty pre komunikáciu

Časový parameter	Popis parametra	Dolné limitné hodnoty (ms)	Horné limitné hodnoty (ms)
		minimum	maximum
P1	Časový rozostup medzi bajtmi pre odpoveď JV	0	20
P2	Čas medzi požiadavkou skúšobného zariadenia a odpoveďou JV alebo dvoch odpovedí JV	25	250
P3	Čas medzi odpoveďami JV a začiatkom novej požiadavky skúšobného zariadenia	55	5 000
P4	Časový rozostup medzi bajtmi pre požiadavku skúšobného zariadenia	5	20

Tabuľka 5

Požiadavková správa StartCommunication

Bajt #	Názov parametra	Hex hodnota	Mnemotechnická skratka
# 1	Formátový bajt – fyzické adresovanie	81	FMT
# 2	Bajt cieľovej adresy	EE	TGT
# 3	Bajt zdrojovej adresy	tt	SRC
# 4	Identifikátor služby pre požiadavku StartCommunication	81	SCR
# 5	Kontrolný súčet	00–FF	CS

Tabuľka 6

Správa Positive Response na StartCommunication

Bajt #	Názov parametra	Hex hodnota	Mnemotechnická skratka
# 1	Formátový bajt – fyzické adresovanie	80	FMT
# 2	Bajt cieľovej adresy	tt	TGT
# 3	Bajt zdrojovej adresy	EE	SRC
# 4	Doplnkový dĺžkový bajt	03	LEN
# 5	Identifikátor služby pre Positive Response na StartCommunication	C1	SCRPR
# 6	Kľúčový bajt 1	EA	KB1
# 7	Kľúčový bajt 2	8F	KB2
# 8	Kontrolný súčet	00–FF	CS

CPR_019 Nie je žiadna záporná odpoveď na požiadavkovú správu StartCommunication; ak nie je žiadna správa s kladnou odpoveďou, ktorá sa má prenášať, potom JV nie je inicializovaná, nič sa neprenáša a JV zostáva vo svojom normálnom prevádzkovom režime.

4.2 **Služba StopCommunication**

4.2.1 ***Popis správy***

Účelom tejto služby komunikačnej vrstvy je ukončiť komunikačnú reláciu.

CPR_020 Po prijatí indikačného prvku StopCommunication JV skontroluje, či súčasné podmienky dovoľujú ukončiť komunikáciu. Ak tomu tak je, JV vykoná všetky činnosti potrebné na ukončenie komunikácie.

CPR_021 Ak je možné ukončiť komunikáciu, JV pre ukončením komunikácie vydá odpovedací prvok StopCommunication so zvolenými parametrami Positive Response.

CPR_022 Ak komunikácia nemôže byť ukončená z akéhokoľvek dôvodu, JV vydá odpovedací prvok StopCommunication so zvolenými parametrami Negative Response.

CPR_023 Ak JV zistí prekročenie času P3 max, komunikácia sa ukončí bez toho, aby bol vydaný akýkoľvek odpovedací prvok.

4.2.2 ***Formát správy***

CPR_024 Formáty správ pre prvky StopCommunication sú uvedené v nasledovných tabuľkách:

Tabuľka 7

Požiadavková správa pre StopCommunication

Bajt #	Názov parametra	Hex hodnota	Mnemotechnická skratka
# 1	Formátový bajt – fyzické adresovanie	80	FMT
# 2	Bajt cieľovej adresy	EE	TGT
# 3	Bajt zdrojovej adresy	tt	SRC
# 4	Doplnkový dĺžkový bajt	01	LEN
# 5	Identifikátor služby pre požiadavku StopCommunication	82	SPR
# 6	Kontrolný súčet	00–FF	CS

Tabuľka 8

Správa Positive Response na StopCommunication

Bajt #	Názov parametra	Hex hodnota	Mnemotechnická skratka
# 1	Formátový bajt – fyzické adresovanie	80	FMT
# 2	Bajt cieľovej adresy	tt	TGT
# 3	Bajt zdrojovej adresy	EE	SRC
# 4	Doplnkový dĺžkový bajt	01	LEN
# 5	Identifikátor služby pre Positive Response na StopCommunication	C2	SPRPR
# 6	Kontrolný súčet	00–FF	CS

Tabuľka 9

Správa Negative Response na StopCommunication

Bajt #	Názov parametra	Hex hodnota	Mnemotechnická skratka
# 1	Formátový bajt – fyzické adresovanie	80	FMT
# 2	Bajt cieľovej adresy	tt	TGT
# 3	Bajt zdrojovej adresy	EE	SRC
# 4	Doplnkový dĺžkový bajt	03	LEN
# 5	Identifikátor služby pre Negative Response	7F	NR
# 6	Identifikátor služby pre požiadavku StopCommunication	82	SPR

# 7	responseCode = generalReject	10	RC_GR
# 8	Kontrolný súčet	00–FF	CS

4.2.3 ***Definícia parametra***

Táto služba si nevyžaduje žiadnu definíciu parametra.

4.3 **Služba TesterPresent**

4.3.1 ***Popis správy***

Službu TesterPresent používa skúšobné zariadenie na oznámenie svojej prítomnosti serveru, aby zabránil serveru v automatickom návrate na normálny prevádzkový režim a prípadne aby zastavil komunikáciu. Táto služba, pravidelne posiela požiadavku, aby sa zostala aktívna diagnostická relácia alebo komunikácia tým, že resetuje časovač P3 vždy, keď sa prijme požiadavka na túto službu.

4.3.2 ***Formát správy***

CPR_079 Formáty správ pre prvky TesterPresent sú uvedené v nasledovných tabuľkách:

Tabuľka 10

Požiadavková správa TesterPresent

Bajt #	Názov parametra	Hex hodnota	Mnemotechnická skratka
# 1	Formátový bajt – fyzické adresovanie	80	FMT
# 2	Bajt cieľovej adresy	EE	TGT
# 3	Bajt zdrojovej adresy	tt	SRC
# 4	Doplnkový dĺžkový bajt	02	LEN
# 5	Identifikátor služby pre TesterPresent	3E	TP
# 6	Sub Function = responseRequired = [yes	01	RESPREQ_Y
	no]	02	RESPREQ_NO
# 7	Kontrolný súčet	00–FF	CS

CPR_080 Ak je parameter responseRequired nastavený na „yes“, potom server odpovedá nasledovnou správou s kladnou odpoveďou. Ak je nastavený na „no“, server neposiela žiadnu odpoveď.

Tabuľka 11

Správa TesterPresent Positive Response

Bajt #	Názov parametra	Hex hodnota	Mnemotechnická skratka
# 1	Formátový bajt – fyzické adresovanie	80	FMT
# 2	Bajt cieľovej adresy	tt	TGT
# 3	Bajt zdrojovej adresy	EE	SRC
# 4	Doplnkový dĺžkový bajt	01	LEN
# 5	Identifikátor služby pre Positive Response TesterPresent	7E	TPPR
# 6	Kontrolný súčet	00–FF	CS

CPR_081 Služba podporuje nasledovné záporné odpovedacie kódy:

Tabuľka 12

Správa TesterPresent Negative Response

Bajt #	Názov parametra	Hex hodnota	Mnemotechnická skratka
# 1	Formátový bajt – fyzické adresovanie	80	FMT
# 2	Bajt cieľovej adresy	tt	TGT
# 3	Bajt zdrojovej adresy	EE	SRC
# 4	Doplnkový dĺžkový bajt	03	LEN
# 5	Identifikátor služby pre Negative Response	7F	NR
# 6	Identifikátor služby pre požiadavku TesterPresent	3E	TP
# 7	responseCode = [SubfunctionNotsupported_InvalidFormat]	12	RC_SFNS_IF
	incorrectMessageLength	13	RC_IML
# 8	Kontrolný súčet	00–FF	CS

5. RIADIACE SLUŽBY

Disponibilné služby sú uvedené v nasledovnej tabuľke:

Tabuľka 13

Riadiace služby

Názov služby	Popis
StartDiagnosticSession	Klient žiada zahájenie diagnostickej relácie s JV
SecurityAccess	Klient žiada prístup k funkciám vyhradeným pre oprávnených užívateľov

5.1 **Služba StartDiagnosticSession**

5.1.1 ***Popis správy***

CPR_025 Služba StartDiagnosticSession sa používa k tomu, aby sa mohli v serveri aktivovať rôzne diagnostické relácie. Diagnostická relácia umožňuje aktivovať určité služby podľa tabuľky 17. Relácia môže aktivovať pre výrobcu vozidla špecifické služby, ktoré nie sú súčasťou tohoto dokumentu. Implementačné pravidlá musia zodpovedať týmto požiadavkám:

– v JV je aktívna vždy presne jedna diagnostická relácia,

– JV vždy zaháji StartDiagnosticSession pri každom zapnutí. Ak sa nezaháji žiadna iná diagnostická relácia, potom StartDiagnosticSession pokračuje tak dlho, ako dlho je zapnutá JV,

– ak si diagnostickú reláciu, ktorá už prebieha, vyžiadalo skúšobné zariadenie, potom JV pošle správu s kladnou odpoveďou (positive response),

– kedykoľvek skúšobné zariadenie požiada o novú diagnostickú reláciu, JV najprv pošle správu StartDiagnosticSession s kladnou odpoveďou predtým, než sa aktivuje v JV nová relácia. Ak JV nemôže zahájiť požadovanú novú diagnostickú reláciu, potom odpovedá správou StartDiagnosticSession so zápornou odpoveďou a pokračuje prebiehajúca relácia.

CPR_026 Diagnostická relácia začne len vtedy keď bola medzi klientom a JV vytvorená komunikácia.

CPR_027 Po úspešnej StartDiagnosticSession sú aktívne časové parametre definované v tabuľke 4, pričom je parameter diagnosticSession v požiadavkovej správe nastavený na „StandardDiagnosticSession“, ak bola predtým aktivovaná iná diagnostická relácia.

5.1.2 ***Formát správy***

CPR_028 Formáty správ pre prvky StartDiagnosticSession sú uvedené v nasledovných tabuľkách:

Tabuľka 14

Požiadavková správa StartDiagnosticSession

Bajt #	Názov parametra	Hex hodnota	Mnemotechnická skratka
# 1	Formátový bajt – fyzické adresovanie	80	FMT
# 2	Bajt cieľovej adresy	EE	TGT
# 3	Bajt zdrojovej adresy	tt	SRC
# 4	Doplnkový dĺžkový bajt	02	LEN
# 5	Identifikátor služby pre požiadavku StartDiagnosticSession	10	STDS
# 6	diagnosticSession = (jedna hodnota z tabuľky 17)	xx	DS_...
# 7	Kontrolný súčet	00–FF	CS

Tabuľka 15

Správa Positive Response na StartDiagnosticSession

Bajt #	Názov parametra	Hex hodnota	Mnemotechnická skratka
# 1	Formátový bajt – fyzické adresovanie	80	FMT
# 2	Bajt cieľovej adresy	tt	TGT
# 3	Bajt zdrojovej adresy	EE	SRC
# 4	Doplnkový dĺžkový bajt	02	LEN
# 5	Identifikátor služby pre Positive Response na StartDiagnosticSession	50	STDSPR
# 6	diagnosticSession = (rovnaká hodnota ako bajt # 6 z tabuľky 14)	xx	DS_...
# 7	Kontrolný súčet	00–FF	CS

Tabuľka 16

Správa Negative Response na StartDiagnosticSession

Bajt #	Názov parametra	Hex hodnota	Mnemotechnická skratka
# 1	Formátový bajt – fyzické adresovanie	80	FMT
# 2	Bajt cieľovej adresy	tt	TGT
# 3	Bajt zdrojovej adresy	EE	SRC
# 4	Doplnkový dĺžkový bajt	03	LEN
# 5	Identifikátor služby pre Negative Response	7F	NR
# 6	Identifikátor služby pre požiadavku StartDiagnosticSession	10	STDS
# 7	ResponseCode = (subFunctionNotSupported([a]) incorrectMessageLength([b]) conditionsNotCorrect([c]))	12 13 22	RC_SFNS RC_IML RC_CNC
# 8	Kontrolný súčet	00–FF	CS

([a]) Hodnota vložená v bajt # 6 požiadavkovej správy nie je podporovaná, t. j. nie je definovaná v tabuľke 17.

([b]) Dĺžka správy je chybná.

([c]) Kritériá pre požiadavku StartDiagnosticSession nie sú splnené.

5.1.3 ***Definícia parametra***

CPR_029 Parameter *diagnosticSession* (DS_) používa služba StartDiagnosticSession na voľbu špecifického správania servera(ov). V tomto dokumente sú špecifikované tieto diagnostické relácie:

Tabuľka 17

Definície hodnôt diagnosticSession

Hex	Popis	Mnemotechnická skratka
81	StandardDiagnosticSession Táto diagnostická relácia umožňuje všetky služby špecifikované v tabuľke 1 v stĺpci 4 „SD“. Tieto služby umožňujú čítanie dát zo servera (JV). Táto diagnostická relácia je aktívna po úspešne dokončenej inicializácii medzi klientom (skúšobným zariadením) a serverom (JV). Táto diagnostická relácia môže byť prepísaná inými diagnostickými reláciami špecifikovanými v tomto odseku.	SD
85	ECUProgrammingSession Táto diagnostická relácia umožňuje všetky služby špecifikované v tabuľke 1 v stĺpci 6 „ECUPS“. Tieto služby podporujú programovanie pamäti servera (JV). Táto diagnostická relácia môže byť prepísaná inými diagnostickými reláciami špecifikovanými v tomto odseku.	ECUPS
87	ECUAdjustmentSession Táto diagnostická relácia umožňuje všetky služby špecifikované v tabuľke 5 v stĺpci 6 „ECUAS“. Tieto služby podporujú riadenie vstupov/výstupov servera (JV). Táto diagnostická relácia môže byť prepísaná inými diagnostickými reláciami špecifikovanými v tomto odseku.	ECUAS

5.2 **Služba SecurityAccess**

Písanie kalibračných dát alebo prístup ku kalibračnému vstupnému/výstupnému vedeniu nie je možný, pokiaľ JV nie je v režime kalibrácie. Okrem vloženia platnej dielenskej karty do JV je potrebné zapísať vhodný PIN do JV predtým, než je udelený prístup k režimu kalibrácie.

Služba SecurityAccess pozostáva z požiadavky „requestSeed“, za ktorou nasleduje prípadne správa SecurityAccess „sendKey“. Služba SecurityAccess sa musí vykonať po službe StartDiagnisticSession.

Pripúšťa sa zápis PIN–u alternatívnymi metódami.

5.2.1 ***Popis správy***

Služba SecurityAccess obsahuje správu SecurityAccess "requestSeed", za ktoru prípadne nasleduje správa SecurityAccess "sendKey". Služba SecurityAccess sa musí vykonať po službe StartDiagnosticSession.

CPR_033 Skúšobné zariadenie používa správu SecurityAccess „requestSeed“ na kontrolu, či je jednotka vozidla pripravená akceptovať PIN.

CPR_034 Ak je už jednotka vozidla v režime KALIBRÁCIE, odpovie na požiadavku odoslaním „seed“ 0x0000, s pomocou služby SecurityAccess Positive Response.

CPR_035 Ak je už jednotka vozidla pripravená akceptovať PIN na overenie dielenskej karty, odpovie na požiadavku odoslaním „seed“ väčším než 0x0000, s pomocou služby SecurityAccess Positive Response.

CPR_036 Ak nie je jednotka vozidla pripravená akceptovať PIN zo skúšobného zariadenia, buď z dôvodu neplatnosti dielenskej karty alebo preto, že nebola vložená žiadna dielenská karty alebo, že jednotka vozidla očakáva udanie PIN–u inou metódou, odpovie na požiadavku s použitím Negative Response s odpovedacím kódom conditionsNotCorrectOrRequestSequenceError.

CPR_037 Skúšobné zariadenie potom prípadne použije správu SecurityAccess „sendKey“ na odoslanie PINU–u na jednotku vozidla. Aby bol dostatok času na uskutočnenie autentifikačného procesu karty, JV použije záporný odpovedací kód „requestCorrectlyReceived_ResponsePending na

predĺženie času na odpoveď. Avšak maximálny čas na odpoveď nesmie prekročiť päť minút. Ihneď po dokončení požadovanej služby, JV odošle správu s kladnou alebo zápornou odpoveďou s iným odpovedacím kódom než bol predchádzajúci. Záporný odpovedací kód requestCorrectlyReceived–ResponsePending môže JV opakovať až kým nie je požadovaná služby dokončená a nie je poslaná konečná odpovedacia správa.

CPR_038 Jednotka vozidla odpovie na túto správu s pomocou služby SecurityAccess Positive Response len vtedy, keď je v režime KALIBRÁCIE.

CPR_039 V nasledovných prípadoch musí jednotka vozidla odpovedať na túto správu správou Negative Response s takto nastavenými odpovedacími kódmi:

– subFunctionNot supported: neplatný formát pre parameter subfunkcie (accessType),

– conditionsNotCorrectOrRequestSequenceError: jednotka vozidla nie je pripravená akceptovať zápis PIN,

– invalidKey: neplatné PIN, počet povolených skúšobných pokusov sa však neprekročil,

– exceededNumberOfAttempts: neplatné PIN, prekročil sa počet povolených skúšobných pokusov,

– generalReject: správne PIN no vzájomná autentifikácia s dielenskou kartou nebola úspešná.

5.2.2 ***Formát správy – SecurityAccess – requestSeed***

CPR_040 Formáty správ pre prvky SecurityAccess „requestSeed“ sú uvedené v nasledovných tabuľkách:

Tabuľka 18

Požiadavková správa SecurityAccess – requestSeed

Bajt #	Názov parametra	Hex hodnota	Mnemotechnická skratka
# 1	Formátový bajt – fyzické adresovanie	80	FMT
# 2	Bajt cieľovej adresy	EE	TGT
# 3	Bajt zdrojovej adresy	tt	SRC
# 4	Doplnkový dĺžkový bajt	02	LEN
# 5	Identifikátor služby pre požiadavku SecurityAccess	27	SA
# 6	accessType – requestSeed	7D	AT_RSD
# 7	Kontrolný súčet	00–FF	CS

Tabuľka 19

Správa Positive Response na SecurityAccess requestSeed

Bajt #	Názov parametra	Hex hodnota	Mnemotechnická skratka
# 1	Formátový bajt – fyzické adresovanie	80	FMT
# 2	Bajt cieľovej adresy	tt	TGT
# 3	Bajt zdrojovej adresy	EE	SRC
# 4	Doplnkový dĺžkový bajt	04	LEN
# 5	Identifikátor služby Positive Response	67	SAPR
# 6	accessType – requestSeed	7D	AT_RSD
# 7	Seed High	00–FF	SEEDH
# 8	Seed Low	00–FF	SEEDL
# 9	Kontrolný súčet	00–FF	CS

Tabuľka 20

Správa Negative Response na SecurityAccess

Bajt #	Názov parametra	Hex hodnota	Mnemotechnická skratka
# 1	Formátový bajt – fyzické adresovanie	80	FMT
# 2	Bajt cieľovej adresy	tt	TGT
# 3	Bajt zdrojovej adresy	EE	SRC
# 4	Doplnkový dĺžkový bajt	03	LEN
# 5	Identifikátor služby pre Negative Response	7F	NR
# 6	Identifikátor služby pre požiadavku SecurityAccess	27	SA
# 7	responseCode=(conditionsNotCorrectOrRequestSequenceError	22	RC_CNC
	incorrectMessageLength	13	RC_IML
# 8	Kontrolný súčet	00–FF	CS

5.2.3 ***Formát správy – SecurityAccess – sendKey***

CPR_041 Formáty správ pre prvky SecurityAccess „sendKey“ sú uvedené v nasledovných tabuľkách:

Tabuľka 21

Požiadavková správa SecurityAccess – sendKey

Bajt #	Názov parametra	Hex hodnota	Mnemotechnická skratka
# 1	Formátový bajt – fyzické adresovanie	80	FMT
# 2	Bajt cieľovej adresy	EE	TGT
# 3	Bajt zdrojovej adresy	tt	SRC
# 4	Doplnkový dĺžkový bajt	m+2	LEN
# 5	Identifikátor služby pre požiadavku SecurityAccess	27	SA
# 6	accessType – sendKey	7E	AT_SK
# 7 až # 0+6	Kľúč # 1 (High) ... Kľúč # m (low, m musí mať hodnoty minimálne 4 a maximálne 8)	xx ... xx	KEY
# 7	Kontrolný súčet	00–FF	CS

Tabuľka 22

Správa Positive Response na SecurityAccess sendKey

Bajt #	Názov parametra	Hex hodnota	Mnemotechnická skratka
# 1	Formátový bajt – fyzické adresovanie	80	FMT
# 2	Bajt cieľovej adresy	tt	TGT
# 3	Bajt zdrojovej adresy	EE	SRC
# 4	Doplnkový dĺžkový bajt	02	LEN
# 5	Identifikátor služby Positive Response na SecurityAccess	67	SAPR
# 6	accessType – sendKey	7E	AT_SK
# 7	Kontrolný súčet	00–FF	CS

Tabuľka 23

Správa Negative Response na SecurityAccess

Bajt #	Názov parametra	Hex hodnota	Mnemotechnická skratka
# 1	Formátový bajt – fyzické adresovanie	80	FMT
# 2	Bajt cieľovej adresy	tt	TGT
# 3	Bajt zdrojovej adresy	EE	SRC
# 4	Doplnkový dĺžkový bajt	03	LEN
# 5	Identifikátor služby pre Negative Response	7F	NR
# 6	Identifikátor služby pre požiadavku SecurityAccess	27	SA
# 7	ResponseCode=(generalReject subFunctionNotSuported IncorrectMessageLength conditionsNotCorrectOrRequest SequenceError InvalideKey ExeededNumberOfAttempts requestCorrectlyReceived–ResponsePending)	10 12 13 22 35 36 78	RC_GR RC_SFNS RC_IML RC_CNC RC_IK RC_ENA RC_RCR_RP
# 8	Kontrolný súčet	00–FF	CS

6. SLUŽBY PRENOSU DÁT

Disponibilné služby sú uvedené v nasledovnej tabuľke:

Tabuľka 24

Služby prenosu dát

Názov služby	Popis
ReadDataByIdentifier	Klient žiada prenos aktuálnej hodnoty záznamu pomocou recordDataIdentifier
WriteDataByIdentifier	Klient žiada napísať záznam sprístupnený pomocou recordDataIdentifier

6.1 **Služba ReadDataByIdentifier**

6.1.1 ***Popis správy***

CPR_050 Službu ReadDataByIdentifier používa klient na vyžiadanie hodnôt dátového záznamu zo servera. Dáta sú identifikované pomocou recordDataIdentifier. Výrobca JV zodpovedný za to, aby boli pri vykonávaní tejto služby splnené podmienky serveru.

6.1.2 ***Formát správy***

CPR_051 Formáty správ pre prvky ReadDataByIdentifier sú uvedené v nasledovných tabuľkách:

Tabuľka 25

Požiadavková správa ReadDataByIdentifier

Bajt #	Názov parametra	Hex hodnota	Mnemotechnická skratka
# 1	Formátový bajt – fyzické adresovanie	80	FMT
# 2	Bajt cieľovej adresy	EE	TGT
# 3	Bajt zdrojovej adresy	tt	SRC
# 4	Doplnkový dĺžkový bajt	03	LEN
# 5	Identifikátor služby pre požiadavku ReadDataByIdentifier	22	RDBI
# 6 a # 7	recordDataIdentifier = (hodnota z tabuľky 28)	xxxx	RDI_...
# 8	Kontrolný súčet	00–FF	CS

Tabuľka 26

Správa Positive Response na ReadDataByIdentifier

Bajt #	Názov parametra	Hex hodnota	Mnemotechnická skratka
# 1	Formátový bajt – fyzické adresovanie	80	FMT
# 2	Bajt cieľovej adresy	tt	TGT
# 3	Bajt zdrojovej adresy	EE	SRC
# 4	Doplnkový dĺžkový bajt	m+3	LEN
# 5	Identifikátor služby Positive Response na ReadDataByIdentifier	62	RDBIPR
# 6 a # 7	recordDataIdentifier = (rovnaká hodnota ako bajty # 6 a # 7 v tabuľke 25)	xxxx	RDI_...
# 8 až #m+ 7	dataRecord = (data # 1 . . data#m)	xx . . xx	DREC_DATA1 . . DREC_DATAm
# m+8	Kontrolný súčet	00–FF	CS

Tabuľka 27

Správa Negative Response na ReadDataByIdentifier

Bajt #	Názov parametra	Hex hodnota	Mnemotechnická skratka
# 1	Formátový bajt – fyzické adresovanie	80	FMT
# 2	Bajt cieľovej adresy	tt	TGT
# 3	Bajt zdrojovej adresy	EE	SRC
# 4	Doplnkový dĺžkový bajt	03	LEN
# 5	Identifikátor služby Negative Response	7F	NR
# 6	Identifikátor služby pre požiadavku ReadDataByIdentifier	22	RDBI
#7	ResponseCode = (requestOutOfRange incorrectMessageLength conditionsNotCorrect)	31 13 22	RC_ROOR RC_IML RC_CNC
# 8	Kontrolný súčet	00–FF	CS

6.1.3 ***Definícia parametra***

CPR_052 Parameter recordDataIdentifier (RDI_) v požiadavkovej správe ReadDataByIdentifier identifikuje dátový záznam.

CPR_053 Hodnoty recordDataIdentifier definované v tomto dokumente sú uvedené v tabuľke nižšie.

Tabuľka recordDataIdentifier sa skladá zo štyroch stĺpcov a viacerých riadkov.

– Prvý stĺpec (Hex) obsahuje „hexadecimálne hodnoty“ priradené k recordDataIdentifier špecifikovanému v treťom stĺpci.

– Druhý stĺpec (dátový prvok) špecifikuje dátový prvok podľa doplnku 1, na ktorom je založený recordDataIdentifier (niekedy je potrebné prekódovanie).

– Tretí stĺpec (popis) obsahuje zodpovedajúci názov recordDataIdentifier.

– Štvrtý stĺpec (Mnemotechnická skratka) udáva symbol písania tohto recordDataIdentifier.

Tabuľka 28

Definícia hodnôt recordDataIdentifier

Hex	Dátový prvok	Názov recordDataIdentifier (pozri formát v odseku 8.2)	Mnemotechnická skratka
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 Parameter dataRecord (DREC_) používa správa Positive Response na ReadDataByIdentifier k tomu, aby poskytla klientovi (skúšobnému zariadeniu) hodnotu dátového záznamu identifikovaného recordDataIdentifier. Dátové formáty sú špecifikované v odseku 8. Užívateľ môže zaviesť voliteľné dataRecords vrátane špecifických vstupných, interných a výstupných dát, ktoré však v tomto dokumente nie sú definované.

6.2 **Služba WriteDataByIdentifier**

6.2.1 ***Popis správy***

CPR_056 Službu WriteDataByIdentifier používa klient na napísanie hodnôt dátového záznamu pre server. Dáta sú identifikované pomocou recordDataIdentifier. Výrobca JV zodpovedný za to, aby boli pri vykonávaní tejto služby splnené podmienky serveru. Na aktualizáciu parametrov uvedených v tabuľke 28 musí byť JV v režime KALIBRÁCIE.

6.2.2 ***Formát správy***

CPR_057 Formáty správ pre prvky WriteDataByIdentifier sú uvedené v nasledovných tabuľkách:

Tabuľka 29

Požiadavková správa WriteDataByIdentifier

Bajt #	Názov parametra	Hex hodnota	Mnemotechnická skratka
# 1	Formátový bajt – fyzické adresovanie	80	FMT
# 2	Bajt cieľovej adresy	EE	TGT
# 3	Bajt zdrojovej adresy	tt	SRC
# 4	Doplnkový dĺžkový bajt	m+3	LEN
# 5	Identifikátor služby pre požiadavku WriteDataByIdentifier	2E	WDBI
# 6 a # 7	recordDataIdentifier = (hodnota z tabuľky 28)	xxxx	RDI_...
# 8 až #m+ 7	dataRecord = (data # 1 . . data#m)	xx . . xx	DREC_DATA1 . . DREC_DATAm
# m+8	Kontrolný súčet	00–FF	CS

Tabuľka 30

Správa Positive Response na WriteDataByIdentifier

Bajt #	Názov parametra	Hex hodnota	Mnemotechnická skratka
# 1	Formátový bajt – fyzické adresovanie	80	FMT
# 2	Bajt cieľovej adresy	tt	TGT
# 3	Bajt zdrojovej adresy	EE	SRC
# 4	Doplnkový dĺžkový bajt	03	LEN
# 5	Identifikátor služby Positive Response na WriteDataByIdentifier	6E	WDBIPR
# 6 a # 7	recordDataIdentifier = (rovnaká hodnota ako bajty # 6 a # 7 v tabuľke 29)	xxxx	RDI_...
# 8	Kontrolný súčet	00–FF	CS

Tabuľka 31

Správa Negative Response na WriteDataByIdentifier

Bajt #	Názov parametra	Hex hodnota	Mnemotechnická skratka
# 1	Formátový bajt – fyzické adresovanie	80	FMT
# 2	Bajt cieľovej adresy	tt	TGT
# 3	Bajt zdrojovej adresy	EE	SRC
# 4	Doplnkový dĺžkový bajt	03	LEN
# 5	Identifikátor služby Negative Response	7F	NR
# 6	Identifikátor služby pre požiadavku WriteDataByIdentifier	2E	WDBI
#7	ResponseCode = (requestOutOfRange incorrectMessageLength conditionsNotCorrect)	31 13 22	RC_ROOR RC_IML RC_CNC
# 8	Kontrolný súčet	00–FF	CS

6.2.3 ***Definícia parametra***

Parameter recordDataIdentifier (RDI_) je definovaný v tabuľke 28.

Parameter recordDataIdentifier (DREC_) používa požiadavková správa WriteDataByIdentifier k tomu, aby poskytla serveru (JV) hodnoty dátového záznamu identifikovaného pomocou recordDataIdentifier. Dátové formáty sú špecifikované v odseku 8.

7. RIADENIE SKÚŠOBNÝCH IMPULZOV – RIADENIE VSTUPU/VÝSTUPU FUNKČNEJ JEDNOTKY

Disponibilné služby sú uvedené v nasledovnej tabuľke:

Tabuľka 32

Riadenie vstupu/výstupu funkčnej jednotky

Názov služby	Popis
InputOutputControlByIdentifier	Klient požaduje riadenie vstupu/výstupu špecifického pre server.

7.1 **Služba InputOutputControlByIdentifier**

7.1.1 ***Popis správy***

Cez predný konektor je možné použitím vhodného skúšobného zariadenia riadiť alebo monitorovať skúšobné impulzy.

CPR_058 Toto kalibračné vstupné/výstupné signalizačné vedenie môže byť konfigurované s príkazom K–vedenie použitím služby InputOutputControlByIdentifier na voľbu vstupnej alebo výstupnej funkcie pre vedenie. Stavy vedenia sú tieto:

– deaktivované,

– speedSignalInput, kde sa kalibračné vstupné/výstupné vedenie používa na vstup rýchlostného signálu (skúšobný signál), ktorým sa nahrádza rýchlostný signál snímača pohybu,

– realTimeSpeedSignalOutputSensor, kde sa kalibračné vstupné/výstupné signalizačné vedenie používa na výstup rýchlostného signálu senzora pohybu,

– RTCOutput, kde sa kalibračné vstupné/výstupné signalizačné vedenie používa na výstup UTCčasového signálu.

CPR_059 Aby sa konfiguroval stav vedenia, musí sa jednotka vozidla nachádzať v relácii nastavenia a musí byť v režime KALIBRÁCIE. Pri skončení relácie nastavenia alebo režimu KALIBRÁCIE musí jednotka vozidla zabezpečiť, aby sa kalibračné vstupné/výstupné signalizačné vedenie vrátilo do „deaktivovaného“ (štandardného) stavu.

CPR_060 Ak sa rýchlostné impulzy vrátia v reálnom čase vstupného signalizačného vedenia JV, zatiaľčo je kalibračné vstupné/výstupné signalizačné vedenie nastavené na vstup, potom kalibračné vstupné/výstupné signalizačné vedenie musí byť nastavené na výstup alebo sa musí vrátiť do deaktivovaného stavu.

CPR_061 Sekvencia musí:

– vytvoriť komunikáciu prostredníctvom služby StartCommunication;

– zaviesť reláciu nastavenia prostredníctvom služby StartDiagnosticSession a prevádzkového režimu KALIBRÁCIE (poradie týchto dvoch operácií nie je dôležité);

– zmeniť stav výstupu prostredníctvom služby InputOutputControlByIdentifier.

7.1.2 ***Formát správy***

CPR_062 Formáty správ pre prvky InputOutputControlByIdentifier sú uvedené v nasledovných tabuľkách:

Tabuľka 33

Požiadavková správa InputOutputControlByIdentifier

Bajt #	Názov parametra	Hex hodnota	Mnemotechnická skratka
# 1	Formátový bajt – fyzické adresovanie	80	FMT
# 2	Bajt cieľovej adresy	EE	TGT
# 3	Bajt zdrojovej adresy	tt	SRC
# 4	Doplnkový dĺžkový bajt	xx	LEN
# 5	Identifikátor služby požiadavku InputOutputControlByIdentifier	2F	IOCBI
# 6 a # 7	InputOutputIdentifier = (CalibrationInputOutput)	P960	IOI_CIO
# 8 alebo # 8 až # 9	ControlOptionRecord=(		COR_...
	InputOutputControlParameter – jedna hodnota z tabuľky 36	xx	IOCP_...
	ControlState – jedna hodnota z ta– buľky 38 (pozri poznámku nižšie))	xx	CS_...
# 9 alebo # 10	Kontrolný súčet	00–FF	CS
Poznámka: parameter controlState je k dispozícii len v niektorých prípadoch (pozri 7.1.3).			

Tabuľka 34

Správa Positive Response na InputOutputControlByIdentifier

Bajt #	Názov parametra	Hex hodnota	Mnemotechnická skratka
# 1	Formátový bajt – fyzické adresovanie	80	FMT
# 2	Bajt cieľovej adresy	tt	TGT
# 3	Bajt zdrojovej adresy	EE	SRC
# 4	Doplnkový dĺžkový bajt	xx	LEN
# 5	Identifikátor služby Positive Response na InputOutputControlByIdentifier	6F	IOCBIPR
# 6 a # 7	InputOutputIdentifier = (CalibrationInputOutput)	F960	IOI_CIO
# 8 alebo # 8 až # 9	ControlStatusRecord=(inputOutputControlParameter (rovnaká hodnota ako # 8 v tabuľke 33) controlState (rovnaká hodnota ako # 9 v tabuľke 33))(ak je to aplikovateľné)	 xx xx	CSR_... IOCP_... CS_...
# 9 alebo # 10	Kontrolný súčet	00–FF	CS

Tabuľka 35

Správa Negative Response na InputOutputControlByIdentifier

Bajt #	Názov parametra	Hex hodnota	Mnemotechnická skratka
# 1	Formátový bajt – fyzické adresovanie	80	FMT
# 2	Bajt cieľovej adresy	tt	TGT
# 3	Bajt zdrojovej adresy	EE	SRC
# 4	Doplnkový dĺžkový bajt	03	LEN
# 5	Identifikátor služby Negative Response	7F	NR
# 6	Identifikátor služby pre požiadavku InputOutputControlByIdentifier	2F	IOCBI
#7	responseCode = (incorrectMessageLength conditionsNotCorrect) requestOutOfRange deviceControlLimitExceeded)	 13 22 31 7A	 RC_IML RC_CNC RC_ROOR RC_DCLE
# 8	Kontrolný súčet	00–FF	CS

7.1.3 ***Definícia parametra***

CPR_064 Parameter InputOutputControlParamater (IOCP_) je definovaný v nasledovnej tabuľke:

Tabuľka 36

Definícia hodnôt pre inputOutputControlParameter

Hex	Popis	Mnemotechnická skratka
00	ReturnControlToECU Táto hodnota oznamuje serveru (JV), že skúšobné zariadenie skončilo s riadením kalibračného vstupného/výstupného signalizačného vedenia.	RCTECU
01	ResetToDefault Táto hodnota oznamuje serveru (JV), že sa od neho požaduje, aby resetoval kalibračné vstupné/výstupné signalizačné vedenie na jeho štandardný stav.	RTD
03	ShortTermAdjustment Táto hodnota oznamuje serveru (JV), že sa od neho požaduje, aby nastavil kalibračné vstupné/výstupné signalizačné vedenie na hodnotu obsiahnutú v parametri controlState.	STA

CPR_065 Parameter controlState je k dispozícii len vtedy, keď inputOutputControlParameter je nastavený na ShortTermAdjustment a je definovaný v nasledovnej tabuľke:

Tabuľka 37

Definícia hodnôt pre controlState

Režim	Hex hodnota	Popis
Deaktivovaný	00	Vstupné/výstupné vedenie je deaktivované (štandardný stav)
Aktivovaný	01	Kalibračné vstupné/výstupné vedenie aktivované ako speedSignalInput
Aktivovaný	02	Kalibračné vstupné/výstupné vedenie aktivované ako realTimeSpeedSignalOutuputSensor
Aktivovaný	03	Kalibračné vstupné/výstupné vedenie aktivované ako RTCOutput

8. FORMÁTY DATARECORDS

Tento odsek obsahuje:

– všeobecné pravidlá uplatňované na parametre prenášané jednotkou vozidla na skúšobné zariadenie,

– formáty používané pre dáta prenášané cez služby prenosu dát popísané v odseku 6.

CPR_067 Všetky identifikované parametre sú podporované jednotkou vozidla.

CPR_068 Dáta prenášané JV na skúšobné zariadenie, ako odpoveď na požiadavkovú správu musia zodpovedať meranému typu (t. j. aktuálnej hodnote požadovaného parametra, ktorý JV meria alebo sleduje).

8.1 **Rozsahy hodnôt prenášaného parametra**

CPR_069 Tabuľka 38 definuje rozsahy používané na stanovenie platnosti prenášaného parametra.

CPR_070 Hodnoty v rozsahu „error indicator“ môžu jednotke vozidla ihneď oznámiť, že platné parametrické dáta nie sú k dispozícii kvôli chybe v záznamovom zariadení.

CPR_071 Hodnoty v rozsahu „not available“ môžu jednotke vozidla podať správu obsahujúcu parameter, ktorý nie je dostupný alebo nie je v tomto module podporovaný. Hodnoty v rozsahu „not requested“ môžu na jednotku vozidla preniesť príkazovú správu a identifikovať také parametre, na ktoré sa od prijímacieho zariadenia neočakáva žiadna odpoveď.

CPR_072 Ak chyba komponentu zabráni prenosu platných dát pre parameter, mal by sa namiesto požadovaných dát parametra, použiť indikátor chýb popísaný v tabuľke 38. Ak však merané alebo vypočítané dáta majú hodnotu, ktorá je síce platná, no leží mimo definovaného rozsahu parametra, indikátor chýb by sa nemal použiť. Dáta by sa mali preniesť s použitím primeranej minimálnej alebo maximálnej hodnoty parametra.

Tabuľka 38

Rozsah hodnôt pre dataRecords

Názov rozsahu hodnôt	1 bajt (Hex hodnota)	2 bajty (Hex hodnota)	4 bajty (Hex hodnota)	ASCII
Platný signál	00 až FA	0000 až FAFF	00000000 až FAFFFFFF	1 až 254
Indikátor špecifický pre parameter	FB	FB00 až FBFF	FB000000 až FBFFFFFF	žiadny
Vyhradený rozsah pre budúce bity indikátora	FC až FD	FC00 až FDFF	FC000000 až FDFFFFFF	žiadny
Indikátor chýb	FE	FE00 až FEFF	FE000000 až FEFFFFFF	0
Nie je k dispozícii alebo sa nepožaduje	FF	FF00 až FFFF	FF000000 až FFFFFFFF	FF

CPR_073 Pre parametre kódovaný v ASCII, je znak ASCII „*“ vyhradený pre oddeľovač.

8.2 **Formáty dataRecords**

Tabuľka 39 až 42 sú uvedené formáty pre služby ReadDataByIdentifier a WriteDataByIdentifier.

CPR_074 V tabuľke 39 je uvedená dĺžka, rozlíšenie a prevádzkový rozsah pre každý parameter identifikovaný pomocou recordDataIdentifier:

Tabuľka 39

Formát dataRecords

Názov parametra	Dĺžka dát (bajty)	Rozlíšenie	Prevádzkový rozsah
TimeDate	8	Pozri tabuľku 40	
HighResolutionTotalVehicleDistance	4	prírastok 5 m/bit, východzia hodnota 0 m	0 až + 21 055 406 km
Kfactor	2	prírastok 0,001 impulz/m/bit, východzia hodnota 0	0 až 64,255 impulz/m
LfactorTyreCircumference	2	prírastok 0,125 10^{-3}/bit, východzia hodnota 0	0 až 8 031 m
WvehicleCharacteristicFactor	2	prírastok 0,001 impulz/m/bit, východzia hodnota 0	0 až 64,255 impulz/m
TyreSize	15	ASCII	ASCII
NextCalibrationDate	3	Pozri tabuľku 41	
SpeedAuthorised	2	prírastok 1/256 km/h/bit, východzia hodnota 0	0 až 250 996 km/h
RegisteringMemberState	3	ASCII	ASCII
VehicleRegistrationNumber	14	Pozri tabuľku 42	
VIN	17	ASCII	ASCII

CPR_075 Tabuľka 40 obsahuje formáty rôznych bajtov parametra TimeData:

Tabuľka 40

Podrobný formát TimeDate (recordDataIdentifier hodnota # F00B)

Bajt	Definícia parametra	Rozlíšenie	Prevádzkový rozsah
1	Sekundy	prírastok 0,25 s/bit, východzia hodnota 0 s	0 až 59,75 s
2	Minúty	prírastok 1 min/bit, východzia hodnota 0 min	0 až 59 min
3	Hodiny	prírastok 1 h/bit, východzia hodnota 0 h	0 až 23 h
4	Mesiac	prírastok 1 mesiac/bit, východzia hodnota 0 mesiacov	1 až 12 mesiacov
5	Deň	prírastok 0,25 dňa/bit, východzia hodnota 0 dní (pozri poznámku pod tabuľkou 41)	0,25 až 31,75 dní
6	Rok	prírastok 1 rok/bit, východzia hodnota rok +1985 (pozri poznámku pod tabuľkou 41)	rok 1985 až 2235
7	Miestna východisková minútová hodnota	prírastok 1 min/bit, východzia hodnota – 125 min	– 59 až 59 min
8	Miestna východisková hodinová hodnota	prírastok 1 h/bit, východzia hodnota –125 h	– 23 až + 23 h

CPR_076 Tabuľka 41 obsahuje formáty rôznych bajtov parametra NextCalibrationDate:

Tabuľka 41

Podrobný formát NextCalibrationDate (recordDataIdentifier hodnota # F022)

Bajt	Definícia parametra	Rozlíšenie	Prevádzkový rozsah
1	Mesiac	prírastok 1 mesiac/bit, východzia hodnota 0 mesiacov	1 až 12 mesiacov
2	Deň	prírastok 0,25 dňa/bit, východzia hodnota 0 dní (pozri poznámku nižšie)	0,25 až 31,75 dní
3	Rok	prírastok 1 rok/bit, východzia hodnota rok +1985 (pozri poznámku nižšie)	rok 1985 až 2235

Poznámka týkajúca sa použitia parametra „deň“:

1. Hodnota dátumu 0 je neplatná. Hodnoty 1, 2, 3 a 4 sa používajú na označenie prvého dňa mesiaca; hodnoty 5, 6,7 a 8 označujú druhý deň mesiaca; atď.
2. Tento parameter nemá vplyv alebo nemení hodinové parametre uvedené vyššie.

Poznámka týkajúca sa použitia parametra „rok“:

Hodnota 0 pre rok označuje rok 1985; hodnota 1 označuje 1986; atď.

CPR_078 Tabuľka 42 obsahuje formáty rôznych bajtov VehicleRegistrationNumber parametra:

Tabuľka 42

Podrobný formát VehicleRegistrationNumber (recordDataIdentifier hodnota # F07E)

Bajt	Definícia parametra	Rozlíšenie	Prevádzkový rozsah
1	Kódovaná strana (definovaná v doplnku 1)	ASCII	01 až 0A
2 až 14	Registračné číslo vozidla (definovaná v doplnku 1)	ASCII	ASCII

Doplnok 9

TYPOVÉ SCHVÁLENIE – ZOZNAM MINIMÁLNE POŽADOVANÝCH SKÚŠOK

Obsah

1. ÚVOD

1.1 **Typové schválenie**

EHS typové schválenie záznamového zariadenia (alebo komponentu) alebo tachografovej karty je založené na:

– bezpečnostnej certifikácii vykonanej orgánom ITSEC na základe bezpečnostného cieľa v úplnej zhode s doplnkom 10 tejto prílohy,

– funkčnej certifikácii vykonanej orgánom členského štátu, ktorou sa potvrdzuje, že skúšaný diel spĺňa požiadavky tejto prílohy z hľadiska vykonávaných funkcií, presnosti merania a environmentálnych charakteristík,

– certifikácii interoperability vykonanej príslušným orgánom, ktorou sa potvrdzuje, že záznamové zariadenie (alebo tachografová karta) je plne interoperabilné s príslušným modelom tachografovej karty (alebo záznamového zariadenia) (pozri kapitolu VIII tejto prílohy).

Tento doplnok špecifikuje skúšky, ktoré ako minimum musí vykonať orgán členského štátu počas funkčných skúšok a ktoré ako minimum musí vykonať príslušný orgán počas skúšok interoperability. Postupy vykonania skúšok prípadne druh skúšok nie je ďalej špecifikovaný.

Aspekty bezpečnostnej certifikácie nie sú predmetom tohto doplnku. Ak niektoré skúšky potrebné na typové schválenie sa vykonajú počas posudzovania bezpečnosti a certifikačného procesu, potom sa tieto skúšky nemusia znovu vykonať. V tomto prípade sa môžu kontrolovať len výsledky týchto bezpečnostných skúšok. Pre informáciu, požiadavky, ktorých skúšanie sa očakáva (alebo ktoré sa úzko viažu k skúškam, ktoré sa majú vykonať) počas bezpečnostnej certifikácie, sú označené v tomto doplnku „*“.

Tento doplnok uvažuje so samostatným typovým schválením snímača pohybu a jednotky vozidla, ako komponentov záznamového zariadenia. Interoperabilita medzi každým modelom snímača a každým modelom jednotky vozidla sa nevyžaduje a preto sa typové schválenie snímača pohybu môže udeliť len v spojení s typovým schválením jednotky vozidla a naopak.

1.2 **Referenčné dokumenty**

V tomto doplnku sú použité tieto referenčné dokumenty:

IEC 68–2–1	Environmental testing – Part 2: Tests – Tests A: Cold. 1990 + Amendment 2: 1994 (Skúšky vplyvu vonkajších činiteľov prostredia – Časť 2 – Skúšky A: Chlad. 1990 + Zmena 2: 1994).
IEC 68–2–2	Environmental testing – Part 2: Tests – Tests B: Dry heat. 1974 + Amendment 2: 1994. (Skúšky vplyvu vonkajších činiteľov prostredia – Časť 2 – Skúšky B: Suché teplo. 1974 + Zmena 2: 1994).
IEC 68–2–6	Basic environmental testing procedures – Test methods – Test Fc and guidance: Vibration (sinusoidal). 6th edition: 1985 (Základné skúšky vplyvu vonkajších činiteľov prostredia – Skúšobné metódy – Skúška Fc a návod: Vibrácie (sínusové). 6. vydanie:1985).
IEC 68–2–14	Basic environmental testing procedures – Test methods – Test N: Change of temperature. Modification 1: 1986. (Základné skúšky vplyvu vonkajších činiteľov prostredia – Skúšobné metódy – Skúška N: Zmena teploty. Modifikácia 1: 1986).
IEC 68–2–27	Basic environmental testing procedures – Test methods – Test Ea and guidance: Shock. Edition 3: 1987. (Základné skúšky vplyvu vonkajších činiteľov prostredia – Skúšobné metódy – Skúška Ea a návod. Údery. Vydanie 3: 1987).
IEC 68–2–30	Basic environmental testing procedures – Test methods – Test Db and guidance: Damp heat, cyclic (12 + 12–hour cycle). Modification 1: 1985. (Základné skúšky vplyvu vonkajších činiteľov prostredia – Skúšobné metódy – Skúška Db a návod. Skúšky vlhkým teplom cyklickým (12 + 12 h cyklus) Modifikácia 1: 1985).

IEC 68–2–35	Basic environmental testing procedure – Test methods – Test Fda: Random vibration wide band – Reproductibility High. Modification 1: 1983 (Základné skúšky vplyvu vonkajších činiteľov prostredia – Skúšobné metódy – Skúška Fda: Širokopásmové náhodné vibrácie – Vysoká reprodukovateľnosť. Modifikácia 1: 1983).
IEC 529	Degrees of protection provided by enclosures (IP code). Edition 2: 1989 (Stupne ochrany krytom (IP kód). Vydanie 2: 1989).
IEC 61000–4–2	Electromagnetic Compatibility (EMC) – Testing and measurement techniques – Electrostatic discharge immunity test: 1995/Amendment 1: 1998 (Elektromagnetická kompatibilita (EMC) – Metódy skúšania a merania – Skúška odolnosti proti elektrostatickému výboju: 1995/Zmena 1: 1998).
ISO 7637–1	Road vehicles – Electrical disturbance by conduction and coupling – Part 1: Passenger cars and light commercial vehicles with nominal 12 V supply voltage – Electrical transient conduction along supply lines only. Edition 2: 1990 (Cestné vozidlá – Elektrické rušenie vedením a väzbou – Časť 1: Osobné vozidlá a ľahké úžitkové vozidlá s menovitým napájacím napätím 12 V – Elektrické rušenie vedené len napájacími vodičmi. Vydanie 2: 1990).
ISO 7637–2	Road vehicles – Electrical disturbance by conduction and coupling – Part 2: Commercial vehicles with nominal 24 V supply voltage– Electrical transient conduction along supply lines only. First edition 2: 1990 (Cestné vozidlá – Elektrické rušenie vedením a väzbou – Časť 1: Úžitkové vozidlá s menovitým napájacím napätím 24 V – Elektrické rušenie vedené len napájacími vodičmi. Prvé vydanie: 1990).
ISO 7637–3	Road vehicles – Electrical disturbance by conduction and coupling – Part 3: Vehicles with 12 V or 24 V supply voltage – Electrical transient transmission by capacitive and inductive coupling via lines other than supply lines. First Edition: 1995 + Cor 1: 1995 (Cestné vozidlá – Elektrické rušenie vedením a väzbou – Časť 1: Vozidlá s menovitým napájacím napätím 12 alebo 24 V – Elektrické rušenie kapacitnou a indukčnou väzbou cez vodiče iné než vedené napájacie vodiče. Prvé vydanie: 1995 + Cor. 1:1995).
ISO/IEC 7816–1	Identification cards – Integrated circuit(s) cards with contacts – Part 1: Physical characteristics. First edition: 1998 (Identifikačné karty – Karty s integrovanými obvodmi a s kontaktmi – Časť 1: Fyzikálne vlastnosti. Prvé vydanie: 1998).
ISO/IEC 7816–2	Information technology – Identification cards – Integrated circuit(s) cards with contacts – Part 2: Dimensions and location of the contacts. First edition: 1999 (Informačné technológie – Identifikačné karty – Karty s integrovanými obvodmi a s kontaktmi – Časť 2: Rozmery a umiestnenie kontaktov. Prvé vydanie: 1999).
ISO/IEC 7816–3	Information technology – Identification cards – Integrated circuit(s) cards with contacts – Part 3: Electronic signals and transmission protocol. Edition 2: 1997 (Informačné technológie – Identifikačné karty – Karty s integrovanými obvodmi a s kontaktmi – Časť 3: Elektronické signály a protokoly procesu. Vydanie 2: 1997).
ISO/IEC 10373	Identification cards – Test methods. First edition: 1993 (Identifikačné karty. Skúšobné metódy. Prvé vydanie: 1993).

2. FUNKČNÉ SKÚŠKY JEDNOTKY VOZIDLA

Číslo	Skúška	Popis	Zodpovedajúce požiadavky
1.	**preskúmanie**	**Administratívne**	
1.1	Dokumentácia	Správnosť dokumentácie	
1.2	Výsledky testu výrobcu	Výsledky testu výrobcu vykonané počas montáže. Dôkazy na papieri.	070, 071, 073

2.	**Vizuálna kontrola**	
2.1	Zhoda s dokumentáciou	
2.2	Identifikácia/Označenie	168, 169
2.3	Materiály	163 až 167
2.4	Plombovanie	251
2.5	Vonkajšie rozhrania	
3.	**Funkčné skúšky**	
3.1	Možné funkcie	002, 004, 244
3.2	Režimy prevádzky	006*, 007*, 008*, 009*, 106, 107
3.3	Funkcie a práva na prístup k dátam	010*, 011*, 240, 246, 247
3.4	Vloženie a vytiahnutie monitorovacích kariet	013, 014, 015*, 016*, 106
3.5	Meranie rýchlosti a vzdialenosti	017 až 026
3.6	Meranie času (test vykonaný pri 20 °C)	027 až 032
3.7	Monitorovanie činností vodiča	033 až 043, 106
3.8	Monitorovanie stavu vedenia vozidla	044, 045, 106
3.9	Manuálne zápisy	046 až 050b
3.10	Podnikové zablokovanie	051 až 055
3.11	Monitorovanie kontrolných činností	056, 057
3.12	Zistenie udalostí a/alebo porúch	059 až 069, 106
3.13	Identifikačné dáta jednotky vozidla	075*, 076*, 079
3.14	Dáta pri vložení a vytiahnutí karty vodiča	081* až 083*
3.15	Dáta o činnosti vodiča	084* až 086*
3.16	Miesta začiatku a konca pracovného času	087* až 089*
3.17	Dáta o stave kilometrov	090* až 092*
3.18	Podrobné dáta o rýchlosti	093*
3.19	Dáta o udalostiach	094*, 095
3.20	Dáta o poruchách	096*
3.21	Kalibračné dáta	097*, 098*
3.22	Dáta nastavenia času	100*, 101*
3.23	Dáta o kontrolnej činnosti	102*, 103*
3.24	Dáta o podnikovom blokovaní	104*
3.25	Dáta o činnosti sťahovania	105*
3.26	Dáta o špecifických podmienkach	105a*, 105b*
3.27	Zaznamenávanie a ukladanie na tachografových kartách	108, 109*, 109a*, 110*, 111, 112

3.28	Zobrazovanie		072, 106, 113 až 128, PIC_001, DIS_001
3.29	Tlač		072, 106, 129 až 138, PIC_001, PRT_001 až PRT_012
3.30	Výstraha		106, 139 až 148, PIC_001
3.31	Sťahovanie dát do vonkajších médií		072, 106, 149 až 151
3.32	Výstupné dáta pre doplnkové vonkajšie zariadenia		152, 153
3.33	Kalibrácia		154*, 155*, 156*, 245
3.34	Nastavenie času		157*, 158*
3.35	Nerušenie doplnkovými funkciami		003, 269
4.	**Skúšky vplyvu vonkajšieho prostredia**		
4.1	Teplota	Overenie funkčnosti podľa: – IEC 68–2–1, skúška Ad, doba trvania 72 hodín pri nižšej teplote (–20 °C), 1 hodina prevádzky, 1 hodina mimo prevádzky, – IEC 68–2–2, skúška Bd, doba trvania 72 hodín pri vyššej teplote (+70 °C), 1 hodina prevádzky, 1 hodina mimo prevádzky, Teplotné cykly: overí sa, či jednotka vozidla môže odolať rýchlym zmenám teploty prostredia podľa IEC 68–2–14, skúška Na, 20 cyklov každý pri teplote meniacej sa od nižšej teploty (–20 °C) po vyššiu teplotu (+70 °C) a 2 hodiny zotrvania pri nižšej a vyššej teplote. Pri nižšej a vyššej teplote ako aj počas teplotných cyklov sa môže vykonať menší počet skúšok (u skúšok uvedených v bode 3 tejto tabuľky).	159
4.2	Vlhkosť	Overí sa, či jednotka vozidla môže odolať cyklickej vlhkosti (teplotná skúška) podľa IEC 68–2–30, skúška Db, šesť 24–hodinových cyklov vždy pri teplote meniacej sa od +25 °C do +55 °C a pri relatívnej vlhkosti 97% pri +25 °C a rovnej 93% pri +55 °C.	160
4.3	Vibrácie	1. Sínusové vibrácie: overí sa, či jednotka vozidla môže odolať sí–nusovým vibráciám s týmito charakteristikami: konštantný posuv medzi 5 a 11 Hz: max. 10 mm konštantné zrýchlenie medzi 11 a 300 Hz: 5 g Táto požiadavka sa overí podľa IEC 68–2–6, skúška Fc, s maximálnou dobou trvania 3 x 12 hodín (12 hodín na každú nápravu)	163

		Náhodné vibrácie: 2. overí sa, či jednotka vozidla môže odolať ná–hodným vibráciám s týmito charakteristikami: frekvencia 5–150 Hz, úroveň 0,02 g^2/Hz Táto požiadavka sa overí podľa IEC 68–2–35, skúška Ffda, s minimálnou dobou trvania 3 x 12 hodín (12 hodín na každú nápravu), 1 hodina prevádzky, 1 hodina mimo prevádzky Dve skúšky popísané vyššie sa vykonajú na dvoch rôznych vzorkách skúšaného zariadenia.	
4.4	Ochrana proti vode a cudzím telesám	Overí sa, či stupeň ochrany jednotky vozidla namontovanej vo vozidle v prevádzkových podmienkach, je podľa IEC 529 aspoň IP 40	164, 165
4.5	Ochrana proti prepätiu	Overí sa, či jednotka vozidla odolá napájaciemu napätiu: verzie 24V: 34 V pri + 40 °C 1 hodina verzie 12V: 17 V pri + 40 °C 1 hodina	161
4.6	Ochrana proti zmene polarity	Overí sa, či jednotka vozidla môže odolať zmene polarity napájacieho napätia.	161
4.7	Ochrana proti skratu	Overí sa, či sú vstupné/výstupné signály chránené proti skratu napájania a uzemnenia	161

5.	*Skúšky EMC*		
5.1	Vyžarované emisie a citlivosť	Zhoda so smernicou 95/54/EHS	162
5.2	Elektrostatické výboje	Zhoda s IEC 61000–4–2, ±2 kV (úroveň 1)	162
5.3	Citlivosť na poruchy vede–ním na napája–cích vodičoch	Pre verzie 24V: zhoda s ISO 7637–2; impulz 1a: Vs = –100 V, Ri = 10 Ohm impulz 2: Vs = +100 V, Ri = 10 Ohm impulz 3a: Vs = –100 V, Ri = 50 Ohm impulz 3b: Vs = +100 V, Ri = 50 Ohm impulz 4: Vs = –16 V, Va = –12 V, t6 = 100 ms impulz 5: Vs = +120 V, Ri = 2,2 Ohm, td = 250 ms Pre verzie 12 V: zhoda s ISO 7637–1; impulz 1: Vs = –100 V, Ri = 10 Ohm impulz 2: Vs = +100 V, Ri = 10 Ohm impulz 3a: Vs = –100 V, Ri = 50 Ohm impulz 3b: Vs = +100 V, Ri = 50 Ohm impulz 4: Vs = –16 V, Va = –5 V, t6 = 15 ms impulz 5: Vs = +65 V, Ri = 3 Ohm, td = 100 ms Impulz 5 sa skúša len u jednotiek vozidiel určených na montáž vo vozidle, u ktorého sa nepredpokladá žiadna spoločná vonkajšia ochrana proti reaktančnej záťaži.	162

3. FUNKČNÉ SKÚŠKY SNÍMAČA POHYBU

Číslo	Skúška	Popis	Zodpovedajúce požiadavky
1.	**Administratívne preskúmanie**		
1.1	Dokumentácia	Správnosť dokumentácie	
2.	**Vizuálna kontrola**		
2.1	Zhoda s dokumentáciou		
2.2	Identifikácia/Označenie		169, 170
2.3	Materiály		163 až 167
2.4	Plombovanie		251
3.	**Funkčné skúšky**		
3.1	Identifikačné dáta snímača		077*
3.2	Snímač pohybu – spárovanie s jednotkou vozidla		099*, 155
3.3	Meranie pohybu		
	Presnosť merania pohybu		022 až 026

Číslo	Skúška	Popis	Zodpovedajúce požiadavky
4.	**Skúšky vplyvu vonkajšieho prostredia**		
4.1	Prevádzková teplota	Overenie funkčnosti (definované v skúške č. 3.3) v rozsahu teplôt [–40 °C; +135 °C] podľa: – IEC 68–2–1, skúška Ad, doba trvania 96 hodín pri najnižšej teplote To_{min} – IEC 68–2–2, skúška Bd, doba trvania 96 hodín pri najvyššej teplote To_{max}	159
4.2	Teplotné cykly	Overenie funkčnosti (definované v skúške č. 3.3) podľa IEC 68–2–14, skúška Na, 20 cyklov každý pri teplote meniacej sa od nižšej teploty (–40 °C) po vyššiu teplotu (+135 °C) a 2 hodiny zotrvania pri nižšej a vyššej teplote. Pri nižšej a vyššej teplote ako aj počas teplotných cyklov sa môže vykonať menší počet skúšok (u skúšok uvedených v bode 3.3).	159
4.3	Cykly vlhkosti	Overenie funkčnosti (definované v skúške č. 3.3) podľa IEC 68–2–30, skúška Db, šesť 24–hodinových cyklov vždy pri teplote meniacej sa od +25 °C do +55 °C a pri relatívnej vlhkosti 97% pri +25 °C a rovnej 93% pri +55 °C.	160
4.4	Vibrácie	Overenie funkčnosti (definované v skúške č. 3.3) podľa IEC 68–2–6, skúška Fc, trvanie skúšky 100 frekvenčných cyklov: konštantný posuv medzi 10 a 57 Hz: max. 1,5 mm konštantné zrýchlenie medzi 57 a 500 Hz: 20 g	163
4.5	Mechanický úder	Overenie funkčnosti (definované v skúške č. 3.3) podľa IEC 68–2–27, skúška Ea, 3 údery v oboch smeroch 3 kolmých osí	163
4.6	Ochrana proti vode a cudzím telesám	Overí sa, či stupeň ochrany snímača pohybu namontovaného vo vozidle v prevádzkových podmienkach, je podľa IEC 529 aspoň IP 64,	165
4.7	Ochrana proti zmene polarity	Overí sa, či snímač pohybu môže odolať zmene polarity napájacieho napätia.	161
4.8	Ochrana proti skratu	Overí sa, či sú vstupné/výstupné signály chránené proti skratu napájania a uzemnenia	161
5.	*EMC*		
5.1	Vyžarované emisie a citlivosť	Overí sa zhoda so smernicou 95/54/EHS	162
5.2	Elektrostatické výboje	Zhoda s IEC 61000–4–2, ±2 kV (úroveň 1)	162
5.3	Citlivosť na po–ruchy vedením na dátových vodičoch	Zhoda s ISO 7637–3 (úroveň III)	162

4. FUNKČNÉ SKÚŠKY TACHOGRAFOVÝCH KARIET

Číslo	Skúška	Popis	Zodpovedajúce požiadavky
1.	**Administratívne preskúmanie**		
1.1	Dokumentácia	Správnosť dokumentácie	
2.	**Vizuálna kontrola**		
2.1		Ubezpečenie, že všetky údaje na ochranu a viditeľné dáta sú správne vytlačené na karte a zodpovedajú požiadavkám	171 až 181
3.	*Fyzické skúšky*		
3.1		Kontrola rozmerov karty a polohy kontaktov	184 ISO/IEC 7816–1 ISO/IEC 7816–2
4.	*Skúšobné protokoly*		
4.1	ATR	Kontrola, či ATR zodpovedá požiadavkám	ISO/IEC 7816–3 TCS 304, 307, 308
4.2	T=0	Kontrola, či protokol T=0 zodpovedá požiadavkám	ISO/IEC 7816–3 TCS 302, 303, 305
4.3	PTS	Kontrola, či príkaz PTS je zhodný s nastavením T=1 z T=0	ISO/IEC 7816–3 TCS 309 až 311
4.4	T=1	Kontrola, či protokol T=1 zodpovedá požiadavkám	ISO/IEC 7816–3 TCS 303, / 306
5.	**Štruktúra karty**		
5.1		Skúša sa, či štruktúra dátových súborov karty zodpovedá požiadavkám. Na tento účel sa kontroluje prítomnosť povinných dátových súborov na karte a ich prístupové podmienky	TCS 312 TCS 400*, 401, 402, 403*, 404, 405*, 406, 407, 408*, 409, 410*, 411, 412, 413*, 414, 415*, 416, 417, 418*, 419
6.	**Funkčné skúšky**		
6.1	Normálne spracovanie	Skúša sa aspoň raz každé povolené použitie každého príkazu (napr. skúška príkazu UPDATE BINARY s CLA = ‘00’, CLA = ‘0C’ a s rôznymi parametrami P1, P2 a Lc). Kontrola, či sa skutočne vykonali činnosti na karte (napr. čítaním dátového súboru v ktorom sa vykonal príkaz)	TCS 313 až TCS 379
6.2	Chybová správa	Skúša sa aspoň raz každá chybová správa (podľa doplnku 2) pre každý príkaz. Skúša sa aspoň raz každá generická chyba (okrem ‘6400’ chýb integrity kontrolovaných počas bezpečnostnej certifikácie)	
7.	**Skúšky vplyvu vonkajšieho prostredia**		
7.1		Ubezpečenie, že karty pracujú v rámci limitných	185 až 188

Číslo	Skúška	Popis	Zodpovedajúce požiadavky
		podmienok definovaných v súlade s ISO/IEC 10373	ISO/IEC 7816–1

5. SKÚŠKY INTEROPERABILITY

Číslo	Skúška	Popis
1.	Vzájomné overovanie	Kontrola, či vzájomné overovanie medzi jednotkou vozidla a tachografovou kartou prebieha normálne.
2.1	Skúšky písania/čítania	Vykonanie typického scenára činnosti na jednotke vozidla. Scenár sa prispôsobí typu skúšanej karty a bude obsahovať čo možno najviac zápisov udalostí a porúch. Pomocou sťahovania z karty sa overí, či boli všetky zodpovedajúce záznamy urobené správne. Pomocou dennej tlače karty sa overí, či sa môžu správne čítať všetky zodpovedajúce záznamy.

Doplnok 10

VŠEOBECNÉ BEZPEČNOSTNÉ POŽIADAVKY

Tento doplnok špecifikuje minimálne požadovaný obsah snímača pohybu, jednotky vozidla a bezpečnostných cieľov tachografovej karty.

Na formulovanie bezpečnostných cieľov, ktoré musia byť splnené pri bezpečnostnej certifikácii, musia výrobcovia podľa potreby konkretizovať a doplniť dokumenty bez toho, aby menili alebo vymazali existujúce bezpečnostné riziká, ciele, postupové možnosti a bezpečnostné vynucovacie funkcie.

OBSAH

Všeobecné bezpečnostné požiadavky na snímač pohybu

4.6.1 Skúšky
4.6.2 Software
4.6.3 Fyzická ochrana
4.6.4 Prerušenie napájania
4.6.5 Podmienky resetovania
4.6.6 Dostupnosť dát
4.6.7 Viacnásobné aplikácie
4.7 Výmena dát
4.8 Kryptografická podpora
5. Definícia bezpečnostných mechanizmov
6. Minimálna odolnosť bezpečnostných mechanizmov
7. Úroveň ručenia
8. Základný princíp

Všeobecné bezpečnostné požiadavky na jednotku vozidla

1. Úvod
2. Skratky, definície a referenčné dokumenty
2.1 Skratky
2.2 Definície
2.3 Referenčné dokumenty
3. Základný princíp produktu
3.1 Popis jednotky vozidla a spôsob používania
3.2 Cyklus životnosti jednotky vozidla
3.3 Bezpečnostné riziká
3.3.1 Bezpečnostné riziká súvisiace s identifikáciou a kontrolou prístupu
3.3.2 Bezpečnostné riziká súvisiace s konštrukciou
3.3.3 Bezpečnostné riziká súvisiace s prevádzkou
3.4 Bezpečnostné ciele
3.5 Informačno–technické bezpečnostné ciele
3.6 Fyzické, personálne alebo postupové prostriedky
3.6.1 Konštrukcia zariadenia
3.6.2 Dodávka zariadenia a aktivácia
3.6.3 Generovanie a dodávka bezpečnostných dát
3.6.4 Dodávka kariet
3.6.5 Inštalovanie záznamového zariadenia, kalibrácia a kontrola
3.6.6 Prevádzka zariadenia
3.6.7 Kontrola dodržiavania predpisov
3.6.8 Modernizácia softwaru
4. Bezpečnostné vynucovacie funkcie
4.1 Identifikácia a autentifikácia
4.1.1 Identifikácia snímača pohybu a autentifikácia
4.1.2 Identifikácia a autentifikácia užívateľa
4.1.3 Identifikácia a autentifikácia diaľkovo pripojeného podniku
4.1.4 Identifikácia a autentifikácia riadiaceho zariadenia
4.2 Kontrola prístupu
4.2.1 Oprávnenie na prístup

4.2.2 Prístupové práva k funkciám
4.2.3 Prístupové práva k dátam
4.2.4 Štruktúra súboru a prístupové podmienky
4.3 Sledovateľnosť
4.4 Audit
4.5 Opätovné použitie pamäťového média
4.6 Presnosť
4.6.1 Opatrenia na kontrolu informačných tokov
4.6.2 Vnútorné prenosy dát
4.6.3 Integrita uložených dát
4.7 Spoľahlivosť služby
4.7.1 Skúšky
4.7.2 Software
4.7.3 Fyzická ochrana
4.7.4 Prerušenie napájania
4.7.5 Podmienky resetovania
4.7.6 Dostupnosť dát
4.7.7 Viacnásobné aplikácie
4.8 Výmena dát
4.8.1 Výmena dát so snímačom pohybu
4.8.2 Výmena dát s tachografovými kartami
4.8.3 Výmena dát s vonkajším pamäťovým médiom (funkcia sťahovania dát)
4.9 Kryptografická podpora
5. Definícia bezpečnostných mechanizmov
6. Minimálna odolnosť bezpečnostných mechanizmov
7. Úroveň ručenia
8. Základný princíp

Všeobecné bezpečnostné požiadavky na tachografovú kartu

1. Úvod
2. Skratky, definície a referenčné dokumenty
2.1 Skratky
2.2 Definície
2.3 Referenčné dokumenty
3. Základný princíp produktu
3.1 Popis tachografovej karty a spôsob používania
3.2 Cyklus životnosti tachografovej karty
3.3 Bezpečnostné riziká
3.3.1 Konečné ciele
3.3.2 Cesty útoku
3.4 Bezpečnostné ciele
3.5 Informačno–technické bezpečnostné ciele
3.6 Fyzické, personálne alebo postupové prostriedky
4. Bezpečnostné vynucovacie funkcie
4.1 Dodržanie ochranných profilov
4.2 Identifikácia a autentifikácia užívateľa

4.2.1 Identifikácia užívateľa
4.2.2 Autentifikácia užívateľa
4.2.3 Chybná autentifikácia
4.3 Kontrola prístupu
4.3.1 Opatrenia na kontrolu prístupu
4.3.2 Funkcie kontroly prístupu
4.4 Sledovateľnosť
4.5 Audit
4.6 Presnosť
4.6.1 Integrita uložených dát
4.6.2 Autentifikácia základných dát
4.7 Spoľahlivosť služby
4.7.1 Skúšky
4.7.2 Software
4.7.3 Napájanie
4.7.4 Podmienky resetovania
4.8 Výmena dát
4.8.1 Výmena dát s jednotkou vozidla
4.8.2 Export dát na mimovozidlovú jednotku (funkcia sťahovania dát)
5. Definícia bezpečnostných mechanizmov
6. Minimálna odolnosť bezpečnostných mechanizmov
7. Úroveň ručenia
8. Základný princíp

VŠEOBECNÉ BEZPEČNOSTNÉ POŽIADAVKY NA SNÍMAČ POHYBU

1. **Úvod**

Tento dokument obsahuje popis snímača pohybu, riziká, ktorým musí čeliť a bezpečnostné ciele, ktoré musí spĺňať. Špecifikuje požadované bezpečnostné vynucovacie funkcie. Stanovuje požadovanú minimálnu odolnosť bezpečnostných mechanizmov a požadovanú úroveň ručenia za vývoj a hodnotenie.

Požiadavky uvedené v dokumente zodpovedajú požiadavkám hlavnej časti prílohy I B. V záujme lepšej zrozumiteľnosti, sa niekedy vyskytujú duplicity medzi požiadavkami hlavnej časti prílohy I B a bezpečnostnými požiadavkami. V prípade rozporu medzi bezpečnostnými požiadavkami a požiadavkami hlavnej časti prílohy I B, na ktoré sa odvolávajú tieto bezpečnostné požiadavky, platia požiadavky hlavnej časti prílohy I B.

Požiadavky hlavnej časti prílohy I B, na ktoré sa neodvolávajú bezpečnostné požiadavky nie sú predmetom bezpečnostných vynucovacích funkcií (SEF).

Za účelom lepšej sledovateľnosti pojmov použitých v dokumentácii o vývoji a hodnotení, boli možným rizikám, cieľom, postupovým prostriedkom a špecifikáciám SEF priradené jednoznačné označenia.

2. **Skratky, definície a referenčné dokumenty**

2.1 ***Skratky***

ROM	Read Memory Only (permanentná pamäť)
SEF	Security enforcing function (Bezpečnostná vynucovacia funkcia)
TBD	To be defined (Je potrebné definovať)
TOE	Target of evaluation (Objekt hodnotenia)
JV	Jednotka vozidla

2.2 ***Definície***

Digitálny tachograf	Záznamové zariadenie
Prístrojová jednotka	Zariadenie pripojené k snímaču pohybu
Pohybové dáta	Dáta o rýchlosti a ubehnutej vzdialenosti vymieňané s JV
Fyzicky oddelené časti	Fyzické komponenty snímača pohybu, ktoré sú na rozdiel od fyzických komponentov uzavretých v puzdre snímača, rozmiestnené vo vozidle
Bezpečnostné dáta	Špecifické dáta potrebné na podporu bezpečnostných vynucovacích funkcií (napr. kryptografický kľúč)
Systém	Vybavenie, ľudia alebo organizácie vzťahujúce sa akýmkoľvek spôsobom k záznamovému zariadeniu
Užívateľ	Osoba používajúca snímač pohybu (keď sa nepoužije vo výraze „užívateľské dáta“)
Užívateľské dáta	Každé dáta, okrem pohybových alebo bezpečnostných dát, zaznamenané alebo uložené snímačom pohybu.

2.3 ***Referenčné dokumenty***

ITSEC ITSEC Information Technology Security Evaluation Criteria 1991 (Kritériá hodnotenia bezpečnosti informačnej techniky)

3. **Základný princíp produktu**

3.1 ***Popis snímača pohybu a spôsob používania***

Snímač pohybu je určený na inštalovanie v cestných dopravných vozidlách. Jeho účelom je poskytovať JV pohybové dáta predstavujúce rýchlosť vozidla a ubehnutú vzdialenosť.

Snímač pohybu je mechanicky prepojený s pohybovou časťou vozidla, ktorého pohyb môže byť vyjadrený rýchlosťou vozidla alebo ubehnutou vzdialenosťou. Môže byť umiestnený v prevodovke vozidla alebo v ktorejkoľvek inej časti vozidla.

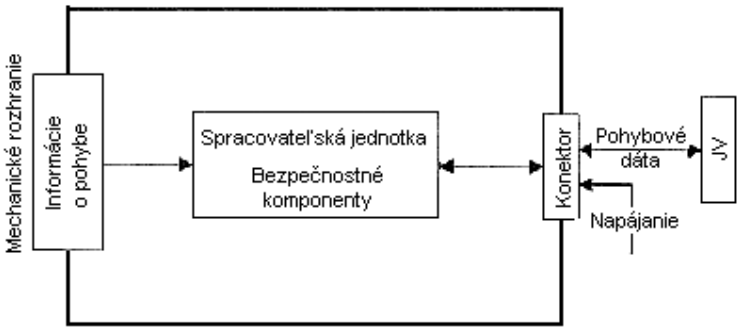
V prevádzkovom režime je snímač pohybu spojený s JV.

Na riadiace účely tiež môže byť spojený so špecifickým zariadením (TBD určí výrobca).

Typický snímač pohybu je popísaný na nasledovnom obrázku:

Obrázok 1

Typický snímač pohybu

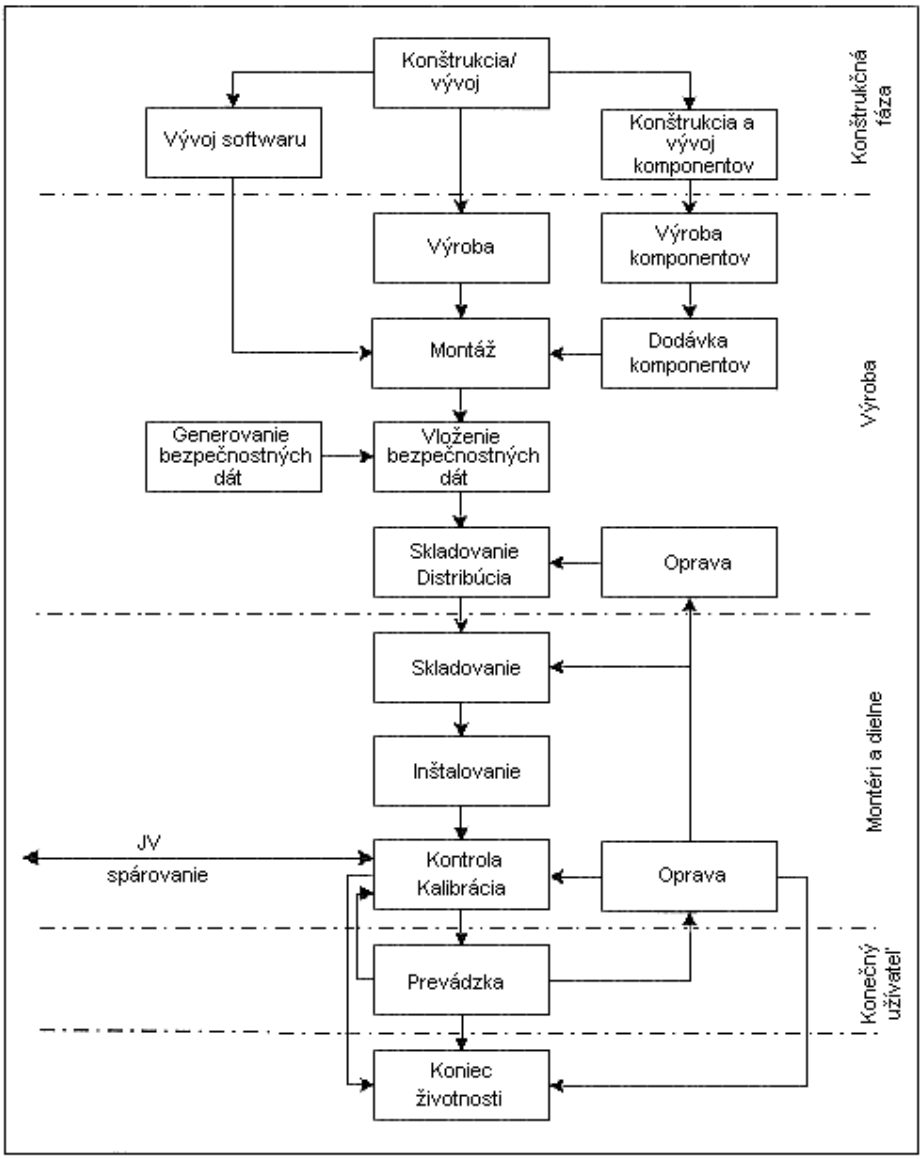


3.2 ***Cyklus životnosti snímača pohybu***

Typický cyklus životnosti snímača pohybu je popísaný na nasledovnom obrázku:

Obrázok 2

Typický cyklus životnosti snímača pohybu



3.3 ***Bezpečnostné riziká***

Tento odsek popisuje možné bezpečnostné riziká pre snímač pohybu.

3.3.1 *Bezpečnostné riziká súvisiace s kontrolou prístupu*

T.Access Užívatelia by sa mohli pokúsiť o prístup k funkciám, ktoré nemajú povolené.

3.3.2 *Bezpečnostné riziká súvisiace s konštrukciou*

T.Faults	Poruchy v hardware, software alebo komunikačnom postupe by mohli dostať snímač pohybu do nepredvídaných situácií ohrozujúcich jeho bezpečnosť
T.Tests	Použitie neplatných skúšobných režimov alebo prípadných existujúcich „zadných dvierok“ by mohli ohroziť bezpečnosť JV
T.Design	Užívatelia by sa mohli pokúsiť o nelegálne získanie znalostí o konštrukcii z materiálov výrobcu (krádežou, podplácaním, ...) alebo metódou „reverse engineering“.

3.3.3 *Bezpečnostné riziká súvisiace s prevádzkou*

T.Environment	Užívatelia by mohli ohroziť bezpečnosť snímača pohybu zásahmi zvonku (tepelnými, elektromagnetickými, optickými, chemickými, mechanickými, ...)
T.Hardware	Užívatelia by sa mohli pokúsiť o zmenu hardwaru snímača pohybu
T.Mechanical_Origin	Užívatelia by sa mohli pokúsiť o manipuláciu so vstupmi snímača pohybu (napr. odstránením z prevodovky)
T.Motion_Data	Užívatelia by sa mohli pokúsiť o zmenu pohybových dát vozidla (doplnenie, zmena, vypustenie, opakovanie signálu)
T.Power_Supply	Užívatelia by sa mohli pokúsiť o anulovanie bezpečnostných cieľov snímača pohybu pomocou manipulácie s dodávkou prúdu (prerušenie, zníženie, zvýšenie)
T.Security_Data	Užívatelia by sa mohli pokúsiť o nelegálne získanie znalostí o bezpečnostných dátach počas generovania bezpečnostných dát alebo počas prenosu alebo ukladania v zariadení
T.Software	Užívatelia by sa mohli pokúsiť o zmenu softwaru snímača pohybu
T.Stored_Data	Užívatelia by sa mohli pokúsiť o zmenu uložených dát (bezpečnostných alebo užívateľských dát).

3.4 ***Bezpečnostné ciele***

Hlavným bezpečnostným cieľom systému digitálneho tachografu je toto:

O.Main	Dáta kontrolované kontrolnými orgánmi musia byť dostupné a musia plne a presne odrážať činnosti kontrolovaných vodičov a vozidiel v čase vedenia vozidla, práce, pohotovosti a odpočinku ako aj rýchlosť vozidla.

Preto je bezpečnostným cieľom snímača pohybu, ktorým prispieva k hlavnému bezpečnostnému cieľu, nasledovné:

O.Sensor_Main	Dáta prenášané snímačom pohybu musia byť pre JV dostupné tak, aby umožňovali JV určiť úplne a presne pohyb vozidla z hľadiska rýchlosti a ubehnutej vzdialenosti.

3.5 ***Informačno–technické bezpečnostné ciele***

Špecifické informačno–technické bezpečnostné ciele snímača pohybu, ktorými prispieva k hlavnému bezpečnostnému cieľu, sú tieto:

O.Access	Snímač pohybu musí riadiť prístup pripojených prístrojových jednotiek k funkciám a dátam
O.Audit	Snímač pohybu musí preverovať pokusy o narušenie bezpečnosti a mal by ich sledovať vo vzťahu k pripojeným prístrojovým jednotkám
O.Authentication	Snímač pohybu musí autentifikovať pripojené prístrojové jednotky

O.Processing	Snímač pohybu musí zabezpečiť presné spracovanie vstupných dát, z ktorých sa odvodia pohybové dáta
O.Reliability	Snímač pohybu musí poskytovať spoľahlivé služby
O.Secured_Data_Exchange	Snímač pohybu musí zabezpečiť výmeny bezpečnostných dát s JV.

3.6 ***Fyzické, personálne alebo postupové prostriedky***

Tento odsek popisuje fyzické, personálne alebo postupové požiadavky, ktoré prispievajú k bezpečnosti snímača pohybu.

3.6.1 *Konštrukcia zariadenia*

M.Development	Vývojoví pracovníci snímača pohybu musia zabezpečiť, aby sa priradenie zodpovednosti počas vývoja vykonávalo spôsobom, ktorý zachová IT bezpečnosť
M.Manufacturing	Výrobcovia snímača pohybu musia zabezpečiť, aby sa priradenie zodpovednosti počas výroby vykonávalo spôsobom, ktorý zachová IT bezpečnosť a aby počas výrobného procesu bol snímač pohybu chránený proti fyzickým zásahom, ktoré by mohli ohroziť IT bezpečnosť.

3.6.2 *Dodávka zariadenia*

M.Delivery	Výrobcovia snímača pohybu, výrobcovia vozidla a montéri alebo dielne musia zabezpečiť, aby sa so snímačom pohybu zaobchádzalo tak, aby sa zachovala IT bezpečnosť.

3.6.3 *Generovanie a dodávka bezpečnostných dát*

M.Sec_Data_Generation	Algoritmy generovania bezpečnostných dát musia byť prístupné len oprávneným a dôveryhodným osobám
M.Sec_Data_Transport	Bezpečnostné dáta musia byť generované, prenášané a vkladané do snímača pohybu tak, aby sa zachovala ich primeraná dôvernosť a integrita.

3.6.4 *Inštalovanie záznamového zariadenia, kalibrácia a kontrola*

M.Approved_Workshops	Inštalovanie, kalibráciu a opravu záznamového zariadenia musia vykonávať dôveryhodní a schválení montéri alebo dielne
M.Mechanical_Interface	Musia sa zabezpečiť prostriedky zisťovania neoprávnených fyzických zásahov do mechanického rozhrania (napr. plomby)
M.Regular_Inspections	Záznamové zariadenie sa musí pravidelne kontrolovať a kalibrovať.

3.6.5 *Kontrola dodržiavania predpisov*

M.Controls	Kontrola dodržiavania predpisov sa musí vykonávať pravidelne a metódou námatkovej skúšky a musí zahŕňať bezpečnostné audity.

3.6.6 *Modernizácia softwaru*

M.Software_Upgrade	Revíziám softwaru musí byť udelená bezpečnostná certifikácia predtým, než sa môžu zaviesť do snímača pohybu.

4. **Bezpečnostné vynucovacie funkcie**

4.1 ***Identifikácia a autentifikácia***

UIA_101 Snímač pohybu musí byť pre každú interakciu schopný stanoviť identitu ktorejkoľvek k nemu pripojenej prístrojovej jednotky.

UIA_102 Identita pripojenej prístrojovej jednotky sa skladá zo:

- skupiny prístrojových jednotiek:
  - JV,
  - riadiace zariadenie,
  - iné prístrojové jednotky,
- identifikácie jednotky (len JV).

UIA_103 Identita prístrojovej jednotky pripojenej JV pozostáva zo schvaľovacieho čísla JV a sériového čísla JV.

UIA_104 Snímač pohybu musí byť schopný autentifikovať každú JV alebo riadiace zariadenie, s ktorým je spojený:

- pri pripojení prístrojovej jednotky,
- pri obnovení napájania.

UIA_105 Snímač pohybu musí byť schopný pravidelne opakovane autentifikovať JV, ku ktorej je pripojený.

UIA_106 Snímač pohybu musí zistiť a zabrániť použitiu autentifikovaných dát, ktoré boli kopírované alebo prehrávané.

UIA_107 Po zistení určitého počtu (určí výrobca a nesmie prekročiť počet 20) po sebe idúcich neúspešných pokusov o autentifikáciu, SEF:

- generuje auditný záznam udalosti,
- varuje prístrojovú jednotku,
- pokračuje v exporte pohybových dát v nezabezpečenom režime.

4.2 ***Kontrola prístupu***

Kontroly prístupu zabezpečujú, aby čítanie, vytváranie a zmeny informácií v TOE vykonávali len k tomu oprávnené osoby.

4.2.1 *Oprávnenie na prístup*

ACC_101 Snímač pohybu musí kontrolovať práva na prístup k funkciám a dátam.

4.2.2 *Prístupové práva k dátam*

ACC_102 Snímač pohybu musí zabezpečiť, aby sa identifikačné dáta snímača pohybu mohli písať len raz (požiadavka 078).

ACC_103 Snímač pohybu musí prijať a/alebo uložiť užívateľské dáta len z autentifikovaných prístrojových jednotiek.

ACC_104 Snímač pohybu si musí vynútiť primerané prístupové práva na čítanie a písanie bezpečnostných dát.

4.2.3 *Štruktúra súboru a prístupové podmienky*

ACC_105 Štruktúra aplikačných a dátových súborov a prístupové podmienky sa vytvoria už počas výrobného procesu a potom sa zablokujú proti akejkoľvek budúcej zmene alebo vymazaniu.

4.3 ***Sledovateľnosť***

ACT_101 Snímač pohybu musí vo svojej pamäti uchovávať svoje identifikačné dáta (požiadavka 077).

ACT_102 Snímač pohybu musí vo svojej pamäti uchovávať inštalačné dáta (požiadavka 099).

ACT_103 Snímač pohybu musí byť na požiadanie autentifikovaných prístrojových jednotiek schopný poskytnúť priraďovacie dáta.

4.4 ***Audit***

AUD_101 Snímač pohybu musí pri udalostiach poškodzujúcich jeho bezpečnosť, generovať auditné záznamy o udalostiach.

AUD_102 Udalosti, ktoré majú vplyv na bezpečnosť snímača pohybu sú tieto:

- pokusy o narušenie bezpečnosti,
  - chybná autentifikácia,
  - chyba integrácie uložených dát,
  - vnútorná chyba prenosu dát,
  - neoprávnené otvorenie puzdra,
  - manipulácia s hardwarom,
- porucha snímača.

AUD_103 Auditné záznamy obsahujú tieto dáta:

- dátum a čas udalosti,
- typ udalosti,
- identita pripojenej prístrojovej jednotky.

Keď nie sú požadované dáta k dispozícii, uvedie sa príslušný štandardný údaj (určí výrobca).

AUD_104 Snímač pohybu odošle generované auditné dáta na JV v okamihu ich generovania a môže ich uložiť aj vo svojej pamäti.

AUD_105 V prípade, keď snímač ukladá auditné dáta zabezpečí, aby sa 20 auditných záznamov uchovávalo nezávisle na vyčerpaní auditnej pamäte a musí byť schopný na požiadanie autentifikovanej prístrojovej jednotky, poskytnúť uložené auditné záznamy.

4.5 **Presnosť**

4.5.1 *Opatrenia na kontrolu informačných tokov*

ACR_101 Snímač pohybu musí zabezpečiť, aby sa pohybové dáta mohli spracovávať a odvodzovať len z mechanického vstupu snímača.

4.5.2 *Vnútorné prenosy dát*

Požiadavky tohto odseku platia len vtedy, keď snímač pohybu využíva fyzicky oddelené časti.

ACR_102 Ak sú dáta prenášané medzi fyzicky oddelenými časťami snímača pohybu, dáta sa musia chrániť pred zmenou.

ACR_103 Po zistení chyby v prenose dát počas vnútorného prenosu, prenos sa opakuje a SEF generuje auditný záznam o udalosti.

4.5.3 *Integrita uložených dát*

ACR_104 Snímač pohybu musí kontrolovať užívateľské dáta uložené vo svojej pamäti z hľadiska chýb integrity.

ACR_105 Po zistení chyby integrity uložených dát, SEF generuje auditný záznam.

4.6 **Spoľahlivosť služby**

4.6.1 *Skúšky*

RLB_101 Všetky príkazy, činnosti alebo skúšobné body špecifické pre skúšobné potreby výrobnej fázy sa pred skončením výrobnej fázy deaktivujú alebo odstránia.

RLB_102 Snímač pohybu vykoná samoskúšky pri prvom zapnutí a počas normálnej prevádzky, aby sa overila jeho správna činnosť. Samoskúšky snímača pohybu zahŕňajú overenie integrity bezpečnostných dát a overenie integrity uloženého vykonávacieho kódu (ak nie je v ROM).

RLB_103 Po zistení vnútornej chyby počas samoskúšky, SEF generuje auditný záznam (chyba senzora).

4.6.2 *Software*

RLB_104 Nesmie existovať možnosť analyzovať alebo ladiť software snímača pri praktickom používaní.

RLB_105 Vstupy z vonkajších zdrojov nesmú byť akceptované ako vykonávací kód.

4.6.3 *Fyzická ochrana*

RLB_106 Ak je snímač pohybu konštruovaný tak, aby sa mohol otvoriť, snímač pohybu musí zistiť každé otvorenie puzdra dokonca aj bez vonkajšieho napájania minimálne po dobu šiestich mesiacov. V takom prípade SEF generuje auditný záznam o udalosti (pripúšťa sa, aby sa auditný záznam generoval a uložil po obnovení napájania).

Ak je snímač pohybu konštruovaný tak, že sa nemôže otvoriť, každý pokus o neoprávnené zásahy sa musí dať ľahko zistiť (napr. vizuálnou kontrolou).

RLB_107 Snímač pohybu musí zistiť určitú (určí výrobca) manipuláciu s hardwarom.

RLB_108 V prípade popísanom vyššie, SEF generuje auditný záznam a snímač pohybu: (určí výrobca).

4.6.4 *Prerušenie napájania*

RLB_109 Snímač pohybu musí zachovávať bezpečnostný stav počas prerušenia alebo zmien napájania.

4.6.5 *Podmienky resetovania*

RLB_110 V prípade prerušenia napájania alebo ak sa prenos zastaví pred dokončením, alebo pri ktorejkoľvek inej podmienke resetovania, sa snímač pohybu musí resetovať.

4.6.6 *Dostupnosť dát*

RLB_111 Snímač pohybu musí zabezpečiť, aby bol na požiadanie možný prístup k zdrojom a aby sa dáta ani zbytočne nevyžadovali ani neuchovávali.

4.6.7 *Viacnásobné aplikácie*

RLB_112 Ak snímač pohybu ponúka aplikácie iné než je tachografová aplikácia, všetky aplikácie musia byť fyzicky a/alebo logicky navzájom oddelené. Tieto aplikácie nesmú mať zdieľané bezpečnostné dáta. Môže byť aktívna vždy len jedna funkcia.

4.7 **Výmena dát**

DEX_101 Snímač pohybu musí exportovať pohybové dáta na JV s príslušnými bezpečnostnými atribútmi tak, aby JV mohla overiť ich integritu a autenticitu.

4.8 **Kryptografická podpora**

Požiadavky tohto odseku sú aplikovateľné len pokiaľ sú potrebné, závisiac na použitom bezpečnostnom mechanizme a na riešeniach výrobcu.

CSP_101 Každá kryptografická operácia vykonávaná snímačom pohybu musí byť v súlade so špecifikovanými algoritmami a špecifikovanou veľkosťou kľúča.

CSP_102 Ak snímač pohybu generuje kryptografické kľúče, musí to byť v súlade so špecifikovanými algoritmami generovania kryptografických kľúčov a špecifikovanými veľkosťami kryptografických kľúčov.

CSP_103 Ak snímač pohybu distribuuje kryptografické kľúče, musí to byť v súlade so špecifikovanými metódami distribúcie kľúča.

CSP_104 Ak snímač pohybu sprístupňuje kryptografické kľúče, musí to byť v súlade so špecifikovanými metódami prístupu ku kryptografickým kľúčom.

CSP_105 Ak snímač pohybu zničí kryptografické kľúče, musí to byť v súlade so špecifikovanými metódami zničenia kryptografických kľúčov.

5. **Definícia bezpečnostných mechanizmov**

Bezpečnostné mechanizmy plniace bezpečnostné vynucovacie funkcie snímača pohybu, sú definované výrobcami snímača pohybu.

6. **Minimálna odolnosť bezpečnostných mechanizmov**

Minimálna odolnosť bezpečnostných mechanizmov snímača pohybu je „Vysoká“, podľa definície v ITSEC.

7. **Úroveň ručenia**

Cieľová úroveň ručenia pre snímač pohybu je ITSEC úroveň E3, podľa definície v ITSEC.

.

8. **Základný princíp**

Základný princíp SEF je založený na nasledovných maticiach, ktoré udávajú:

– ktoré SEF alebo prostriedky sú vystavené ktorým bezpečnostným rizikám,

– ktoré SEF spĺňajú ktoré IT bezpečnostné ciele.

	Bezpečnostné riziká												IT ciele					
	Prístup	Chyby	Skúšky	Konštrukcia	Prostredie	Hardware	Mechanický pôvod	Pohybové dáta	Napájanie	Bezpečnostné dáta	Software	Uložené dáta	Prístup	Audit	Autentifikácia	Spracovanie	Spoľahlivosť	Výmena bezpečn. dát
Fyzické, personálne, postupové prostriedky																		
Vývoj		x	x	x														
Výroba			x	x														
Dodávka						x					x	x						
Generovanie bezpečnostných dát										x								
Prenos bezpečnostných dát										x								
Schválené dielne							x											
Mechanické rozhranie							x											
Pravidelná kontrola						x	x		x		x							
Kontroly dodržiavania predpisov					x	x	x		x	x	x							
Modernizácia softwaru											x							

	Bezpečnostné riziká												IT ciele					
	Prístup	Chyby	Skúšky	Konštrukcia	Prostredie	Hardware	Mechanický pôvod	Pohybové dáta	Napájanie	Bezpečnostné dáta	Software	Uložené dáta	Prístup	Audit	Autentifikácia	Spracovanie	Spoľahlivosť	Výmena bezpečn. dát
Bezpečnostné vynucovacie funkcie																		
Identifikácia a autentifikácia																		
UIA_101 Identifikácia prístrojových jednotiek	x							x					x		x			x
UIA_102 Identita prístrojových jednotiek	x												x		x			
UIA_103 Identita JV														x				
UIA_104 Autentifikácia prístrojových jednotiek	x							x					x		x			x
UIA_105 Opakovaná autentifikácia	x							x					x		x			x
UIA_106 Autentifikácia zabezpečená proti falšovaniu	x							x					x		x			
UIA_107 Neúspešná autentifikácia								x						x			x	
Kontrola prístupu																		
ACC_101 Pravidla prístupovej kontroly	x									x		x	x					
ACC_102 Identifikácia snímača pohybu												x	x					
ACC_103 Užívateľské dáta												x	x					
ACC_104 Bezpečnostné dáta										x		x	x					
ACC_105 Štruktúra súboru a prístupové podmienky	x									x		x	x					

	Bezpečnostné riziká												IT ciele					
	Prístup	Chyby	Skúšky	Konštrukcia	Prostredie	Hardware	Mechanický pôvod	Pohybové dáta	Napájanie	Bezpečnostné dáta	Software	Uložené dáta	Prístup	Audit	Autentifikácia	Spracovanie	Spoľahlivosť	Výmena bezpečn. dát
Sledovateľnosť																		
ACT_101 Identifikačné dáta snímača pohybu														x				
ACT_102 Dáta o spárovaní														x				
ACT_103 Priraďovacie dáta														x				
Audit																		
AUD_101 Auditné záznamy														x				
AUD_102 Zoznam auditných udalostí	x				x	x						x		x				
AUD_103 Auditné dáta														x				
AUD_104 Auditné nástroje														x				
AUD_105 Uloženie auditných záznamov v pamäti														x				
Presnosť																		
ACR_101 Opatrenia na kontrolu informačných tokov								x								x	x	
ACR_102 Vnútorné prenosy dát																x	x	
ACR_103 Vnútorné prenosy dát														x				
ACR_104 Integrita uložených dát												x					x	
ACR_105 Integrita uložených dát												x		x				

	Bezpečnostné riziká												IT ciele					
	Prístup	Chyby	Skúšky	Konštrukcia	Prostredie	Hardware	Mechanický pôvod	Pohybové dáta	Napájanie	Bezpečnostné dáta	Software	Uložené dáta	Prístup	Audit	Autentifikácia	Spracovanie	Spoľahlivosť	Výmena bezpečn. dát
Spoľahlivosť																		
RLB_101 Výrobné skúšky			x	x													x	
RLB_102 Samoskúšky		x				x			x		x						x	
RLB_103 Samoskúšky						x			x		x			x				
RLB_104 Analýza softwaru				x							x						x	
RLB_105 Softwarové vstupy											x					x	x	
RLB_106 Otvorenie puzdra				x	x	x				x	x	x					x	
RLB_107 Manipulácia s hardwarom						x											x	
RLB_108 Manipulácia s hardwarom						x								x				
RLB_109 Prerušenie napájania									x								x	
RLB_110 Resetovanie		x															x	
RLB_111 Dostupnosť dát																x	x	
RLB_112 Viacnásobné aplikácie																	x	
Výmena dát																		
Dex_101 Bezpečný export pohybových dát								x										x

	Bezpečnostné riziká												IT ciele					
	Prístup	Chyby	Skúšky	Konštrukcia	Prostredie	Hardware	Mechanický pôvod	Pohybové dáta	Napájanie	Bezpečnostné dáta	Software	Uložené dáta	Prístup	Audit	Autentifikácia	Spracovanie	Spoľahlivosť	Výmena bezpečn. dát
Kryptografická podpora																		
CSP_101 Algoritmy																	x	x
CSP_102 Generovanie kľúča																	x	x
CSP_103 Distribúcia kľúča																	x	x
CSP_104 Prístup ku kľúču																	x	x
CSP_105 Zničenie kľúča																	x	x

VŠEOBECNÉ BEZPEČNOSTNÉ POŽIADAVKY NA JEDNOTKU VOZIDLA

1. **Úvod**

Tento dokument obsahuje popis jednotky vozidla, riziká, ktorým musí čeliť a bezpečnostné ciele, ktoré musí spĺňať. Špecifikuje požadované bezpečnostné vynucovacie funkcie. Stanovuje požadovanú minimálnu odolnosť bezpečnostných mechanizmov a požadovanú úroveň ručenia za vývoj a hodnotenie.

Požiadavky uvedené v dokumente zodpovedajú požiadavkám hlavnej časti prílohy I B. V záujme lepšej zrozumiteľnosti, sa niekedy vyskytujú duplicity medzi požiadavkami hlavnej časti prílohy I B a bezpečnostnými požiadavkami. V prípade rozporu medzi bezpečnostnými požiadavkami a požiadavkami hlavnej časti prílohy I B, na ktoré sa odvolávajú tieto bezpečnostné požiadavky, platia požiadavky hlavnej časti prílohy I B.

Požiadavky hlavnej časti prílohy I B, na ktoré sa neodvolávajú bezpečnostné požiadavky nie sú predmetom bezpečnostných vynucovacích funkcií.

Za účelom lepšej sledovateľnosti pojmov použitých v dokumentácii o vývoji a hodnotení, boli možným rizikám, cieľom, postupovým prostriedkom a špecifikáciám SEF priradené jednoznačné označenia.

2. **Skratky, definície a referenčné dokumenty**

2.1 ***Skratky***

PIN	Personal identification number (Osobné identifikačné číslo)
ROM	Read Memory Only (permanentná pamäť)
SEF	Security enforcing function (Bezpečnostná vynucovacia funkcia)
TOE	Target of evaluation (Objekt hodnotenia)
JV	Jednotka vozidla

2.2 ***Definície***

Digitálny tachograf	Záznamové zariadenie
Pohybové dáta	Dáta o rýchlosti a ubehnutej vzdialenosti vymieňané so snímačom pohybu
Fyzicky oddelené časti	Fyzické komponenty JV, ktoré sú na rozdiel od fyzických komponentov uzavretých v puzdre JV, rozmiestnené vo vozidle
Bezpečnostné dáta	Špecifické dáta potrebné na podporu bezpečnostných vynucovacích funkcií (napr. kryptografické kľúče)
Systém	Vybavenie, ľudia alebo organizácie vzťahujúce sa akýmkoľvek spôsobom k záznamovému zariadeniu
Užívateľ	Ako užívatelia sa rozumejú osoby používajúce zariadenie. Normálni užívatelia JV zahŕňajú vodičov, kontrolórov, dielne a podniky
Užívateľské dáta	Každé dáta, okrem bezpečnostných dát, zaznamenané alebo uložené JV, požadované podľa kapitoly III.12.

2.3 ***Referenčné dokumenty***

ITSEC ITSEC Information Technology Security Evaluation Criteria 1991 (Kritériá hodnotenia bezpečnosti informačnej techniky)

3. **Základný princíp produktu**

3.1 ***Popis jednotky vozidla a spôsob používania***

Jednotka vozidla je určená na inštalovanie v cestných dopravných vozidlách. Jej účelom je zaznamenávať, skladovať, zobrazovať a tlačiť a vypisovať dáta vzťahujúce sa k činnostiam vodiča.

Je prepojená so snímačom pohybu, s ktorým si vymieňa dáta o pohybe vozidla.

Užívatelia sa voči JV identifikujú s pomocou tachografových kariet.

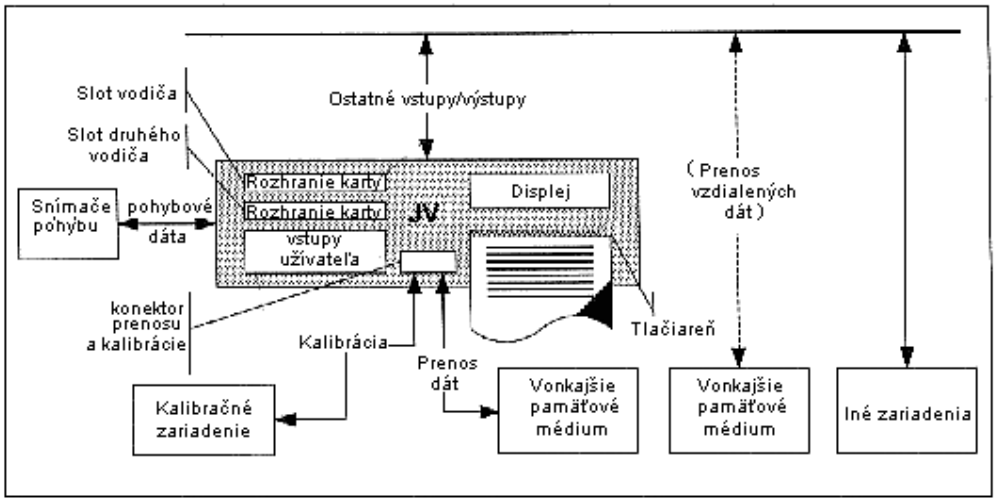
JV zaznamenáva a ukladá vo svojej dátovej pamäti dáta o činnostiach užívateľov a zaznamenáva ich aj na tachografových kartách.

JV poskytuje dáta pre displej, tlačiareň a vonkajšie zariadenie.

Prevádzkové prostredie jednotky vozidla inštalovanej vo vozidle je popísané na nasledovnom obrázku:

Obrázok 1

Prevádzkové prostredie JV



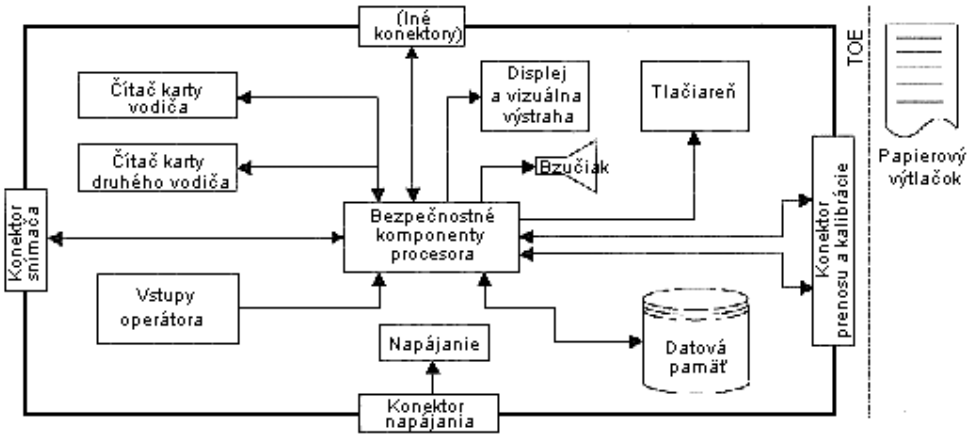
Všeobecné charakteristiky, funkcie a prevádzkové režimy JV sú popísané v kapitole II prílohy I B.

Funkčné požiadavky JV sú špecifikované v kapitole III prílohy I B.

Typická JV je popísaná na nasledovnom obrázku:

Obrázok 2

Typická JV (...) nepovinná



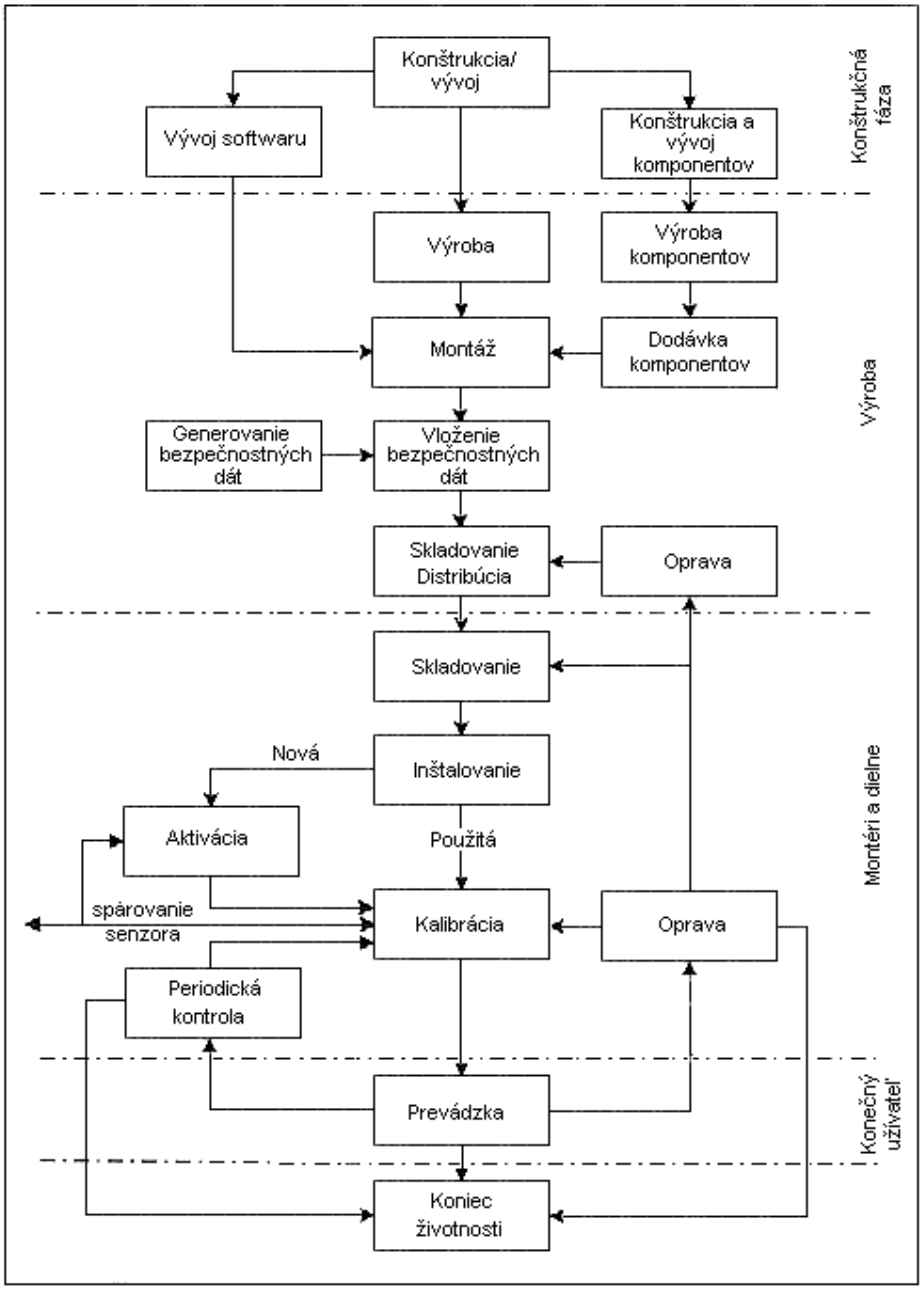
Je treba poznamenať, že hoci je tlačiarenský mechanizmus súčasťou TOE (objektu hodnotenia), neplatí to pre raz vytlačený dokument.

3.2 ***Cyklus životnosti jednotky vozidla***

Typický cyklus životnosti JV je popísaný na nasledovnom obrázku:

Obrázok 3

Typický cyklus životnosti JV



3.3 ***Bezpečnostné riziká***

Tento odsek popisuje možné bezpečnostné riziká pre JV.

3.3.1 *Bezpečnostné riziká súvisiace s identifikáciou a kontrolou prístupu*

T.Access	Užívatelia by sa mohli pokúsiť o prístup k funkciám, ktoré nemajú povolené (napr. vodič žiada o prístup ku kalibračnej funkcii)
T.Identification	Užívatelia by sa mohli pokúsiť o niekoľkonásobnú alebo žiadnu identifikáciu.

3.3.2 *Bezpečnostné riziká súvisiace s konštrukciou*

T.Faults	Poruchy v hardware, software alebo komunikačnom postupe by mohli dostať JV do nepredvídaných situácií ohrozujúcich jej bezpečnosť
T.Tests	Použitie neplatných skúšobných režimov alebo prípadných existujúcich „zadných dvierok“ by mohli ohroziť bezpečnosť JV
T.Design	Užívatelia by sa mohli pokúsiť o nelegálne získanie znalostí o konštrukcii z materiálov výrobcu (krádežou, podplácaním, ...) alebo metódou „reverse engineering“.

3.3.3 *Bezpečnostné riziká súvisiace s prevádzkou*

T.Calibration_Parameters	Užívatelia by sa mohli pokúsiť použiť nesprávne kalibrované prístroje (zmenou kalibračných dát alebo organizačnými nedostatkami)
T.Card_Data_Exchange	Užívatelia by sa mohli pokúsiť o zmenu dát pri ich výmene medzi JV a tachografovými kartami (doplnenie, zmena, vypustenie, opakovanie signálu)
T.Clock	Užívatelia by sa mohli pokúsiť o zmenu hodín systému
T.Environment	Užívatelia by mohli ohroziť bezpečnosť JV zásahmi zvonku (tepelnými, elektromagnetickými, optickými, chemickými, mechanickými, ...)
T.Fake_Devices	Užívatelia by sa mohli pokúsiť pripojiť k JV falošné zariadenia (snímač pohybu, inteligentné karty)
T.Hardware	Užívatelia by sa mohli pokúsiť o zmenu hardwaru JV
T.Motion_Data	Užívatelia by sa mohli pokúsiť o zmenu pohybových dát vozidla (doplnenie, zmena, vypustenie, opakovanie signálu)
T.Non_Activated	Užívatelia by sa mohli pokúsiť o použitie neaktivovaného zariadenia
T.Output_Data	Užívatelia by sa mohli pokúsiť o zmenu výstupu dát (tlač, zobrazovanie alebo sťahovanie)
T.Power_Supply	Užívatelia by sa mohli pokúsiť o anulovanie bezpečnostných cieľov JV pomocou manipulácie s dodávkou prúdu (prerušenie, zníženie, zvýšenie)
T.Security_Data	Užívatelia by sa mohli pokúsiť o nelegálne získanie znalostí o bezpečnostných dátach počas generovania bezpečnostných dát alebo počas prenosu alebo ukladania v zariadení
T.Software	Užívatelia by sa mohli pokúsiť o zmenu softwaru JV
T.Stored_Data	Užívatelia by sa mohli pokúsiť o zmenu uložených dát (bezpečnostných alebo užívateľských dát).

3.4 ***Bezpečnostné ciele***

Hlavným bezpečnostným cieľom systému digitálneho tachografu je toto:

O.Main	Dáta kontrolované kontrolnými orgánmi musia byť dostupné a musia plne a presne odrážať činnosti kontrolovaných vodičov a vozidiel v čase vedenia vozidla, práce, pohotovosti a odpočinku ako aj rýchlosť vozidla

Preto je bezpečnostným cieľom JV, ktorým prispieva k hlavnému bezpečnostnému cieľu, nasledovné:

O.VU_Main	Merané a zaznamenané dáta, ktoré sú potom kontrolované kontrolnými orgánmi, musia byť dostupné a musia presne odrážať činnosti kontrolovaných vodičov a vozidiel v čase vedenia vozidla, práce, pohotovosti a odpočinku ako aj rýchlosť vozidla
O.VU_Export	JV musí byť schopná exportovať dáta na vonkajšie pamäťové médium tak, aby bolo možno overiť ich integritu a autenticitu.

3.5 ***Informačno–technické bezpečnostné ciele***

Špecifické informačno–technické bezpečnostné ciele JV, ktorými prispieva k hlavnému bezpečnostnému cieľu, sú tieto:

O.Access	JV musí riadiť prístup užívateľa k funkciám a dátam
O.Accountability	JV musí zhromažďovať presne priraditeľné dáta
O.Audit	JV musí preverovať pokusy o narušenie bezpečnosti systému a mala by ich sledovať vo vzťahu k pripojeným užívateľom
O.Authentication	JV by mala autentifikovať užívateľov a pripojené prístrojové jednotky (keď sa má vytvoriť dôveryhodné spojenie medzi jednotkami)
O.Integrity	JV musí uchovávať integritu uložených dát
O.Output	JV musí zabezpečiť, aby datový výstup presne odrážal merané alebo uložené dáta
O.Processing	JV musí zabezpečiť presné spracovanie vstupných dát, z ktorých sa odvodia užívateľské dáta
O.Reliability	JV musí poskytovať spoľahlivé služby
O.Secured_Data_Exchange	JV musí zabezpečiť výmeny bezpečnostných dát so snímačom pohybu a s tachografovými kartami.

3.6 ***Fyzické, personálne alebo postupové prostriedky***

Tento odsek popisuje fyzické, personálne alebo postupové požiadavky, ktoré prispievajú k bezpečnosti JV.

3.6.1 *Konštrukcia zariadenia*

M.Development	Vývojoví pracovníci JV musia zabezpečiť, aby sa priradenie zodpovednosti počas vývoja vykonávalo spôsobom, ktorý zachová IT bezpečnosť
M.Manufacturing	Výrobcovia JV musia zabezpečiť, aby sa priradenie zodpovednosti počas výroby vykonávalo spôsobom, ktorý zachová IT bezpečnosť a aby počas výrobného procesu bola JV chránená proti fyzickým zásahom, ktoré by mohli ohroziť IT bezpečnosť.

3.6.2 *Dodávka zariadenia a aktivácia*

M.Delivery	Výrobcovia JV, výrobcovia vozidla a montéri alebo dielne musia zabezpečiť, aby sa s neaktivovanou JV zaobchádzalo tak, aby sa zachovala bezpečnosť JV

M.Activation Výrobcovia vozidla a montéri alebo dielne musia aktivovať JV po jej inštalovaní predtým než vozidlo opustí prevádzkové priestory, v ktorých sa inštalovanie uskutočnilo.

3.6.3 *Generovanie a dodávka bezpečnostných dát*

M.Sec_Data_Generation Algoritmy generovania bezpečnostných dát musia byť prístupné len oprávneným a dôveryhodným osobám

M.Sec_Data_Transport Bezpečnostné dáta musia byť generované, prenášané a vkladané do JV tak, aby sa zachovala ich primeraná dôvernosť a integrita.

3.6.4 *Dodávka kariet*

M.Card_Availibility Tachografové karty sa musia sprístupniť a dodať len oprávneným osobám

M.Driver_Card_Uniqeuness Vodiči musia vlastniť vždy len jednu platnú kartu vodiča

M.Card_Traceability Odovzdanie karty musí byť sledovateľné (biele a čierne zoznamy) a čierne zoznamy sa musia použiť počas bezpečnostných auditov.

3.6.5 *Inštalovanie záznamového zariadenia, kalibrácia a kontrola*

M.Approved_Workshops Inštalovanie, kalibráciu a opravu záznamového zariadenia musia vykonávať dôveryhodní a schválení montéri alebo dielne

M.Regular_Inspections Záznamové zariadenie sa musí pravidelne kontrolovať a kalibrovať

M.Faithful_Calibration Schválení montéri a dielne musia počas kalibrácie do záznamového zariadenia zapísať správne parametre vozidla

3.6.6 *Prevádzka zariadenia*

M.Faithful_Drivers Vodiči musia dodržiavať predpisy a konať zodpovedne (napr. používať svoje karty vodiča, správne zvoliť svoju činnosť z činností, ktoré sa vyberajú manuálne, ...).

3.6.7 *Kontrola dodržiavania predpisov*

M.Controls Kontrola dodržiavania predpisov sa musí vykonávať pravidelne a metódou námatkovej skúšky a musí zahŕňať bezpečnostné audity.

3.6.8 *Modernizácia softwaru*

M.Software_Upgrade Revíziám softwaru musí byť udelená bezpečnostná certifikácia predtým, než sa môžu zaviesť do JV.

4. **Bezpečnostné vynucovacie funkcie**

4.1 ***Identifikácia a autentifikácia***

4.1.1 *Identifikácia snímača pohybu a autentifikácia*

UIA_201 JV musí byť pre každú interakciu schopná stanoviť identitu snímača pohybu, ku ktorému je pripojená.

UIA_202 Identita snímača pohybu sa skladá zo schvaľovacieho číslo snímača a zo sériového číslo snímača.

UIA_203 JV musí autentifikovať pripojený snímač pohybu

- pri pripojení snímača pohybu,
- pri každej kalibrácii záznamového zariadenia,

– pri obnovení napájania.

Autentifikácia musí byť vzájomná a spúšťa ju JV.

UIA_204 JV musí pravidelne (interval určí výrobca a musí sa vykonať častejšie než raz za hodinu) opakovane autentifikovať snímač pohybu, ku ktorému je pripojená a musí zabezpečiť, aby snímač pohybu identifikovaný počas poslednej kalibrácie záznamového zariadenia, nebol vymenený.

UIA_205 JV musí zistiť a zabrániť použitiu autentifikovaných dát, ktoré boli kopírované alebo prehrávané.

UIA_206 Po zistení určitého počtu (určí výrobca a nesmie prekročiť počet 20) po sebe idúcich neúspešných pokusov o autentifikáciu a/alebo po zistení, že identita snímača pohybu bola bez oprávnenia zmenená (t. j. nie počas kalibrácie záznamového zariadenia) SEF:

– generuje auditný záznam udalosti,

– varuje užívateľa,

– pokračuje v prijímaní a využívaní nezabezpečených pohybových dát odosielaných snímačom pohybu.

4.1.2 *Identifikácia a autentifikácia užívateľa*

UIA_207 JV pravidelne a selektívne overuje identitu dvoch užívateľov monitorovaním tachografových kariet vložených do príslušného slotu vodiča alebo druhého vodiča.

UIA_208 Identita užívateľa sa skladá zo:

- skupiny užívateľov:
  - VODIČ (karta vodiča),
  - KONTROLÓR (kontrolná karta),
  - DIELŇA (dielenská karta),
  - PODNIK (podniková karta),
  - NEZNÁME (nie je vložená žiadna karta),
- identifikácie užívateľa pozostávajúcej z:
  - kódu členského štátu vydávajúceho kartu a čísla karty,
  - NEZNÁME, ak je skupina užívateľov NEZNÁMA.

NEZNÁME identity môžu byť implicitne alebo explicitne známe.

UIA_209 JV musí svojich užívateľov autentifikovať pri vložení karty.

UIA_210 JV musí svojich užívateľov znovu autentifikovať:

- pri obnovení napájania,
- pravidelne alebo po výskyte špecifických udalostí (určí výrobca a musí to byť častejšie než raz za deň).

UIA_211 Autentifikácia sa vykoná pomocou dôkazu o platnosti vloženej tachografovej karty obsahujúcej bezpečnostné dáta, ktoré môžu pochádzať len zo systému. Autentifikácia musí byť vzájomná a spúšťa ju JV.

UIA_212 Okrem toho sa od dielne vyžaduje, aby bola úspešne autentifikovaná pomocou kontroly PIN–u. PIN musí mať aspoň štyri znaky.

Poznámka: v prípade, že je PIN prenášaný na JV z vonkajšieho zariadenia umiestneného v blízkosti JV, PIN nemusí byť počas prenosu chránený.

UIA_213 JV musí zistiť a zabrániť použitiu autentifikovaných dát, ktoré boli kopírované alebo prehrávané.

UIA_214 Po zistení piatich po sebe idúcich neúspešných pokusov o autentifikáciu, SEF:

- generuje auditný záznam udalosti,
- varuje užívateľa,
- predpokladá, že užívateľ je neznámy a karta neplatná (definícia z) a požiadavka 007).

4.1.3 *Identifikácia a autentifikácia diaľkovo pripojeného podniku*

Spôsobilosť diaľkového pripojenia je nepovinná. Tento odsek platí preto len vtedy, keď je táto možnosť realizovaná.

UIA_215 JV musí byť pre každú interakciu s diaľkovo pripojeným podnikom schopná stanoviť identitu podniku.

UIA_216 Identita diaľkovo pripojeného podniku sa skladá z kódu členského štátu vydávajúceho kartu a čísla podnikovej karty.

UIA_217 JV musí úspešne autentifikovať diaľkovo pripojený podnik predtým, než povolí akýkoľvek export dát tomuto podniku.

UIA_218 Autentifikácia sa vykoná pomocou dôkazu o tom, že podnik vlastní platnú podnikovú kartu obsahujúcu bezpečnostné dáta, ktoré môžu pochádzať len zo systému.

UIA_219 JV musí zistiť a zabrániť použitiu autentifikovaných dát, ktoré boli kopírované alebo prehrávané.

UIA_220 Po zistení piatich po sebe idúcich neúspešných pokusov o autentifikáciu, JV:

– varuje diaľkovo pripojený podnik.

4.1.4 *Identifikácia a autentifikácia riadiaceho zariadenia*

Výrobcovia JV môžu plánovať špeciálne zariadenia pre doplnkové riadiace funkcie JV (napr. modernizácia softwaru, opätovné načítanie dát, ...). Tento odsek platí preto len vtedy, keď je táto možnosť realizovaná.

UIA_221 JV musí byť pre každú interakciu s riadiacim zariadením schopná stanoviť identitu zariadenia.

UIA_222 Pred akoukoľvek ďalšou interakciou musí JV úspešne autentifikovať riadiace zariadenie.

UIA_223 JV musí zistiť a zabrániť použitiu autentifikovaných dát, ktoré boli kopírované alebo prehrávané.

4.2 **Kontrola prístupu**

Kontroly prístupu zabezpečujú, aby čítanie, vytváranie a zmeny informácií v TOE vykonávali len k tomu oprávnené osoby.

Je treba poznamenať, že užívateľské dáta zaznamenané JV, hoci obsahujú súkromne prípadne komerčne citlivé aspekty, nemajú dôverný charakter. Preto nie je funkčná požiadavka vzťahujúca sa k právam na prístup k dátam (požiadavka 011), predmetom bezpečnostnej vynucovacej funkcie.

4.2.1 *Oprávnenie na prístup*

ACC_201 JV musí riadiť a kontrolovať práva na prístup k funkciám a dátam.

4.2.2 *Prístupové práva k funkciám*

ACC_202 JV musí uplatniť pravidlá voľby prevádzkového režimu (požiadavky 006 až 009).

ACC_203 JV použije prevádzkový režim na uplatnenie pravidiel týkajúcich sa kontroly prístupu k funkciám (požiadavka 010).

4.2.3 *Prístupové práva k dátam*

ACC_204 JV musí uplatniť pravidlá zápisového prístupu k identifikačným dátam JV. (požiadavka 076).

ACC_205 JV musí uplatniť pravidlá zápisového prístupu k identifikačným dátam spárovaného snímača pohybu (požiadavky 079 a 155).

ACC_206 Po aktivácii JV musí JV zabezpečiť, aby sa mohli kalibračné dáta vložiť do JV a uložiť do jej dátovej pamäti len v režime kalibrácie (požiadavky 154 a 156)

ACC_207 Po aktivácii JV musí JV uplatniť pravidlá zápisového prístupu ku kalibračným dátam a pravidlá vymazania (požiadavka 097).

ACC_208 Po aktivácii JV musí JV zabezpečiť, aby sa mohli dáta nastavenia času vložiť do JV a uložiť do jej dátovej pamäti len v režime kalibrácie (Táto požiadavka neplatí pri malých nastaveniach času povolených v rámci požiadaviek 157 a 158).

ACC_209 Po aktivácii JV musí JV uplatniť pravidlá zápisového prístupu k dátam nastavenia času a pravidlá vymazania (požiadavka 100).

ACC_210 JV musí uplatniť príslušné čítacie a zápisové pravidlá prístupu k bezpečnostným dátam (požiadavka 080).

4.2.4 *Štruktúra súboru a prístupové podmienky*

ACC_211 Štruktúra aplikačných a dátových súborov a prístupové podmienky sa vytvoria už počas výrobného procesu a potom sa zablokujú proti akejkoľvek budúcej zmene alebo vymazaniu.

4.3 **Sledovateľnosť**

ACT_201 JV musí zabezpečiť, aby sa mohli vodičom priradiť ich činnosti (požiadavky 081, 084, 087, 105a, 109 a 109a).

ACT_202 JV trvalo uchováva identifikačné dáta (požiadavka 075).

ACT_203 JV musí zabezpečiť, aby sa mohli dielňam priradiť ich činnosti (požiadavky 098, 101 a 109).

ACT_204 JV musí zabezpečiť, aby sa mohli kontrolórom priradiť ich činnosti (požiadavky 102, 103 a 109).

ACT_205 JV zaznamenáva stav kilometrov (požiadavka 090) a podrobné rýchlostné dáta (požiadavka 093).

ACT_206 JV musí zabezpečiť, aby užívateľské dáta vzťahujúce sa k požiadavkám 081 až 093 a 102 až 105b vrátane, po zázname nemenili okrem prípadov, kedy sa po vyčerpaní kapacity pamäte stávajú najstaršími uloženými dátami, ktoré sa prepíšu novými dátami.

ACT_207 JV nesmie meniť dáta, ktoré sú už uložené na tachografovej karte (požiadavky 109 a 109a) okrem prepísania najstarších dát novými dátami (požiadavka 110) alebo v prípade popísanom v poznámke k odseku 2.1 doplnku 1.

4.4 ***Audit***

Možnosť vykonania auditu sa vyžaduje len u udalostí, ktoré môžu poukazovať na manipuláciu alebo pokus o narušenie bezpečnosti. Nevyžaduje sa pri normálnom uplatňovaní práv aj keď sú tieto relevantné pre bezpečnosť.

AUD_201 JV musí pri udalostiach poškodzujúcich jej bezpečnosť, zaznamenať tieto udalosti spolu s príslušnými dátami (požiadavky 094, 096 a 109).

AUD_202 Udalosti, ktoré majú vplyv na bezpečnosť JV sú tieto:

- pokusy o narušenie bezpečnosti,
- chybná autentifikácia snímača pohybu,
- chybná autentifikácia tachografovej karty,
- neoprávnená zmena snímača pohybu,
- chyba integrácie vstupných dát karty,
- chyba integrácie uložených užívateľských dát,
- vnútorná chyba prenosu dát,
- neoprávnené otvorenie puzdra,
- manipulácia s hardwarom,
- nesprávne uzavretá posledná relácia karty,
- udalosť chybné pohybové dáta,
- udalosť prerušenie napájania,
- vnútorná porucha JV.

AUD_203 JV musí uplatniť pravidlá ukladania do pamäti (požiadavky 094 a 096).

AUD_204 JV musí vo svojej pamäti uchovávať auditné záznamy generované snímačom pohybu.

AUD_205 Musí byť možné tlačiť, zobrazovať a prenášať auditné záznamy.

4.5 ***Opätovné použitie pamäťového média***

REU_201 JV musí zabezpečiť, aby sa dočasné pamäťové médiá mohli znovu použiť bez toho, aby to zahŕňalo neprístupný informačný tok.

4.6 ***Presnosť***

4.6.1 *Opatrenia na kontrolu informačných tokov*

ACR_201 JV musí zabezpečiť, aby sa dáta vzťahujúce sa k požiadavkám 081, 084, 087, 090, 093, 102, 104, 105, 105a a 109 mohli spracovávať len vtedy, keď pochádzajú zo správnych vstupných zdrojov:

- pohybové dáta vozidla,
- reálny čas JV,
- kalibračné parametre záznamového zariadenia,
- tachografové karty,
- vstupy užívateľa.

ACR_201a JV musí zabezpečiť, aby sa dáta vzťahujúce sa k požiadavke 109a mohli zapisovať len počas časového úseku od posledného vytiahnutia karty do aktuálneho vloženia karty (požiadavka 050a).

4.6.2 *Vnútorné prenosy dát*

Požiadavky tohto odseku platia len vtedy, keď JV využíva fyzicky oddelené časti.

ACR_202 Ak sú dáta prenášané medzi fyzicky oddelenými časťami JV, dáta sa musia chrániť pred zmenou.

ACR_203 Po zistení chyby v prenose dát počas vnútorného prenosu, prenos sa opakuje a SEF generuje auditný záznam o udalosti.

4.6.3 *Integrita uložených dát*

ACR_204 JV musí kontrolovať užívateľské dáta uložené vo svojej pamäti z hľadiska chýb integrity.

ACR_205 Po zistení chyby integrity uložených dát, SEF generuje auditný záznam.

4.7 ***Spoľahlivosť služby***

4.7.1 *Skúšky*

RLB_201 Všetky príkazy, činnosti alebo skúšobné body špecifické pre skúšobné potreby výrobnej fázy JV sa pred aktiváciou JV deaktivujú alebo odstránia.

RLB_202 JV vykoná samoskúšky pri prvom zapnutí a počas normálnej prevádzky, aby sa overila jej správna činnosť. Samoskúšky JV zahŕňajú overenie integrity bezpečnostných dát a overenie integrity uloženého vykonávacieho kódu (ak nie je v ROM).

RLB_203 Po zistení vnútornej chybnej funkcie počas samoskúšky, SEF:

– generuje auditný záznam (okrem režimu kalibrácie) (vnútorná porucha JV),

– zachová integritu uchovávaných dát.

4.7.2 *Software*

RLB_204 Po aktivovaní JV nesmie existovať možnosť analyzovať alebo ladiť software pri praktickom používaní.

RLB_205 Vstupy z vonkajších zdrojov nesmú byť akceptované ako vykonávací kód.

4.7.3 *Fyzická ochrana*

RLB_206 Ak je JV konštruovaná tak, aby sa mohla otvoriť, JV musí zistiť každé otvorenie puzdra, dokonca aj bez vonkajšieho napájania minimálne po dobu šiestich mesiacov. V takom prípade SEF generuje auditný záznam o udalosti (pripúšťa sa, aby sa auditný záznam generoval a uložil po obnovení napájania).

Ak je JV konštruovaná tak, že sa nemôže otvoriť, každý pokus o neoprávnené zásahy sa musí dať ľahko zistiť (napr. vizuálnou kontrolou).

RLB_207 Po svojej aktivácii musí JV zistiť určitú (určí výrobca) manipuláciu s hardwarom.

RLB_208 V prípade popísanom vyššie, SEF generuje auditný záznam a JV: (určí výrobca).

4.7.4 *Prerušenie napájania*

RLB_209 JV musí zistiť odchýlky od špecifikovaných hodnôt napájania, vrátane prerušenia dodávky prúdu.

RLB_210 V prípade popísanom vyššie, SEF:

– generuje auditný záznam (okrem režimu kalibrácie),

– zachová bezpečnostný stav JV,

– zachová prevádzkyschopné bezpečnostné funkcie vzťahujúce sa ku komponentom alebo procesom,

– zachová integritu uložených dát.

4.7.5 *Podmienky resetovania*

RLB_211 V prípade prerušenia napájania alebo ak sa prenos zastaví pred dokončením, alebo pri ktorejkoľvek inej podmienke resetovania, JV sa musí resetovať.

4.7.6 *Dostupnosť dát*

RLB_212 JV musí zabezpečiť, aby bol na požiadanie možný prístup k zdrojom a aby sa dáta ani zbytočne nevyžadovali ani neuchovávali.

RLB_213 JV musí zabezpečiť, aby sa karta nemohla uvoľniť skôr, než budú na ňu uložené príslušné dáta (požiadavka 015 a 016).

RLB_214 V prípade popísanom vyššie, SEF generuje auditný záznam o udalosti.

4.7.7 *Viacnásobné aplikácie*

RLB_215 Ak JV ponúka aplikácie iné než je tachografová aplikácia, všetky aplikácie musia byť fyzicky a/alebo logicky navzájom oddelené. Tieto aplikácie nesmú mať zdieľané bezpečnostné dáta. Môže byť aktívna vždy len jedna funkcia.

4.8 **Výmena dát**

Tento odsek sa týka výmeny medzi JV a pripojenými zariadeniami.

4.8.1 *Výmena dát so snímačom pohybu*

DEX_201 JV musí overiť integritu a autenticitu pohybovaných dát importovaných zo snímača pohybu.

DEX_202 Po zistení chyby integrity alebo autenticity pohybových dát, SEF

- generuje auditný záznam,
- pokračuje v používaní importovaných dát.

4.8.2 *Výmena dát s tachografovými kartami*

DEX_203 JV musí overiť integritu a autenticitu pohybovaných dát importovaných z tachografových kariet.

DEX_204 Po zistení chyby integrity alebo autenticity pohybových dát, JV:

- generuje auditný záznam,
- nepoužije dáta.

DEX_205 JV exportuje dáta na tachografové inteligentné karty s príslušnými bezpečnostnými atribútmi tak, aby sa mohla overiť integrita a autenticita sťahovaných dát.

4.8.3 *Výmena dát s vonkajším pamäťovým médiom (funkcia sťahovania (prenosu) dát)*

DEX_206 JV generuje dôkaz o pôvode dát prenášaných na vonkajšie médium.

DEX_207 JV poskytne príjemcovi možnosť overenia dôkazu o pôvode sťahovaných dát.

DEX_208 JV exportuje dáta na vonkajšie médium s príslušnými bezpečnostnými atribútmi tak, aby sa mohla overiť integrita a autenticita sťahovaných dát.

4.9 ***Kryptografická podpora***

Požiadavky tohto odseku sú aplikovateľné len pokiaľ sú potrebné, závisiac na použitom bezpečnostnom mechanizme a na riešeniach výrobcu.

CSP_201 Každá kryptografická operácia vykonávaná JV musí byť v súlade so špecifikovanými algoritmami a špecifikovanou veľkosťou kľúča.

CSP_202 Ak JV generuje kryptografické kľúče, musí to byť v súlade so špecifikovanými algoritmami generovania kryptografických kľúčov a špecifikovanými veľkosťami kryptografických kľúčov.

CSP_203 Ak JV distribuuje kryptografické kľúče, musí to byť v súlade so špecifikovanými metódami distribúcie kľúča.

CSP_204 Ak JV sprístupňuje kryptografické kľúče, musí to byť v súlade so špecifikovanými metódami prístupu ku kryptografickým kľúčom.

CSP_205 Ak JV zničí kryptografické kľúče, musí to byť v súlade so špecifikovanými metódami zničenia kryptografických kľúčov.

5. **Definícia bezpečnostných mechanizmov**

Požadované bezpečnostné mechanizmy sú špecifikované v doplnku 11.

Všetky ostatné bezpečnostné mechanizmy stanovia výrobcovia.

6. **Minimálna odolnosť bezpečnostných mechanizmov**

Minimálna odolnosť bezpečnostných mechanizmov jednotky vozidla je „Vysoká“, podľa definície v ITSEC.

7. **Úroveň ručenia**

Cieľová úroveň ručenia pre jednotku vozidla je ITSEC úroveň **E3**, podľa definície v ITSEC.

8. **Základný princíp**

Základný princíp SEF je založený na nasledovných maticiach, ktoré udávajú:

– ktoré SEF alebo prostriedky sú vystavené ktorým bezpečnostným rizikám,

– ktoré SEF spĺňajú ktoré IT bezpečnostné ciele.

	Bezpečnostné riziká																		IT ciele								
	Prístup	Identifikácia	Chyby	Skúšky	Konštrukcia	Kalibračné parametre	Výmena kartových dát	Hodiny	Prostredie	Falošné zariadenia	Hardware	Pohybové dáta	Neaktivované	Výstupné dáta	Napájanie	B	ezpečnostné dáta	Software	Uložené dáta	Prístup	Sledovateľnosť	Audit	Autentifikácia	Integrita	Výstup	Spracovanie	Spoľahlivosť	Výmena bezpečn. dát
Fyzické, personálne, postupové prostriedky																												
Vývoj			x	x	x																							
Výroba				x	x																							
Dodávka													x															
Aktivovanie	x												x															
Generovanie bezpečnostných dát																	x											
Prenos bezpečnostných dát																	x											
Dostupnosť karty		x																										
Len jedna karta na vodiča		x																										
Sledovateľnosť karty		x																										
Schválené dielne						x		x																				

	Bezpečnostné riziká																			IT ciele									
	Prístup	Identifikácia	Chyby	Skúšky	Konštrukcia	Kalibračné parametre	Výmena kartových dát	Hodiny	Prostredie	Falošné zariadenia	Hardware	Pohybové dáta	Neaktivované	Výstupné dáta	Napájanie	B	ezpečnostné dáta	Software	Uložené dáta	Prístup	Sledovateľnosť	Audit	Autentifikácia	Integrita	Výstup	Spracovanie	Spoľahlivosť	Výmena bezpečn. dát
Pravidelná kontrola, kalibrácia						x		x				x	x			x													
Spoľahlivé dielne						x		x																					
Spoľahliví vodiči		x																											
Kontroly dodržiavania predpisov		x				x		x	x		x		x		x			x	x										
Modernizácia softwaru																			x										
Bezpečnostné vynucovacie funkcie																													
Identifikácia a autentifikácia																													
UIA_201 Identifikácia snímača										x		x											x						x
UIA_202 Identita snímača										x		x											x						x
UIA_203 Autentifikácia snímača										x		x											x						x
UIA_204 Nová identifikácia a autentifi–kácia snímača										x		x											x						x
UIA_205 Autentifikácia bezpečná voči falšovaniu										x		x											x						
UIA_206 Chybná autentifikácia										x		x										x						x	
UIA_207 Identifikácia užívateľa	x	x								x										x			x						x
UIA_208 Identita užívateľa	x	x								x										x			x						x

	Bezpečnostné riziká																			IT ciele								
	Prístup	Identifikácia	Chyby	Skúšky	Konštrukcia	Kalibračné parametre	Výmena kartových dát	Hodiny	Prostredie	Falošné zariadenia	Hardware	Pohybové dáta	Neaktivované	Výstupné dáta	Napájanie	B	ezpečnostné dáta	Software	Uložené dáta	Prístup	Sledovateľnosť	Audit	Autentifikácia	Integrita	Výstup	Spracovanie	Spoľahlivosť	Výmena bezpečn. dát
UIA_209 Autentifikácia užívateľa	x	x								x										x			x					x
UIA_210 Nová autentifikácia užívateľa	x	x								x										x			x					x
UIA_211 Prostriedky autentifikácie	x	x								x										x			x					x
UIA_212 Kontroly PIN–u	x	x				x		x												x			x					
UIA_213 Autentifikácia bezpečná voči falšovaniu	x	x								x										x			x					
UIA_214 Chybná autentifikácia	x	x								x												x						
UIA_215 Identifikácia vzdialeného užívateľa	x	x																		x			x					x
UIA_216 Identita vzdialeného užívateľa	x	x																		x			x					
UIA_217 Autentifikácia vzdialeného užívateľa	x	x																		x			x					x
UIA_218 Prostriedky autentifikácie	x	x																		x			x					
UIA_219 Autentifikácia bezpečná voči falšovaniu	x	x																		x			x					
UIA_220 Chybná autentifikácia	x	x																										

	Bezpečnostné riziká																		IT ciele								
	Prístup	Identifikácia	Chyby	Skúšky	Konštrukcia	Kalibračné parametre	Výmena kartových dát	Hodiny	Prostredie	Falošné zariadenia	Hardware	Pohybové dáta	Neaktivované	Výstupné dáta	Napájanie	B	ezpečnostné dáta	Software	Uložené dáta	Prístup	Sledovateľnosť	Audit	Autentifikácia	Integrita	Výstup	Spracovanie	Spoľahlivosť	Výmena bezpečn. dát
UIA_221 Identifikácia riadiaceho zariadenia	x	x																		x			x					
UIA_222 Autentifikácia riadiaceho zariadenia	x	x																		x			x					
UIA_223 Autentifikácia bezpečná voči falšovaniu	x	x																		x			x					
Kontrola prístupu																												
ACC_201 Oprávnenie na prístup	x					x		x									x		x	x								
ACC_202 Prístupové práva k funkciám	x					x		x												x								
ACC_203 Prístupové práva k funkciám	x					x		x												x								
ACC_204 Identifikácia JV																			x	x								
ACC_205 Identifikácia pripojeného snímača										x									x	x								
ACC_206 Kalibračné dáta	x					x													x	x								
ACC_207 Kalibračné dáta						x													x	x								
ACC_208 Dáta nastavenia času								x											x	x								
ACC_209 Dáta nastavenia času								x											x	x								
ACC_210 Bezpečnostné dáta																	x		x	x								

	Bezpečnostné riziká																			IT ciele								
	Prístup	Identifikácia	Chyby	Skúšky	Konštrukcia	Kalibračné parametre	Výmena kartových dát	Hodiny	Prostredie	Falošné zariadenia	Hardware	Pohybové dáta	Neaktivované	Výstupné dáta	Napájanie	B	ezpečnostné dáta	Software	Uložené dáta	Prístup	Sledovateľnosť	Audit	Autentifikácia	Integrita	Výstup	Spracovanie	Spoľahlivosť	Výmena bezpečn. dát
ACC_211 Štruktúra súboru a prístupo– vé podmienky	x					x											x		x	x								
Sledovateľnosť																												
ACT_201 Priradenie k vodičom																					x							
ACT_202 Identifikačné dáta JV																					x	x						
ACT_203 Priradenie k dielňam																					x							
ACT_204 Priradenie ku kontrolórom																					x							
ACT_205 Priradenie k vozidlám																					x							
ACT_206 Zmena priraďovacích dát																			x					x			x	
ACT_207 Zmena priraďovacích dát																			x					x			x	
Audit																												
AUD_201 Auditné záznamy																						x						
AUD_202 Zoznam auditných udalostí	x						x				x	x		x	x				x			x						
AUD_203 Pravidlá ukladania audit– ných záznamov pamäti																						x						
AUD_204 Auditné záznamy snímača																						x						
AUD_205 Auditné nástroje																						x						

	Bezpečnostné riziká																		IT ciele								
	Prístup	Identifikácia	Chyby	Skúšky	Konštrukcia	Kalibračné parametre	Výmena kartových dát	Hodiny	Prostredie	Falošné zariadenia	Hardware	Pohybové dáta	Neaktivované	Výstupné dáta	Napájanie	B	ezpečnostné dáta	Software	Uložené dáta	Prístup	Sledovateľnosť	Audit	Autentifikácia	Integrita	Výstup	Spracovanie	Spoľahlivosť	Výmena bezpečn. dát
Opätovné použitie																												
REU_201 Opätovné použitie																	x									x	x	
Presnosť																												
ACR_201 Opatrenia na kontrolu informačných tokov						x			x		x															x	x	
ACR_202 Vnútorné prenosy														x											x	x	x	
ACR_203 Vnútorné prenosy														x								x						
ACR_204 Integrita uložených dát																			x					x			x	
ACR_205 Integrita uložených dát																			x			x						
Spoľahlivosť																												
RLB_201 Výrobné skúšky				x	x																						x	
RLB_202 Samoskúšky			x								x				x			x									x	
RLB_203 Samoskúšky											x				x			x				x						
RLB_204 Analýza softwaru					x													x									x	
RLB_205 Vstupy softwaru																		x						x	x	x		
RLB_206 Otvorenie puzdra					x				x		x			x			x	x	x						x		x	

	Bezpečnostné riziká																			IT ciele									
	Prístup	Identifikácia	Chyby	Skúšky	Konštrukcia	Kalibračné parametre	Výmena kartových dát	Hodiny	Prostredie	Falošné zariadenia	Hardware	Pohybové dáta	Neaktivované	Výstupné dáta	Napájanie	B	ezpečnostné dáta	Software	Uložené dáta	Prístup	Sledovateľnosť	Audit	Autentifikácia	Integrita	Výstup	Spracovanie	Spoľahlivosť	Výmena bezpečn. dát
RLB_207 Manipulácia s hardwarom											x																x	
RLB_208 Manipulácia s hardwarom											x											x						
RLB_209 Prerušenie napájania															x												x	
RLB_210 Prerušenie napájania															x							x						
RLB_211 Resetovanie			x																								x	
RLB_212 Dostupnosť dát																										x	x	
RLB_213 Uvoľnenie karty																											x	
RLB_214 Nesprávne uzavretá relácia karty																							x					
RLB_215 Viacnásobné aplikácie																											x	
Výmena dát																												
DEX_201 Bezpečný import pohybo–vých dát												x																x
DEX_202 Bezpečný import pohybo–vých dát												x							x									
DEX_203 Bezpečný import kartových dát							x																					x

	Bezpečnostné riziká																			IT ciele									
	Prístup	Identifikácia	Chyby	Skúšky	Konštrukcia	Kalibračné parametre	Výmena kartových dát	Hodiny	Prostredie	Falošné zariadenia	Hardware	Pohybové dáta	Neaktivované	Výstupné dáta	Napájanie	B	ezpečnostné dáta	Software	Uložené dáta	Prístup	Sledovateľnosť	Audit	Autentifikácia	Integrita	Výstup	Spracovanie	Spoľahlivosť	Výmena bezpečn. dát
DEX_204 Bezpečný import kartových dát							x															x						
DEX_205 Bezpečný export dát na karty							x																					x
DEX_206 Dôkaz o pôvode														x											x			
DEX_207 Dôkaz o pôvode														x											x			
DEX_208 Bezpečný export dát na vonkajšie médium														x											x			
Kryptografická podpora																												
CSP_201 Algoritmy																											x	x
CSP_202 Generovanie kľúča																											x	x
CSP_203 Distribúcia kľúča																											x	x
CSP_204 Prístup ku kľúču																											x	x
CSP_205 Zničenie kľúča																											x	x

VŠEOBECNÉ BEZPEČNOSTNÉ POŽIADAVKY NA TACHOGRAFOVÚ KARTU

1. **Úvod**

Tento dokument obsahuje popis tachografovej karty, riziká, ktorým musí čeliť a bezpečnostné ciele, ktoré musí spĺňať. Špecifikuje požadované bezpečnostné vynucovacie funkcie. Stanovuje požadovanú minimálnu odolnosť bezpečnostných mechanizmov a požadovanú úroveň ručenia za vývoj a hodnotenie.

Požiadavky uvedené v dokumente zodpovedajú požiadavkám hlavnej časti prílohy I B. V záujme lepšej zrozumiteľnosti, sa niekedy vyskytujú duplicity medzi požiadavkami hlavnej časti prílohy I B a bezpečnostnými požiadavkami. V prípade rozporu medzi bezpečnostnými požiadavkami a požiadavkami hlavnej časti prílohy I B, na ktoré sa odvolávajú tieto bezpečnostné požiadavky, platia požiadavky hlavnej časti prílohy I B.

Požiadavky hlavnej časti prílohy I B, na ktoré sa neodvolávajú bezpečnostné požiadavky nie sú predmetom bezpečnostných vynucovacích funkcií.

Tachografová karta je štandardná inteligentná karta so špeciálnou tachografovou aplikáciou, ktorá musí spĺňať aktuálne funkčné a bezpečnostné požiadavky aplikovateľné na inteligentné karty. Tieto bezpečnostné požiadavky preto zahŕňajú len doplnkové bezpečnostné požiadavky potrebné pre tachografovú aplikáciu.

Za účelom lepšej sledovateľnosti pojmov použitým v dokumentácii o vývoji a hodnotení, boli možným rizikám, cieľom, postupovým prostriedkom a špecifikáciám SEF priradené jednoznačné označenia.

2. **Skratky, definície a referenčné dokumenty**

2.1 ***Skratky***

IC Integrovaný obvod (elektronický komponent určený na vykonávanie funkcií týkajúcich sa spracovania dát a/alebo pamäťových funkcií

OS	Operačný systém
PIN	Personal identification number (Osobné identifikačné číslo)
ROM	Read Memory Only (permanentná pamäť)
SFP	Pravidlá bezpečnostných funkcií
TOE	Target of evaluation (Objekt hodnotenia)
TSF	TOE security function (Bezpečnostná funkcia objektu hodnotenia)
JV	Jednotka vozidla

2.2 ***Definície***

Digitálny tachograf	Záznamové zariadenie
Citlivé dáta	Dáta ukladané tachografovou kartou, ktoré musia byť chránené z hľadiska integrity, neoprávnenej zmeny a dôvernosti (pokiaľ sa to týka bezpečnostných dát). Citlivé dáta zahŕňajú bezpečnostné a užívateľské dáta.
Bezpečnostné dáta	Špecifické dáta potrebné na podporu bezpečnostných vynucovacích funkcií (napr. kryptografické kľúče)
Systém	Vybavenie, ľudia alebo organizácie vzťahujúce sa akýmkoľvek spôsobom k záznamovému zariadeniu
Užívateľ	Každý subjekt (osoba alebo vonkajšia IT prístrojová jednotka) mimo TOE, ktorá je v interakcii s TOE (keď sa nepoužije vo výraze „užívateľské dáta“)
Užívateľské dáta	Citlivé dáta uložené na tachografovej karte, okrem bezpečnostných dát. Užívateľské dáta zahŕňajú identifikačné dáta a dáta o činnostiach.
Identifikačné dáta karty	Identifikačné dáta zahŕňajú identifikačné dáta karty definované požiadavkami 190, 191, 192, 194, 215, 231 a 235.

Identifikačné dáta držiteľa karty	Užívateľské dáta vzťahujúce sa k identifikácii držiteľa karty definované požiadavkami 195, 196, 216, 232 a 236.
Dáta o činnosti	Dáta o činnosti zahŕňajú dáta o činnostiach držiteľa karty, dáta o udalostiach a poruchách a dáta o kontrolnej činnosti
Dáta o činnostiach držiteľa karty	Užívateľské dáta vzťahujúce sa k činnostiam vykonávaným držiteľom karty definované požiadavkami 197, 199, 202, 212, 212a, 217, 219, 221, 226, 227, 229, 230a, 233 a 237.
Dáta o udalostiach a poruchách	Užívateľské dáta vzťahujúce sa k udalostiam alebo poruchám definované požiadavkami 204, 205, 207, 208 a 223.
Dáta o kontrolnej činnosti	Užívateľské dáta vzťahujúce sa ku kontrole dodržiavania predpisov definované požiadavkami 210 a 225.

2.3 ***Referenčné dokumenty***

ITSEC	ITSEC Information Technology Security Evaluation Criteria 1991 (Kritériá hodnotenia bezpečnosti informačnej techniky)
IC PP	Smartcard Integrated Circuit Protection Profile (Profil ochrany inteligentnej karty s integrovaným obvodom) – verzia 2.0 – vydanie september 1998. Registrované u Francúzskeho certifikačného orgánu pod číslom PP/9806
ES PP	Smart Card Integrated Circuit With Embedded Software Protection Profile (Profil ochrany inteligentnej karty s integrovaným obvodom a s vloženým softwarom) – verzia 2.0 – vydanie jún 99. Registrované u Francúzskeho certifikačného orgánu pod číslom PP/9911

3. **Základný princíp produktu**

3.1 ***Popis tachografovej karty a spôsob používania***

Tachografová karta je inteligentná karta popísaná v (IC PP) a (ES PP), ktorá sa používa spolu so záznamovým zariadením.

Základné funkcie karty sú:

– uchovávať identifikačné dáta karty a držiteľa karty. Tieto dáta používa jednotka vozidla na identifikáciu držiteľa karty, na zaručenie zodpovedajúcich funkcií a prístupových práv k dátam a na zabezpečenie sledovateľnosti držiteľa karty z hľadiska jeho činností,

– uchovávať dáta o činnostiach držiteľa karty, dáta o udalostiach, poruchách a kontrolných činnostiach, vzťahujúce sa k držiteľovi karty.

Tachografovú kartu preto používa rozhranie jednotky vozidla. Môže ju používať každé čítacie zariadenie karty (napr. osobný počítač), ktoré má neobmedzené prístupové práva k čítaniu akýchkoľvek užívateľských dát.

Počas konečnej fázy cyklu životnosti tachografovej karty (fáza 7 cyklu životnosti podľa popisu v (ES PP)), môžu užívateľské dáta na kartu písať len jednotky vozidla.

Funkčné požiadavky na tachografovú kartu sú špecifikované v hlavnej časti prílohe I B a v doplnku 2.

3.2 ***Cyklus životnosti tachografovej karty***

Typický cyklus životnosti tachografovej karty zodpovedá cyklu životnosti inteligentnej karty, ktorý je popísaný v (ES PP).

3.3 ***Bezpečnostné riziká***

Okrem bezpečnostných rizík uvedených v (ES PP) a (IC PP), môže byť tachografová karta vystavená týmto rizikám:

3.3.1 Konečné ciele

Konečným cieľom útokov bude zmena užívateľských dát uložených v TOE.

T.Ident_Data Úspešná zmena identifikačných dát uložených v TOE (napr. typ karty alebo dátum skončenia platnosti alebo identifikačné dáta držiteľa karty) by umožnila podvodné použitie TOE a ohrozila by globálny bezpečnostný cieľ systému.

T.Activity_Data Úspešná zmena dát o činnosti uchovávaných v TOE by ohrozila bezpečnosť TOE.

T.Data_Exchange Úspešná zmena dát o činnosti (doplnenie, vymazanie, zmena) počas importu alebo exportu by ohrozila bezpečnosť TOE.

3.3.2 Cesty útoku

Útoky na TOE môžu byť tieto:

– pokusy o nelegálne získanie znalostí o konštrukcii hardwaru a softwaru TOE a najmä o jeho bezpečnostných funkciách alebo bezpečnostných dátach. Nelegálne znalosti sa môžu získať útokom na materiály konštruktéra alebo výrobcu (krádežou, podplácaním, ...) alebo priamym skúmaním TOE (fyzické skúšky, interferenčné analýzy).

– využitie slabých miest v konštrukcii prípadne v realizácii TOE (využitie chýb v hardware, software, prenosových porúch, chýb TOE vyvolaných vonkajším prostredím, využitie slabých miest v bezpečnostných funkciách ako sú autentifikačné postupy, kontrola prístupu k dátam, kryptografické operácie, ...),

– manipulácia s TOE alebo jeho bezpečnostnými funkciami pomocou fyzických, elektrických alebo logických útokov alebo ich kombináciou.

3.4 ***Bezpečnostné ciele***

Hlavným bezpečnostným cieľom celého systému digitálneho tachografu je toto:

O.Main Dáta kontrolované kontrolnými orgánmi musia byť dostupné a musia plne a presne odrážať činnosti kontrolovaných vodičov a vozidiel v čase vedenia vozidla, práce, pohotovosti a odpočinku ako aj rýchlosť vozidla.

Preto je bezpečnostným cieľom TOE, ktorým prispieva k tomuto globálnemu bezpečnostnému cieľu, nasledovné:

O.Card_Idetification_Data TOE musí uchovávať identifikačné dáta karty a identifikačné dáta držiteľa karty, uložené počas procesu personalizácie karty,

O.Card_Activity_Storage TOE musí uchovávať užívateľské dáta ukladané na kartu jednotkami vozidla.

3.5 ***Informačno–technické bezpečnostné ciele***

Okrem všeobecných bezpečnostných cieľov inteligentnej karty uvedených v (ES PP) a (IC PP), špecifické IT bezpečnostné ciele TOE, ktoré prispievajú k hlavnému bezpečnostnému cieľu počas jeho konečnej fázy cyklu životnosti, sú tieto:

O.Data_Access TOE musí obmedziť prístupové práva k zápisovému prístupu k užívateľským dátam na oprávnené jednotky vozidla,

O.Data_Communications TOE musí podporovať bezpečné komunikačné protokoly a postupy medzi kartou a rozhraním karty, keď si to aplikácia vyžaduje.

3.6 ***Fyzické, personálne alebo postupové prostriedky***

Fyzické, personálne alebo postupové požiadavky, ktoré prispievajú k bezpečnosti TOE sú uvedené v (ES PP) a (IC PP) (kapitoly týkajúce sa bezpečnostných cieľov pre prostredie).

4. **Bezpečnostné vynucovacie funkcie**

Tento odsek bližšie špecifikuje niektoré povolené operácie ako je napr. priraďovanie alebo voľba (ES PP) a stanovuje doplnkové funkčné požiadavky.

4.1 ***Dodržanie ochranných profilov***

CPP_301 TOE musí byť zhodné s (IC PP).

CPP_302 TOE musí byť zhodné s (ES PP) ako je bližšie špecifikované ďalej.

4.2 ***Identifikácia a autentifikácia užívateľa***

Karta musí identifikovať prístrojovú jednotku, v ktorej je vložená a rozpoznať, či ide o autentifikovanú jednotku vozidla alebo nie. Karta môže exportovať akékoľvek užívateľské dáta bez ohľadu na pripojenú prístrojovú jednotku, s výnimkou kontrolnej karty, ktorá môže exportovať identifikačné dáta držiteľa karty len na autentifikovanú jednotku vozidla (tak sa kontrolór prečítaním mena na displeji alebo na výtlačku ubezpečí, že jednotka vozidla nie je falošná).

4.2.1 *Identifikácia užívateľa*

Priradenie (FIA_UID.1.1) *Zoznam TSF sprostredkovaných akcií*: žiadny

Priradenie (FIA_ATD.1.1) *Zoznam bezpečnostných atribútov:*

USER_GROUP VEHICLE_UNIT, NON_VEHICLE_UNIT,

USER_ID registračné číslo vozidla (VRN) a kód členského štátu registrácie (USER_ID je známy len pre USER_GROUP = VEHICLE_UNIT)

4.2.2 *Autentifikácia užívateľa*

Priradenie (FIA_UAU.1.1) *Zoznam TSF sprostredkovaných akcií*:

– karta vodiča a dielenská karta: export užívateľských dát s bezpečnostnými atribútmi (kartové dáta – sťahovacie (prenosové) funkcie)),

– kontrolná karta: export užívateľských dát bez bezpečnostných atribútov s výnimkou identifikačných dát držiteľa karty.

UIA_301 Autentifikácia jednotky vozidla sa vykoná pomocou dôkazu o tom, že obsahuje bezpečnostné dáta, ktoré mohol distribuovať len systém.

Voľba (FIA_UAU.3.1 a FIA_UAU.3.2): zabrániť

Priradenie (FIA_UAU.4.1) *Identifikovaný(é) autentifikačný(é) mechanizmus(y)*: akýkoľvek autentifikačný mechanizmus.

UIA_302 Dielenská karta poskytuje doplnkový autentifikačný mechanizmus tým, že kontroluje PIN kód (tento mechanizmus je určený pre jednotku vozidla aby overila identitu držiteľa karty, nie je určená na ochranu obsahu dielenskej karty).

4.2.3 *Chybná autentifikácia*

Nasledovné priradenia popisujú reakciu karty na každú jednotlivú chybnú autentifikáciu užívateľa.

Priradenie (FIA_AFL.1.1) *Číslo: 1, zoznam autentifikačných udalostí:* autentifikácia rozhrania karty.

Priradenie (FIA_AFL.1.2) *zoznam akcií*:

– varovanie pripojenej prístrojovej jednotky,

– predpokladá sa, že užívateľ je NON_VEHICLE_UNIT.

Nasledovné priradenia popisujú reakciu karty v prípade chyby doplnkového autentifikačného mechanizmu podľa požiadavky UIA_302.

Priradenie (FIA_AFL.1.1) *Číslo 5, zoznam autentifikačných udalostí:* kontroly PIN–u (dielenská karta).

Priradenie (FIA_AFL.1.2) *zoznam akcií*:

– varovanie pripojenej prístrojovej jednotky,

– zablokovanie postupu kontroly PIN–u tak, že každý ďalší pokus bude chybný,

– možnosť oznámiť ďalšiemu užívateľovi dôvody zablokovania.

4.3 ***Kontrola prístupu***

4.3.1 *Opatrenia na kontrolu prístupu*

Počas konečnej fázy svojho cyklu životnosti, je tachografová karta predmetom bezpečnostnej funkcie (SFP) pre jednoduchú kontrolu prístupu s označením AC_SFP.

Priradenie (FDP_ACC.2.1) *Kontrola prístupu* SFP: AC_SFP

4.3.2 *Funkcie kontroly prístupu*

Priradenie (FDP_ACF.1.1) *Kontrola prístupu* SFP: AC_SFP

Priradenie (FDP_ACF.1.1) *Menované skupiny bezpečnostných atribútov:* USER_GROUP.

Priradenie (FDP_ACF.1.2) *Pravidlá riadiace prístup medzi kontrolované subjekty a objekty, s použitím kontrolovaných operácií u kontrolovaných objektov:*

GENERAL_READ:	Užívateľské dáta môže čítať z TOE každý užívateľ, s výnimkou identifikačných dát držiteľa karty, ktoré sa môžu čítať z kontrolných kariet len prostredníctvom VEHICLE_UNIT.
IDENTIF_WRITE:	Identifikačné dáta sa môžu zapísať len raz a pred skončením fázy 6 cyklu životnosti karty. Žiadny užívateľ nesmie zapisovať alebo meniť identifikačné dáta počas konečnej fázy cyklu životnosti karty.
ACTIVITY_WRITE:	Dáta o činnostiach môže do TOE zapísať len VEHICLE_UNIT.
SOFT_UPGRADE:	Žiadny užívateľ nesmie modernizovať software TOE.
FILE_STRUCTURE:	Štruktúra súboru a prístupové podmienky sa vytvoria pred skončením fázy 6 cyklu životnosti TOE a potom sa zablokujú pred akoukoľvek budúcou zmenou alebo vymazaním zo strany ktoréhokoľvek užívateľa.

4.4 ***Sledovateľnosť***

ACT_301 TOE musí vo svojej pamäti uchovávať svoje identifikačné dáta.

ACT_302 Musí existovať údaj o čase a dátume personalizácie TOE. Tento údaj sa nesmie dať zmeniť

4.5 ***Audit***

TOE musí monitorovať udalosti, ktoré znamenajú potenciálne ohrozenie jeho bezpečnosti.

Priradenie (FAU_SAA.1.2) *Podmnožina definovaných auditu podliehajúcich udalostí*:

– chybná autentifikácia držiteľa karty (5 po sebe idúcich neúspešných kontrol PIN–u),

– chyba pri samoskúške,

– chyba integrity uložených dát,

– chyba integrity dát o činnosti.

4.6 ***Presnosť***

4.6.1 *Integrita uložených dát*

Priradenie (FDP_SDI.2.2) *Prijaté opatrenia*: varovanie pripojenej prístrojovej jednotky.

4.6.2 *Autentifikácia základných dát*

Priradenie (FDP_DAU.1.1) *Zoznam objektov alebo druhov informácií*: dáta o činnosti.

Priradenie (FDP_DAU.1.2) *Zoznam subjektov:* ľubovolných.

4.7 ***Spoľahlivosť služby***

4.7.1 *Skúšky*

Voľba (FPT_TST.1.1): pri prvom zapnutí, pravidelne počas bežnej prevádzky.

Poznámka: Pri prvom zapnutí znamená predtým, než sa vykoná kód (a nie nevyhnutne počas odpovede na postup resetovania).

RLB_301 Samoskúšky TOE zahŕňajú overenie integrity každého softwarového kódu, ktorý nie je uložený v ROM.

RLB_302 Po zistení chyby pri samoskúške TSF varuje pripojenú prístrojovú jednotku.

RLB_303 Po dokončení OS skúšky, všetky špeciálne skúšobné príkazy a kroky sa deaktivujú alebo odstránia. Nesmie byť možné prepisovať tieto riadiace prvky a znovu ich aktivovať za účelom ďalšieho použitia. K príkazu spojenému výlučne s jedným štádiom cyklu životnosti, nesmie byť nikdy prístup počas iného štádia.

4.7.2 *Software*

RLB_304 Nesmie existovať možnosť analyzovať, ladiť alebo meniť software TOE pri praktickom používaní.

RLB_305 Vstupy z vonkajších zdrojov nesmú byť akceptované ako vykonávací kód.

4.7.3 *Napájanie*

RLB_306 TOE musí zachovávať bezpečnostný stav počas prerušenia alebo zmien napájania.

4.7.4 *Podmienky resetovania*

RLB_307 V prípade prerušenia napájania (alebo ak nastane zmena v napájaní) TOE alebo ak sa prenos zastaví pred dokončením, alebo pri ktorejkoľvek inej podmienke resetovania, sa TOE musí resetovať.

4.8 ***Výmena dát***

4.8.1 *Výmena dát s jednotkou vozidla*

DEX_301 TOE overí integritu a autenticitu dát importovaných z jednotky vozidla.

DEX_302 Po zistení chyby v integrite dát importovaných z jednotky vozidla TOE:

– varuje prístrojovú jednotku exportujúcu dáta,

– nepoužije dáta.

DEX_303 TOE exportuje užívateľské dáta na jednotku vozidla s príslušnými bezpečnostnými atribútmi tak, aby jednotka vozidla bola schopná overiť integritu a autenticitu prijatých dát.

4.8.2 *Export dát na mimovozidlovú jednotku (funkcia sťahovania dát)*

DEX_304 TOE musí byť schopný generovať dôkaz o pôvode dát sťahovaných na vonkajšie médium.

DEX_305 TOE musí byť schopný príjemcovi preukázať spôsobilosť na overenie dôkazu o pôvode dát sťahovaných na vonkajšie médium.

DEX_306 TOE musí byť schopný sťahovať dáta na vonkajšie médium s príslušnými bezpečnostnými atribútmi tak, aby sa mohla overiť integrita sťahovaných dát.

4.9 ***Kryptografická podpora***

CSP_301 Ak TSF generuje kryptografické kľúče, musí to byť v súlade so špecifikovaným algoritmom generovania kryptografického kľúča a špecifikovanou veľkosťou kryptografického kľúča. Generované kryptografické kľúče relácie musia mať limitovaný počet (stanoví výrobca a nesmie byť väčší než 240) možných použití.

CSP_302 Ak TSF distribuuje kryptografické kľúče, musí to byť v súlade so špecifikovanými metódami distribúcie kryptografického kľúča.

5. **Definícia bezpečnostných mechanizmov**

Požadované bezpečnostné mechanizmy sú špecifikované v doplnku 11.

Všetky ostatné bezpečnostné mechanizmy musí určiť výrobca TOE.

6. **Minimálna odolnosť bezpečnostných mechanizmov**

Minimálna odolnosť bezpečnostných mechanizmov pre tachografovú kartu je **Vysoká** podľa definície v (ITSEC).

7. **Úroveň ručenia**

Cieľová úroveň ručenia pre tachografovú kartu je ITSEC úroveň **E3** podľa definície v (ITSEC).

8. **Základný princíp**

Základný princíp doplnkových SEF je založený na nasledovných maticiach, ktoré udávajú:

– ktoré SEF sú vystavené ktorým bezpečnostným rizikám,

– ktoré SEF spĺňajú ktoré IT bezpečnostné ciele.

	Bezpečnostné riziká											IT ciele								
	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.FLAW*	O.DIS_MECHANISM2	O.DIS_MEMORY*	O.MOD_MEMORY*	Data_Access	Secured_Communications
UIA_301 Autentifikačné prostriedky																			x	
UIA_302 Kontrola PIN–u																			x	
ACT_301 Identifikačné dáta																				
ACT_302 Personalizačné dáta																				
RLB_301 Integrita softwaru												x		x						
RLB_302 Samoskúšky												x		x						
RLB_303 Výrobné skúšky					x	x						x		x						
RLB_304 Analýza softwaru					x		x	x				x		x						
RLB_305 Softwarový vstup					x	x		x				x		x						
RLB_306 Napájanie									x	x		x		x						
RLB_307 Resetovanie												x		x						

	Bezpečnostné riziká											IT ciele								
	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.FLAW*	O.DIS_MECHANISM2	O.DIS_MEMORY*	O.MOD_MEMORY*	Data_Access	Secured_Communications
DEX_301 Bezpečný import dát											x									x
DEX_302 Bezpečný import dát											x									x
DEX_303 Bezpečný export dát na JV											x									x
DEX_304 Dôkaz o pôvode											x									x
DEX_305 Dôkaz o pôvode											x									x
DEX_306 Bezpečný export dát na externé médium											x									x
CSP_301 Generovanie kľúča												x								x
CSP_302 Distribúcia kľúča												x								x

Doplnok 11

SPOLOČNÉ BEZPEČNOSTNÉ MECHANIZMY

OBSAH

1. VŠEOBECNE

Tento doplnok špecifikuje bezpečnostné mechanizmy, ktoré zabezpečujú:

– vzájomnú autentifikáciu medzi JV a tachografovými kartami, vrátane odsúhlasenia relačného kľúča,

– dôvernosť, integritu a autentifikáciu dát prenášaných medzi JV a tachografovými kartami,

– integritu a autentifikáciu dát sťahovaných z JV na vonkajšie pamäťové médium,

– integritu a autentifikáciu dát sťahovaných z tachografových kariet na vonkajšie pamäťové médium.

1.1 **Referenčné dokumenty**

V tomto doplnku sú použité tieto referenčné dokumenty:

SHA–1	National Institute of Standards and Technology (NIST). FIPS Publication 180–1: Secure Hash Standard. April 1995
PKCS1	RSA Laboratories. PKCS # 1: RSA Encryption Standard. Version 2.0. Oktober 1998
TDES	National Institute of Standards and Technology (NIST). FIPS Publication 46–3: Data Encryption Standard. Draft 1999
TDES–OP	ANSI X9.52, Triple Data Encryption Algorithm Modes of Operation. 1998
ISO/IEC 7816–4	Information technology – Identification cards – Integrated circuit(s) cards with contacts – Part 4: Interindustry commands for interexchange. First edition: 1995 + Amendment 1: 1997 (Informačné technológie – Identifikačné karty – Karty s integrovanými obvodmi a s kontaktmi – Časť 4: Medziodborové príkazy pre výmenu. Prvé vydanie: 1995 + zmeny 1:1997)
ISO/IEC 7816–6	Information technology – Identification cards – Integrated circuit(s) cards with contacts – Part 6: Interindustry data elements. First Edition: 1996 + Cor 1: 1998 (Informačné technológie – Identifikačné karty – Karty s integrovanými obvodmi a s kontaktmi – Časť 6: Medziodborové dátové prvky. Prvé vydanie: 1996 + cor. 1:1998)
ISO/IEC 7816–8	Information technology – Identification cards – Integrated circuit(s) cards with contacts – Part 8: Security related interindustry commands. First Edition: 1999 (Informačné technológie – Identifikačné karty – Karty s integrovanými obvodmi a s kontaktmi – Časť 8: Medziodborové príkazy vzťahujúce sa k bezpečnosti. Prvé vydanie: 1999)
ISO/IEC 9796–2	Information Technology – Security techniques – Digital signature schemes giving message recovery – Part 2: Mechanisms using a hash function. First edition: 1997. (Informačná technológia – Bezpečnostné techniky – Mechanizmy digitálneho podpisu s opätovným získaním správy – Časť 2: Mechanizmy používajúce hash funkciu. Prvé vydanie 1997.)
ISO/IEC 9798–3	Information Technology – Security techniques – Entity authentication mechanisms – Part 3: Entity authentication using a public key algorithm. Second edition 1998. (Informačná technológia – Bezpečnostné techniky – Mechanizmus overovania entít – Časť 3: Overovanie entít pomocou algoritmu verejného kľúča. Druhé vydanie 1998)
ISO 16844–3	Road vehicles – Tachograph systems – Part 3: Motion Sensor Interface. (Cestné vozidlá – Tachografové systémy – Rozhranie snímača pohybu. WD 3– 20/05/99).

1.2 **Notácie a skratky**

V tomto doplnku sa použili nasledovné notácie a skratky:

(K_a, K_b, K_c)	zväzok kľúčov, ktorý používa riple Data Encryption Algorithm
CA	Certification authority (certifikačný orgán)
CAR	Certification authority reference (referencia certifikačného orgánu)
CC	Cryptographic checksum (kryptografický kontrolný súčet)

CG	Cryptogram (kryptogram)
CH	Command header (záhlavie príkazu)
CHA	Certificate holder authorisation (autorizácia držiteľa osvedčenia)
CHR	Certificate holder reference (referencia držiteľa osvedčenia)
D()	dekódovanie s DES
DE	dátový prvok
DO	dátový objekt
d	RSA súkromný kľúč, súkromný exponent
e	RSA verejný kľúč, verejný exponent
E()	kódovanie s DES
EQT	Equipment (zariadenie)
Hash()	hash hodnota, výstup hash–u
Hash	hash funkcia
KID	Key identifier (identifikátor kľúča)
Km	TDES kľúč. Hlavný kľúč podľa ISO 16844–3
Km_{vu}	TDES kľúč zavedený v jednotkách vozidla
Km_{wc}	TDES kľúč zavedený v dielenských kartách
m	representant správy, celé číslo medzi 0 a *n*–1
n	RSA kľúče, modulus
PB	Padding bytes (vyplňovacie bajty)
PI	Padding indicator byte (použitie v kryptograme pre dôvernosť DO)
PV	Plain value (čitateľná hodnota)
s	reprezentant podpisu, celé číslo medzi 0 a *n*–1
SSC	Send sequence counter (počítadlo odoslaných sekvencií)
SM	Secure messaging
TCBC	TDEA prevádzkový režim Cipher Block Chaining
TDEA	Triple data encryption algorithm (algoritmus kódovania trojnásobných dát)
TLV	Tag length value (dĺžková hodnota tag–u)
VU	Vehicle Unit VU (jednotka vozidla JV)
X.C	osvedčenie užívateľa X vydané certifikačným orgánom
X.CA	certifikačný orgán užívateľa X
$X.CA.PK_oX.C$	priebeh rozbaľovania osvedčenia aby sa získal verejný kľúč. Ide o infix–operátor, ktorého ľavý operand je verejným kľúčom certifikačného orgánu, a pravý operand je osvedčením vydaným týmto certifikačným orgánom. Výsledkom je verejný kľúč užívateľa X, ktorého osvedčenie predstavuje pravý operand
X.PK	verejný kľúč užívateľa X
X.PK[I]	RSA šifrovanie niektorých informácií I, s použitím verejného kľúča užívateľa X
X.SK	RSA súkromný kľúč užívateľa X
X.SK[I]	RSA šifrovanie niektorých informácií I, s použitím súkromného kľúča užívateľa X

'xx' hexadecimálna hodnota

|| operátor zreťazenia.

2. KRYPTOGRAFICKÉ SYSTÉMY A ALGORITMY

2.1 **Kryptografické systémy**

CSM_001 Jednotky vozidla a tachografové karty používajú klasický RSA kryptografický systém verejného kľúča tak aby boli k dispozícii tieto bezpečnostné mechanizmy:

– autentifikácia medzi jednotkami vozidla a kartami,

– prenos Triple–DES–relačných kľúčov medzi jednotkami vozidla a tachografovými kartami,

– digitálny podpis dát sťahovaných z jednotiek vozidla alebo tachografových kariet na vonkajšie médiá.

CSM_002 Jednotky vozidla a tachografové karty používajú symetrický Triple–DES kryptografický systém tak, aby bol k dispozícii mechanizmus pre zabezpečenie integrity dát počas výmeny užívateľských dát medzi jednotkami vozidla a tachografovými kartami a aby bola prípadne zabezpečená dôvernosť výmeny dát medzi jednotkami vozidla a tachografovými kartami.

2.2 **Kryptografické algoritmy**

2.2.1 ***RSA algoritmus***

CSM_003 RSA algoritmus je úplne definovaný nasledovnými vzťahmi:

$$X.SK[m] = s = m^d \bmod n$$
$$X.PK[s] = m = s^e \bmod n$$

Podrobnejší popis RSA funkcie sa nachádza v referenčnom dokumente (PKCS1).

Verejný exponent "***e***" pre výpočty RSA sa vo všetkých generovaných RSA kľúčoch nebude rovnať 2.

2.2.2 ***Hash algoritmus***

CSM_004 Mechanizmus digitálneho podpisu používa SHA–1–Hash algoritmus podľa definície v referenčnom dokumente (SHA–1).

2.2.3 ***Algoritmus kódovania dát***

CSM_005 Algoritmy založené na DES sa používajú v prevádzkovom režime Cipher Block Chaining.

3. KĽÚČE A OSVEDČENIA

3.1 **Generovanie a distribúcia kľúčov**

3.1.1 ***Generovanie a distribúcia RSA kľúčov***

CSM_006 RSA kľúče sa generujú na troch funkčne hierarchických úrovniach:

– európska úroveň,

– úroveň členského štátu,

– úroveň zariadenia.

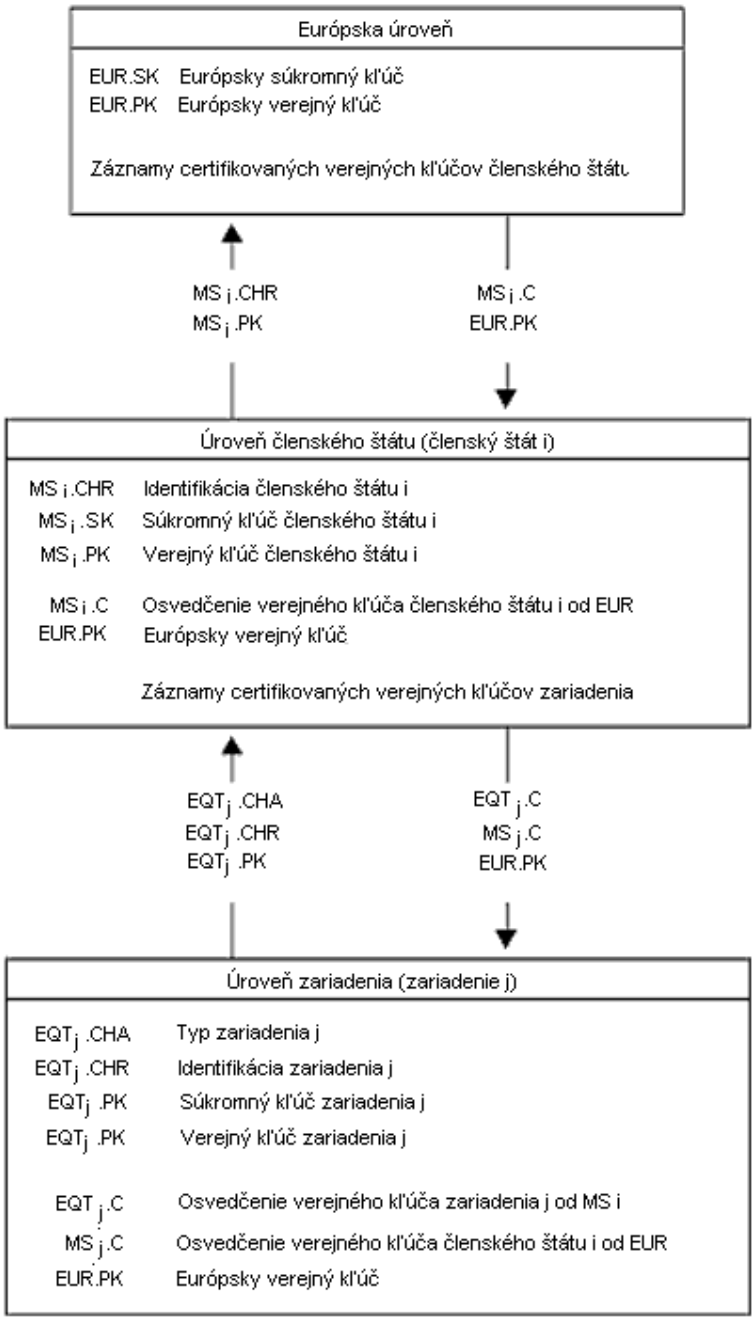
CSM_007 Na európskej úrovni sa generuje jeden európsky kľúčový pár (EUR.SK a EUR.PK). Európsky súkromný kľúč sa používa na certifikovanie verejných kľúčov členského štátu. Musia sa uchovávať záznamy všetkých certifikovaných kľúčov. Tieto úlohy plní Európsky certifikačný orgán podliehajúci Európskej komisii.

CSM_008 Na úrovni členského štátu sa generuje jeden kľúčový pár členského štátu (MS.SK a MS.PK). Verejné kľúče členského štátu musia byť certifikované Európskym certifikačným orgánom. Súkromný kľúč členského štátu sa používa na certifikovanie verejných kľúčov zavedených do zariadenia (jednotka vozidla alebo tachografová karta). Musia sa uchovávať záznamy všetkých certifikovaných verejných kľúčov spolu s identifikáciou zariadenia, pre ktoré sú určené. Tieto úlohy plní certifikačný orgán členského štátu. Členský štát môže pravidelne meniť svoj kľúčový pár.

CSM_009 Na úrovni zariadenia sa generuje jeden kľúčový pár (EQT.SK a EQT.PK) a zavedie sa do každého zariadenia. Verejné kľúče zariadenia musia byť certifikované certifikačným orgánom členského štátu. Tieto úlohy môžu plniť výrobcovia zariadenia, montéri zariadenia alebo certifikačný orgán členského štátu. Tento kľúčový pár sa používa na autentifikáciu, na digitálny podpis ako aj na šifrovacie služby.

CSM_010 Dôvernosť súkromných kľúčov sa musí zachovať počas generovania, prenosu a uloženia.

Na nasledovnom obrázku je zhrnutý dátový tok tohto procesu:



3.1.2 ***RSA skúšobný kľúč***

CSM_011 Na účely skúšky zariadenia (vrátane skúšok interoperability) Európsky certifikačný orgán generuje rôzne jednotlivé európske skúšobné kľúčové páry a aspoň dva skúšobné kľúčové páry členského štátu, ktorého verejné kľúče musia byť certifikované Európskym súkromným skúšobným kľúčom. Výrobcovia musia zaviesť do zariadenia, podliehajúceho typovým schvaľovacím testom, skúšobné kľúče certifikované jedným z týchto skúšobných kľúčov členského štátu.

3.1.3 ***Kľúč snímača pohybu***

Dôvernosť troch TDES kľúčov popísaný nižšie sa musí príslušne uchovávať počas generovania, prípadného prenosu a uloženia.

Na zaručenie zhody záznamového zariadenia s ISO 16844, Európsky certifikačný orgán a certifikačné orgány členského štátu musia okrem toho zabezpečiť toto:

CSM_036 Európsky certifikačný orgán generuje Km_{VU} a Km_{wc}, dva nezávislé a jednorazové Triple–DES kľúče a generuje Km ako:

$$Km = Km_{VU} \text{ XOR } Km_{WC}$$

Európsky certifikačný orgán pomocou vhodne zabezpečeného postupu odošle tieto kľúče na požiadanie certifikačným orgánom členských štátov.

CSM_037 Certifikačné orgány členských štátov:

- použijú Km na zakódovanie dát snímača pohybu, ktoré vyžadujú výrobcovia snímača pohybu (dáta kódované s Km sú definované v ISO 16844–3),
- pošle Km_{VU} pomocou vhodne zabezpečeného postupu výrobcom jednotky vozidla, za účelom jeho zavedenia do jednotiek vozidla,
- zabezpečí, aby Km_{WC} bol zavedený vo všetkých dielenských kartách (SensorInstallationSecData v základnom súbore Sensor_Installation_Data) počas personalizácie karty.

3.1.4 ***Generovanie a distribúcia T–DES relačných kľúčov***

CSM_012 Jednotky vozidla a tachografové karty si musia, ako časť vzájomného autentifikačného procesu, generovať a vymieňať dáta nevyhnutné na zhotovenie spoločného Triple–DES relačného kľúča. Táto výmena dát musí byť chránená z hľadiska dôvernosti pomocou RSA kódovacieho mechanizmu.

CSM_013 Tento kľúč sa používa na všetky následné kryptografické operácie s použitím secure messaging. Jeho platnosť skončí na konci relácie (vytiahnutie karty alebo resetovanie karty) a/alebo po 240. použití (jedno použitie kľúča = jeden príkaz používajúci secure messaging posielaný na kartu a príslušná odpoveď).

3.2 **Kľúče**

CSM_014 RSA kľúče musia mať (na ktorejkoľvek úrovni) túto dĺžku: modul ***n*** 1024 bitov, verejný exponent ***e*** maximálne 64 bitov, súkromný exponent ***d*** 1024 bitov.

CSM_015 Triple–DES kľúč musí mať formu (K_a, K_b, K_a) kde K_a a K_b sú nezávislé 64 bitov dlhé kľúče. Nesmie byť stanovená žiadna paritná chyba detekčných bitov.

3.3 **Osvedčenia**

CSM_016 Osvedčenia RSA verejného kľúča musia byť osvedčeniami zodpovedajúcimi definícii "non self–descriptive" a "Card Verifiavle" (referenčný dokument: ISO/IEC 7816–8).

3.3.1 ***Obsah osvedčení***

CSM_017 Osvedčenia RSA verejného kľúča sú zhotovené z nasledovných dát v tomto poradí:

Dáta	Formát	Bajty	Poznámky
CPI	INTEGER	1	Certificate profile identifier (identifikátor profilu certifikátu '01' v tejto verzii)
CAR	OCTET STRING	8	Certification authority reference (referencia certifikačného orgánu)
CHA	OCTET STRING	7	Certificate holder authorisation (autorizácia držiteľa osvedčenia)
EOV	TimeReal	4	Certificate end of validity. (koniec platnosti osvedčenia). Nepovinné, ak sa nepoužije vyplní sa s 'FF'
CHR	OCTET STRING	8	Certificate holder reference (referencia držiteľa osvedčenia)
n	OCTET STRING	128	Public key (verejný kľúč) (modul)
e	OCTET STRING	8	Public kKey (verejný exponent)
		164	

Poznámky:

1. "Certificate profile identifier" (identifikátor profilu certifikátu, CPI) ohraničuje presnú štruktúru osvedčenia. Môže sa použiť ako vnútorný identifikátor zariadenia príslušného zoznamu záhlaví, ktorý popisuje zreťazenie dátových prvkov vo vnútri osvedčenia.

Zoznam záhlaví pre toto osvedčenie je takýto:

'4D'	'16'	'5F 29'	'01'	'042'	'08'	'5F 4B'	'07'	'5F 24'	'04'	'5F 20'	'08'	'7F 49'	'05'	'81'	'81 80'	'82'	'08'
Tag pre rozšírený zoznam záhlaví	Dĺžka zoznamu záhlaví	CPI Tag	CPI dĺžka	CAT Tag	CAR dĺžka	CHA Tag	CHA dĺžka	EOV Tag	EOV dĺžka	CHR Tag	CHR dĺžka	Tag pre verejný kľúč (konštruovaný)	Dĺžka následného DOs	Tag modulu	Dĺžka modulu	Tag pre verejný exponent	Dĺžka verejného exponentu

2. "Certification authority reference" (Referencia certifikačného orgánu, CAR) má za účel identifikovať orgán vydávajúci osvedčenie takým spôsobom, aby sa dátový prvok mohol použiť v rovnakom čase ako Authority Key Identifier (identifikátor kľúča orgánu) na špecifikáciu verejného kľúča certifikačného orgánu (kódovanie, pozri Key Identifier nižšie).

3. "Certificate holder authorisation" ((autorizácia držiteľa osvedčenia, CHA) sa používa na identifikovanie práv držiteľa osvedčenia. Pozostáva z tachografovej aplikácie ID a typu zariadenia, ktorému je osvedčenie určené (podľa dátového prvku EquipmentType, "00 pre členský štát).

4. "Certificate holder reference (referencia držiteľa osvedčenia, CHR) má za účel identifikovať jednoznačne držiteľa osvedčenia takým spôsobom, aby sa dátový prvok mohol použiť v rovnakom čase ako Subject Key Identifier (identifikátor kľúča subjektu) na špecifikáciu verejného kľúča držiteľa osvedčenia.

5. "Key Identifiers" (identifikátory kľúča) identifikujú držiteľa osvedčenia alebo certifikačné orgány. Sú kódované takto:

   5.1 Zariadenie (JV alebo karta):

Dáta	Sériové číslo zariadenia	Dátum	Typ	Výrobca
DÍžka	4 bajty	2 Bajty	1 bajt	1 bajt
Hodnota	Celé číslo	mm rr BCD kódovanie	Špecifické pre výrobcu	Kód výrobcu

   V prípade JV, výrobca pri žiadosti o osvedčenia môže alebo nemusí poznať identifikáciu zariadenia, v ktorom má byť kľúč zavedený.

   V prvom prípade výrobca pošle identifikáciu zariadenia s verejným kľúčom za účelom certifikácie certifikačnému orgánu svojho členského štátu. Osvedčenie potom bude obsahovať identifikáciu zariadenia a výrobca musí zabezpečiť, aby boli kľúče a osvedčenia priložené k príslušnému zariadeniu. Key Identifier má formu uvedenú vyššie.

   V druhom prípade výrobca musí jednoznačne identifikovať každú žiadosť o osvedčenie a poslať túto identifikáciu s verejným kľúčom za účelom certifikácie certifikačnému orgánu svojho členského štátu. Osvedčenie potom bude obsahovať identifikáciu žiadosti. Výrobca musí orgánu svojho členského štátu po inštalovaní kľúča v zariadení, oznámiť priradenie kľúča k zariadeniu (t. j. identifikáciu žiadosti o osvedčenie, identifikáciu zariadenia).

Dáta	Sériové číslo žiadosti o osvedčenie	Dátum	Typ	Výrobca
DÍžka	4 bajty	2 Bajty	1 bajt	1 bajt
Hodnota	BCD kódovanie	mm rr BCD kódovanie	'FF'	Kód výrobcu

5.1 Certifikačný orgán:

Dáta	Identifikácia orgánu	Sériové číslo kľúča	Doplňujúce informácie	Identifikátor
Dĺžka	4 bajty	2 Bajty	2 bajty	1 bajt
Hodnota	numerický kód členského štátu– 1 bajt alfanumerický kód členského štátu – 3 bajty	Celé číslo	Doplnkové kódovanie (CA–špecifické) 'FF FF' ak sa nepoužíva	'01'

Sériové číslo kľúča sa používa na rozlíšenie rôznych kľúčov členského štátu v prípade zmeny kľúča.

6. Overovateľom osvedčenia je implicitne známe, že u certifikovaného verejného kľúča ide o RSA kľúč relevantný pre autentifikáciu, overenie digitálneho podpisu a tajné šifrovanie (osvedčenie neobsahuje žiadny identifikátor objektu pre jeho špecifikáciu).

3.3.2 ***Vydané osvedčenia***

CSM_018 Vydané osvedčenie je digitálnym podpisom s čiastočne obnoviteľným obsahom osvedčenie v súlade s ISO/IEC 9796–2, s priloženým "Certification Authority Reference".

$$X.C = X.CA.SK['6A' \| Cr \| \mathit{Hash}(Cc) \| 'BC'] \| C_n \| X.CAR$$

pričom obsah osvedčenia $= Cc = C_r \| C_n$ (106 bajtov, 58 bajtov)

Poznámky:

1. Toto osvedčenie má dĺžku 194 bajtov.
2. CAR skrytá podpisom je tiež priložená k podpisu tak, aby na overenie osvedčenia mohol byť zvolený verejný kľúč certifikačného orgánu.
3. Overovateľovi osvedčenia je implicitne známy algoritmus použitý certifikačným orgánom na podpis osvedčenia.
4. Hlavička zoznamu patriaca vydanému osvedčeniu je takáto:

'7F 21'	'09'	'5F 37'	'81 80'	'5F 38'	'3A'	'42'	'08'
Tag pre CV osvedčenie (konštruovaný)	Dĺžka nasledujúceho DOs	Tag podpisu	Dĺžka podpisu	Zvyšný Tag	Zvyšná dĺžka	CAR Tag	CAR dĺžka

3.3.3 ***Overenie a rozbalenie osvedčenia***

Overenie osvedčenia a rozbalenie pozostáva z overenia podpisu v súlade s ISO/IEC 9796–2, čím sa vyvolá obsah osvedčenia a obsiahnutý verejný kľúč: X.PK = X.CA.PK$_o$X.C a overí sa platnosť osvedčenia.

CSM_019 Zahŕňa tieto kroky:

overenie podpisu a vyvolanie obsahu:

– z X.C vyvolanie Sign, C_n' a CAR': X.C= Sign (128 bajtov) || C_n' (58 bajtov) || CAR' (8 bajtov)

– z CAR' voľba vhodného verejného kľúča certifikačného orgánu (keď už predtým nebola urobená inými prostriedkami)

– otvorenie Sign s verejným CA kľúčom: Sr' = X.CA.PK [Sign]

– kontrola Sr' začína s '6A' a končí s 'BC'

– výpočet Cr' a H' z Sr' = '6A' || C_r' (106 bajtov) || H' (20 bajtov) || 'BC'

– Opätovné zhotovenie obsahu osvedčenia C' = C_r' || C_n',

– kontrola *Hash*(*C*') = H'

Ak sú kontroly pozitívne osvedčenie je pravé a jeho obsah je C'.

Overenie platnosti. Z C':

– ak je to použiteľné, kontrola dátumu skončenia platnosti,

vyvolanie a uloženie verejného kľúča, Key Identifier, Certificate Holder Authorisation a skončenia platnosti osvedčenia z C':

– X.PK = ***n*** || ***e***

– X.KID = CHR

– X.CHA = CHA

– X.EOV = EOV.

4. MECHANIZMUS VZÁJOMNEJ AUTENTIFIKÁCIE

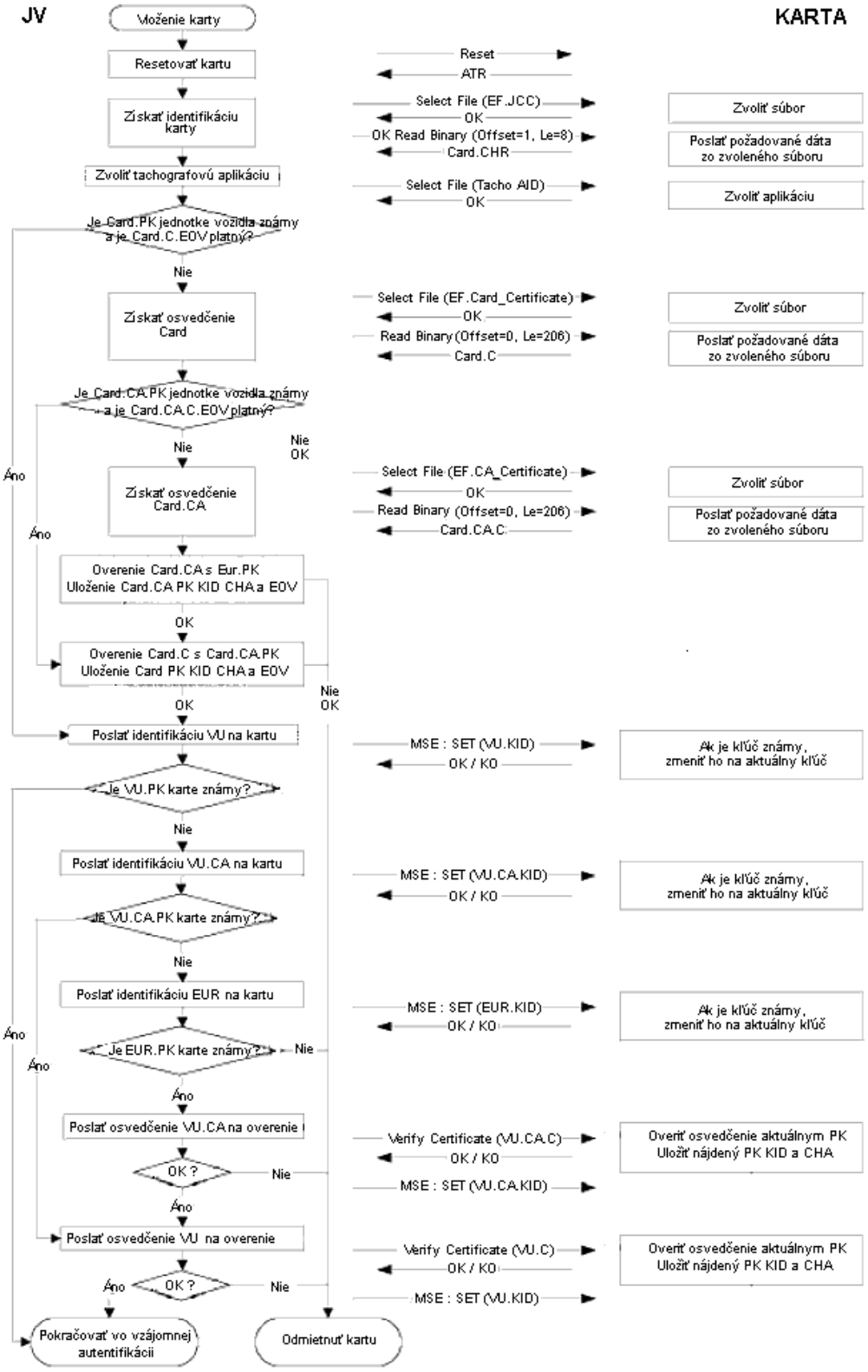
Vzájomná autentifikácia medzi kartami a JV je založená na nasledovných princípoch:

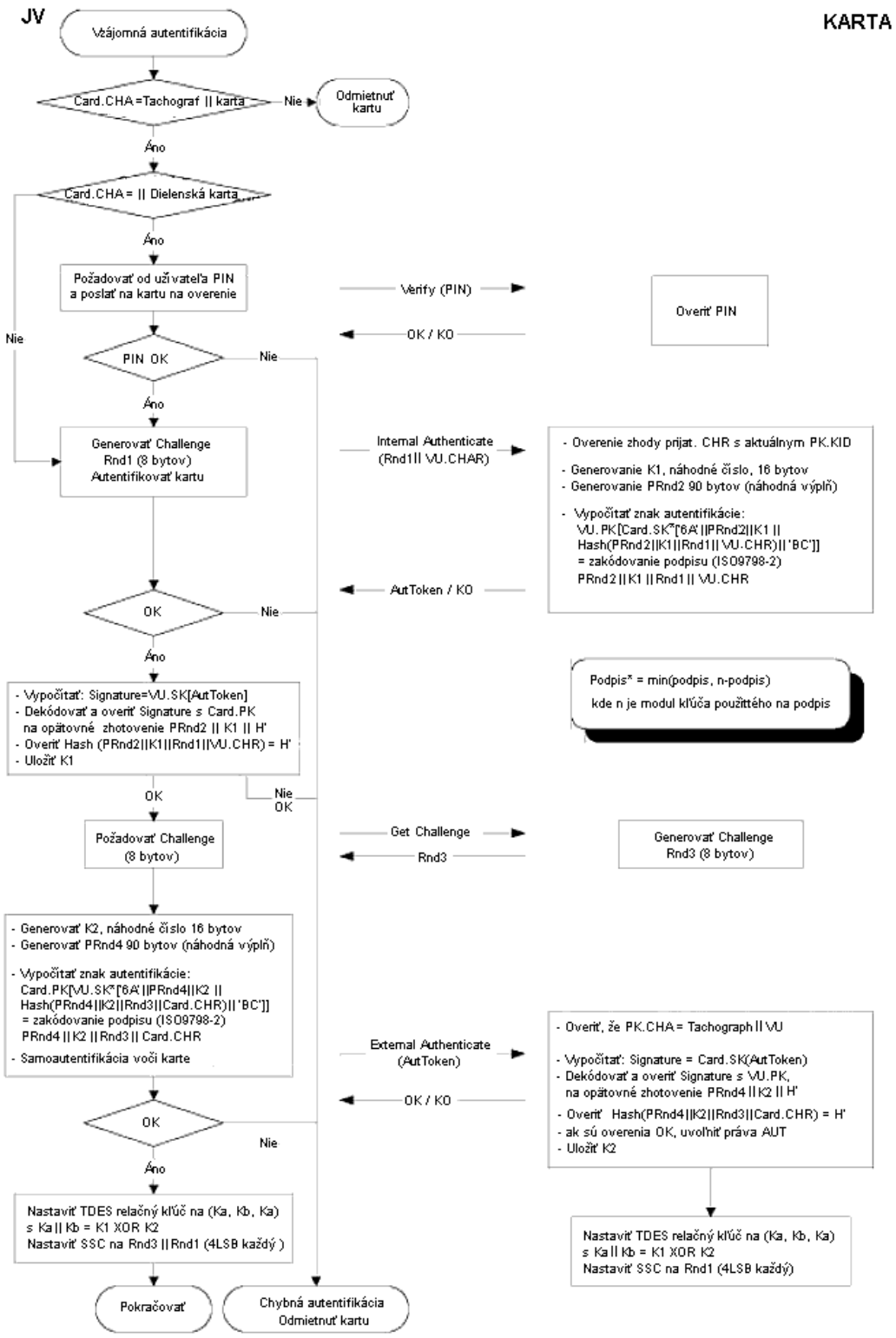
Každá strana preukáže druhej strane, že vlastní platný pár kľúčov, ktorého verejný kľúč bol certifikovaný certifikačným orgánom členského štátu, ktorý samotný bol certifikovaný Európskym certifikačným orgánom.

Preukázanie sa vykoná podpisom náhodného čísla pomocou verejného kľúča poslaného druhej strane, ktorá musí pri overení tohto podpisu vyvolať poslané náhodné číslo.

Mechanizmus spustí JV pri vložení karty. Začne výmenou osvedčení a rozbaľovanie verejných kľúčov a končí zhotovením relačného kľúča.

CSM_20 Použije sa nasledovný protokol (šípky označujú príkazy a vymieňané dáta (pozri doplnok 2)):


JV
KARTA
Vloženie karty
Resetovať kartu
Reset
ATR
Získať identifikáciu karty
Select File (EF.JCC)
OK
Zvoliť súbor
OK Read Binary (Offset=1, Le=8)
Card.CHR
Poslať požadované dáta zo zvoleného súboru
Zvoliť tachografovú aplikáciu
Select File (Tacho AID)
OK
Zvoliť aplikáciu
Je Card.PK jednotke vozidla známy a je Card.C.EOV platný?
Nie
Získať osvedčenie Card
Select File (EF.Card_Certificate)
OK
Zvoliť súbor
Read Binary (Offset=0, Le=206)
Card.C
Poslať požadované dáta zo zvoleného súboru
Je Card.CA.PK jednotke vozidla známy a je Card.CA.C.EOV platný?
Nie
Nie OK
Ano
Získať osvedčenie Card.CA
Select File (EF.CA_Certificate)
OK
Zvoliť súbor
Read Binary (Offset=0, Le=206)
Card.CA.C
Poslať požadované dáta zo zvoleného súboru
Ano
Overenie Card.CA s Eur.PK
Uloženie Card.CA.PK KID CHA a EOV
OK
Overenie Card.C s Card.CA.PK
Uloženie Card PK KID CHA a EOV
Nie OK
OK
Poslať identifikáciu VU na kartu
MSE : SET (VU.KID)
OK / KO
Ak je kľúč známy, zmeniť ho na aktuálny kľúč
Je VU.PK karte známy?
Nie
Poslať identifikáciu VU.CA na kartu
MSE : SET (VU.CA.KID)
OK / KO
Ak je kľúč známy, zmeniť ho na aktuálny kľúč
Je VU.CA.PK karte známy?
Nie
Poslať identifikáciu EUR na kartu
MSE : SET (EUR.KID)
OK / KO
Ak je kľúč známy, zmeniť ho na aktuálny kľúč
Ano
Je EUR.PK karte známy?
Nie
Ano
Ano
Poslať osvedčenie VU.CA na overenie
Verify Certificate (VU.CA.C)
OK / KO
Overiť osvedčenie aktuálnym PK
Uložiť nájdený PK KID a CHA
OK ?
Nie
MSE : SET (VU.CA.KID)
Ano
Poslať osvedčenie VU na overenie
Verify Certificate (VU.C)
OK / KO
Overiť osvedčenie aktuálnym PK
Uložiť nájdený PK KID a CHA
Ano
OK ?
Nie
MSE : SET (VU.KID)
Pokračovať vo vzájomnej autentifikácii
Odmietnuť kartu


JV
KARTA
Vzájomná autentifikácia
Card.CHA=Tachograf || karta
Nie
Odmietnuť kartu
Áno
Card.CHA = || Dielenská karta
Áno
Požadovať od užívateľa PIN a poslať na kartu na overenie
Verify (PIN)
Overiť PIN
OK / KO
Nie
PIN OK
Nie
Áno
Generovať Challenge Rnd1 (8 bytov) Autentifikovať kartu
Internal Authenticate (Rnd1|| VU.CHAR)
- Overenie zhody prijat. CHR s aktuálnym PK.KID
- Generovanie K1, náhodné číslo, 16 bytov
- Generovanie PRnd2 90 bytov (náhodná výplň)
- Vypočítať znak autentifikácie:
VU.PK[Card.SK'['6A'||PRnd2||K1 || Hash(PRnd2||K1||Rnd1|| VU.CHR)||'BC']] = zakódovanie podpisu (ISO9798-2)
PRnd2||K1||Rnd1|| VU.CHR
AutToken / KO
OK
Nie
Áno
Podpis* = min(podpis, n-podpis)
kde n je modul kľúča použittého na podpis
- Vypočítať: Signature=VU.SK[AutToken]
- Dekódovať a overiť Signature s Card.PK na opätovné zhotovenie PRnd2 || K1 || H'
- Overiť Hash (PRnd2||K1||Rnd1||VU.CHR) = H'
- Uložiť K1
OK
Nie
OK
Požadovať Challenge (8 bytov)
Get Challenge
Rnd3
Generovať Challenge Rnd3 (8 bytov)
- Generovať K2, náhodné číslo 16 bytov
- Generovať PRnd4 90 bytov (náhodná výplň)
- Vypočítať znak autentifikácie:
Card.PK[VU.SK'['6A'||PRnd4||K2 || Hash(PRnd4||K2||Rnd3||Card.CHR)||'BC']] = zakódovanie podpisu (ISO9798-2)
PRnd4||K2||Rnd3|| Card.CHR
- Samoautentifikácia voči karte
External Authenticate (AutToken)
- Overiť, že PK.CHA = Tachograph || VU
- Vypočítať: Signature = Card.SK(AutToken)
- Dekódovať a overiť Signature s VU.PK, na opätovné zhotovenie PRnd4||K2||H'
- Overiť Hash(PRnd4||K2||Rnd3||Card.CHR) = H'
- ak sú overenia OK, uvoľniť práva AUT
- Uložiť K2
OK / KO
OK
Nie
Áno
Nastaviť TDES relačný kľúč na (Ka, Kb, Ka)
s Ka|| Kb = K1 XOR K2
Nastaviť SSC na Rnd3 ||Rnd1 (4LSB každý)
Nastaviť TDES relačný kľúč na (Ka, Kb, Ka)
s Ka|| Kb = K1 XOR K2
Nastaviť SSC na Rnd1 (4LSB každý)
Pokračovať
Chybná autentifikácia
Odmietnuť kartu

5. MECHANIZMUS DÔVERNOSTI, INTEGRITY A AUTENTIFIKÁCIE DÁTOVÉHO PRENOSU KARTY JV

5.1 **Secure messaging**

CSM_021 Integrita prenosu dát medzi JV a kartou je chránená prostredníctvom Secure Messaging v súlade s referenčnými dokumentmi (ISO/IEC 7816–4 a ISO/IEC 7816–8).

CSM_022 Keď musia byť dáta počas prenosu chránené, v rámci príkazu alebo odpovede sa k odoslaným dátovým objektom pripojí dátový objekt „Cryptographic Checksum“. Kryptografický kontrolný súčet overuje prijímateľ.

CSM_023 Kryptografický kontrolný súčet dát odosielaných v rámci príkazu integruje záhlavie príkazu a všetky odosielané dáta (= › CLA = ‘0C’ a všetky dáta musia byť obalené tagmi pričom b1 = 1).

CSM_024 Keď odpoveď neobsahuje žiadne dátové pole musia byť bajty týkajúce sa informácií o stave odpovede chránené kryptografickým kontrolným súčtom.

CSM_025 Kryptografický kontrolný súčet musí mať dĺžku štyri bajty.

Štruktúra príkazov a odpovedí pri použití secure messaging je preto nasledovná:

Použité DOs (dátové objekty) sú podmnožinou DOs popísaných v ISO/IEC 7816–4:

Tag	Mnemotechnická skratka	Význam
‘81’	T_{PV}	Čitateľná hodnota nekódovaná v BER–TLV (chránená prostredníctvom CC)
‘97’	T_{LE}	Hodnota Le v nezabezpečenom príkaze (chránená prostredníctvom CC)
‘99’	T_{SW}	Status–Info (chránená prostredníctvom CC)
‘8E’	T_{CC}	Kryptografický kontrolný súčet
‘87’	$T_{PI\ CG}$	Padding Indicator Byte ‖ Cryptogram (čitateľná hodnota nekódovaná v BER–TLV)

Vychádzajúc z nezabezpečeného páru príkaz – odpoveď:

Záhlavie príkazu	Telo príkazu
CLA INS P1 P2	(L_c–pole) (Dátové pole) (L_e–pole)
štyri bajty	L bajty, označené ako B_1 až B_L

Telo odpovede	Telo príkazu
(Dátové pole)	SW1 SW2
L_r dátové bajty	dva bajt

Zodpovedajúci zabezpečený pár príkaz – odpoveď je:

Zabezpečený príkaz:

Záhlavie príkazu	Telo príkazu											
CLA INS P1 P2	(Nové L_c pole)	(Nové dátové pole)										(Nové L_e pole)
‘OC’	Dĺžka nového dátového poľa	T_{PV}	L_{PV}	PV	T_{LE}	L_{LE}	L_e	T_{CC}	L_{CC}	CC		‘00’
		‘81’	L_c	Dátové pole	‘97’	‘01’	L_e	‘8E’	‘04’	CC		

Dáta integrované v kontrolnom súčte = CH || PB || T_{PV} || L_{PV} || PV || T_{LE} || L_{LE} || L_e || PB

PB = padding bytes (80 .. 00) podľa ISO/IEC 7816–4 a ISO 979, metóda 2.

DOs PV a LE sú k dispozícii len keď existujú nejaké zodpovedajúce dáta v nezabezpečenom príkaze.

Zabezpečená odpoveď:

1. Keď dátové pole odpovede nie je prázdne a nemusí byť chránené vzhľadom na dôvernosť dát.

Telo odpovede						Koncový znak odpovede
(Nové dátové pole)						nové SW1 SW2
T_{PV}	L_{PV}	PV	T_{CC}	L_{CC}	CC	
‘81’	L_r	Dátové pole	‘8E’	‘04’	CC	

Dáta integrované v kontrolnom súčte = T_{PV} || L_{PV} || PV || PB

2. Keď dátové pole odpovede nie je prázdne a musí byť chránené vzhľadom na dôvernosť dát.

Telo odpovede						Koncový znak odpovede
(Nové dátové pole)						nové SW1 SW2
$T_{PV\ CG}$	$L_{PI\ CG}$	PI CG	T_{CC}	L_{CC}	CC	
‘87’		PI || CG	‘8E’	‘04’	CC	

Dáta v CG : dáta nekódované v BER–TLV a vyplňovacie bajty.

Dáta integrované v kontrolnom súčte = $T_{PI\ CG}$ || $L_{PI\ CG}$ || PI CG || PB

3. Keď je dátové pole odpovede prázdne.

Telo odpovede						Koncový znak odpovede
(Nové dátové pole)						nové SW1 SW2
T_{SW}	L_{SW}	SW	T_{CC}	L_{CC}	CC	
‘99’	‘02’	Nové SW1 SW2	‘8E’	‘04’	CC	

Dáta integrované v kontrolnom súčte = T_{SW} || L_{SW} || SW || PB

5.2 **Spracovanie chýb secure messaging**

CSM_026 Keď tachografová karta spozná chybu SM pri interpretácii príkazu, potom stavové bajty sa musia vrátiť bez SM. V súlade s ISO/IEC 7816–4 sú na oznámenie SM chýb definované tieto stavové bajty:

’66 88’ chybné overenie kryptografického kontrolného súčtu,

’69 87’ chýbajú očakávané SM dátové objekty,

’69 88’ nesprávne SM dátové objekty.

CSM_027 Keď tachografová karta vráti stavové bajty bez SM DOs alebo s chybné SM DOs, JV musí reláciu ukončiť.

5.3 **Algoritmus výpočtu kryptografických kontrolných súčtov**

CSM_028 Kryptografické kontrolné súčty skonštruované s využitím zvyšných MAC v súlade s ANSI X9.19 s DES:

– východisková etapa: počiatočný kontrolný blok y0 je E(Ka, SSC);

– nasledujúca etapa: kontrolné bloky y1, ..., yn sa vypočítajú s použitím Ka;

– konečná etapa: kryptografický kontrolný súčet sa vypočíta z posledného kontrolného bloku yn takto: E(Ka, D(Kb, yn)).

E() znamená kódovanie s DES a D() znamená dekódovanie s DES.

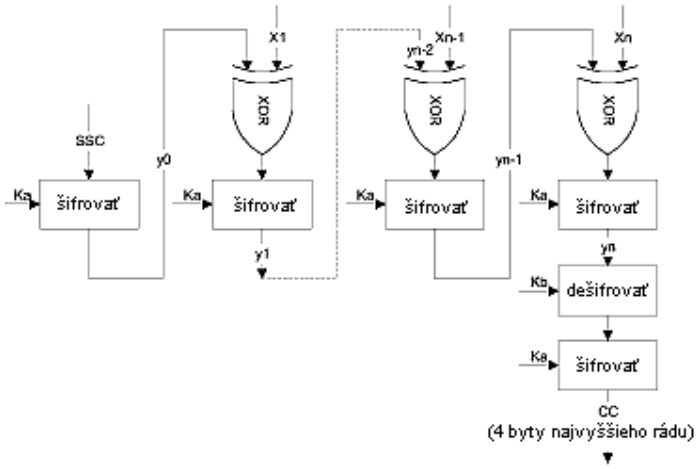
Prenášajú sa štyri bajty nyjvyššieho rádu kryptografického kontrolného súčtu.

CSM_029 Počítadlo odoslaných sekvencií (SSC) sa iniciuje počas postupu odsúhlasovania kľúča takto:

Počiatočné SSC: Rnd3 (4 bajty najnižšieho rádu) || Rnd1 (4 bajty najnižšieho rádu).

CSM_030 Počítadlo odoslaných sekvencií sa zvýši o 1 vždy pred výpočtom MAC (t. j. SSC pre prvý príkaz je Initial SSC +1, SSC pre prvú odpoveď je Initial SSC + 2).

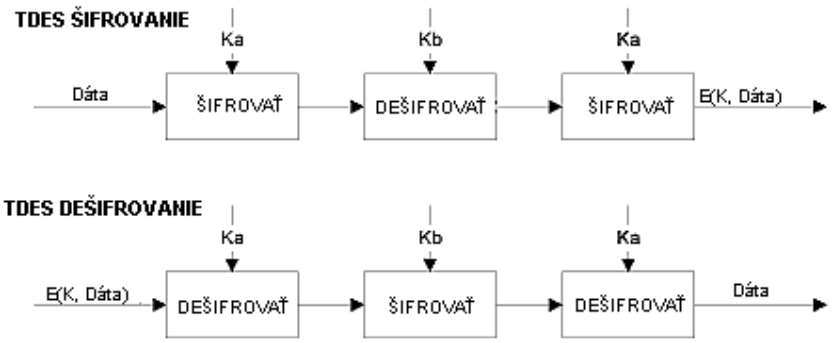
Nasledovný obrázok ukazuje výpočet zvyšného MAC:



5.4 **Algoritmus výpočtu kryptogramov pre dôverné DOs**

CSM_031 Kryptogramy sa vypočítajú s použitím TDEA v prevádzkovom režime TCBC v súlade s referenčnými dokumentami (TDES) a (TDES–OP) a nulovým vektorom ako Initial Value Block.

Nasledovný obrázok ukazuje aplikáciu kľúčov v TDES:



6. MECHANIZMUS DIGITÁLNEHO PODPISU PRI SŤAHOVANÍ DÁT

CSM_032 Inteligentné vyhradené zariadenie (Inteligent Dedicated Equipment – IDE) uchováva dáta prijímané z JV alebo karty počas jednej prenosovej relácie v jednom fyzickom dátovom súbore. Tento súbor musí obsahovať osvedčenia MS_i.C a EQT.C. Súbor obsahuje digitálne podpisy dátových blokov podľa doplnku 7 protokolov sťahovania dát.

CSM_033 Digitálne podpisy sťahovaných dát používajú digitálny podpisový systém s dodatkom tak, aby sa na požiadanie mohli sťahované dáta čítať bez dešifrovania.

6.1 **Generovanie podpisu**

CSM_034 Generovanie dátového podpisu zariadením sa uskutočňuje podľa podpisového systému s dodatkom, ktorý je definovaný v referenčnom dokumente (PKCS1) s hash funkciou SHA–1:

Podpis = EQT.SK['00' || '01' || PS || '00' || DER(SHA–1(Data))]

PS = vyplňovací reťazec oktetov s hodnotou 'FF' tak, aby bola dĺžka 128.

DER(SHA–1(M)) je kódovanie algoritmu ID pre hash funkciu a hash hodnoty v ASN.1 hodnote typu *DigestInfo* (odlišné kódovacie pravidlá):

'30'||'21'||'30'||'09'||'06'||'05'||'2B'||'0E'||'03'||'02'||'1A'||'05'||'00'||'04'||'14'||Hash hodnota.

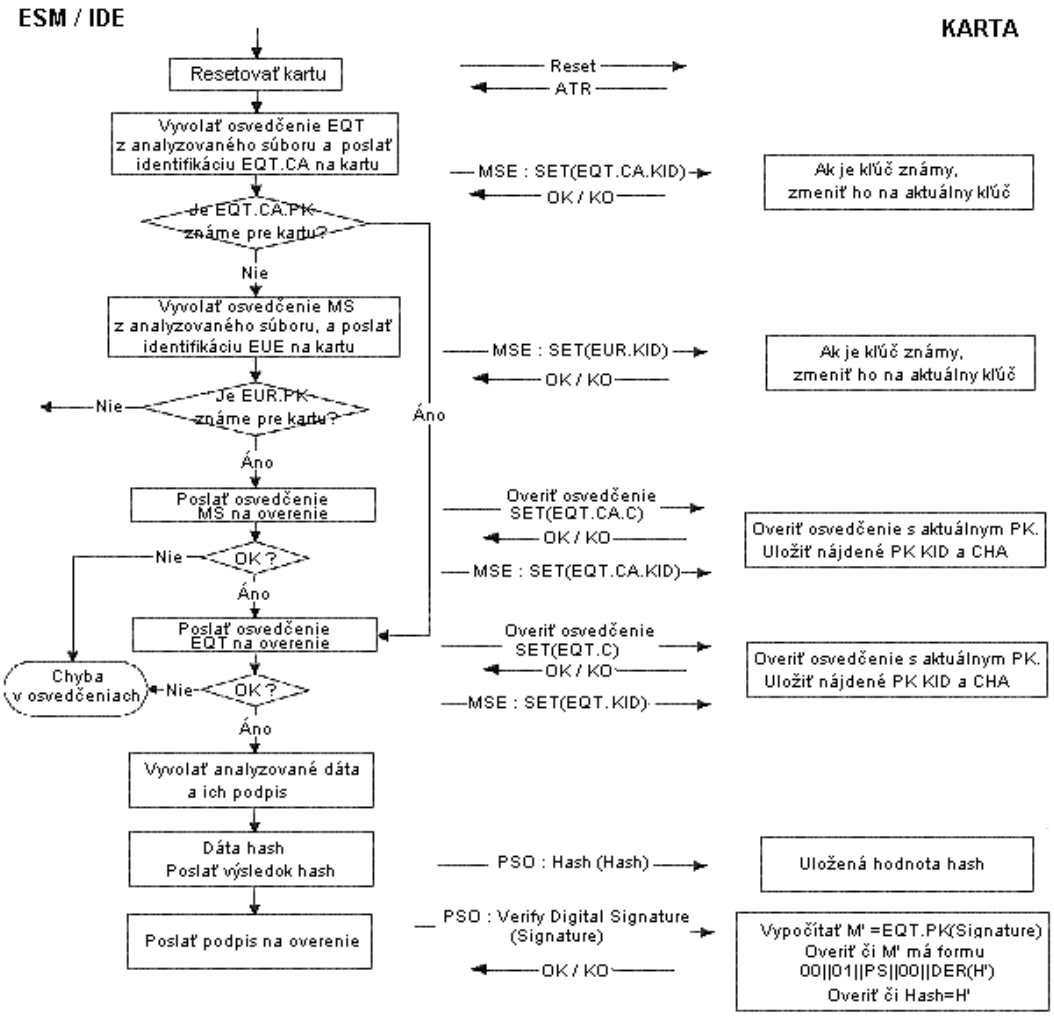
6.2 **Overenie podpisu**

CSM_035 Overenie dátového podpisu sťahovaných dát sa uskutočňuje podľa podpisového systému s dodatkom, ktorý je definovaný v referenčnom dokumente (PKCS1) s hash funkciou SHA–1.

Európsky verejný kľúč EUR.PK musí byť overovateľovi známy z nezávislého a (dôveryhodného) zdroja.

V nasledovnej tabuľke je znázornený protokol ktorým sa IDE s kontrolnou kartou môže riadiť overovanie integrity sťahovaných dát, ukladaných na ESM (vonkajšie pamäťové médium). Kontrolná karta sa používa na dešifrovanie digitálnych podpisov. Táto funkcia nesmie byť v tomto prípade implementovaná v IDE.

Zariadenie, ktoré stiahlo a podpísalo analyzované dáta je označené ako EQT.


ESM / IDE
KARTA
Resetovať kartu
Reset
ATR
Vyvolať osvedčenie EQT z analyzovaného súboru a poslať identifikáciu EQT.CA na kartu
MSE : SET(EQT.CA.KID)
OK / KO
Ak je kľúč známy, zmeniť ho na aktuálny kľúč
Je EQT.CA.PK známe pre kartu?
Nie
Áno
Vyvolať osvedčenie MS z analyzovaného súboru, a poslať identifikáciu EUE na kartu
MSE : SET(EUR.KID)
OK / KO
Ak je kľúč známy, zmeniť ho na aktuálny kľúč
Je EUR.PK známe pre kartu?
Nie
Áno
Poslať osvedčenie MS na overenie
Overiť osvedčenie SET(EQT.CA.C)
OK / KO
Overiť osvedčenie s aktuálnym PK. Uložiť nájdené PK KID a CHA
MSE : SET(EQT.CA.KID)
OK ?
Nie
Áno
Poslať osvedčenie EQT na overenie
Overiť osvedčenie SET(EQT.C)
OK / KO
Overiť osvedčenie s aktuálnym PK. Uložiť nájdené PK KID a CHA
MSE : SET(EQT.KID)
Chyba v osvedčeniach
OK ?
Nie
Áno
Vyvolať analyzované dáta a ich podpis
Dáta hash
Poslať výsledok hash
PSO : Hash (Hash)
Uložená hodnota hash
Poslať podpis na overenie
PSO : Verify Digital Signature (Signature)
OK / KO
Vypočítať M' =EQT.PK(Signature)
Overiť či M' má formu 00||01||PS||00||DER(H')
Overiť či Hash=H'

PRÍLOHA II

SCHVAĽOVACIA ZNAČKA A OSVEDČENIE

I. SCHVAĽOVACIA ZNAČKA

1. Schvaľovaciu značku tvorí:

- obdĺžnik, v ktorom je umiestnené písmeno "e", za ktorým nasleduje rozlišovacie číslo alebo písmeno štátu, ktorý vydal schválenie v súlade s nasledujúcimi dohodnutými znakmi:

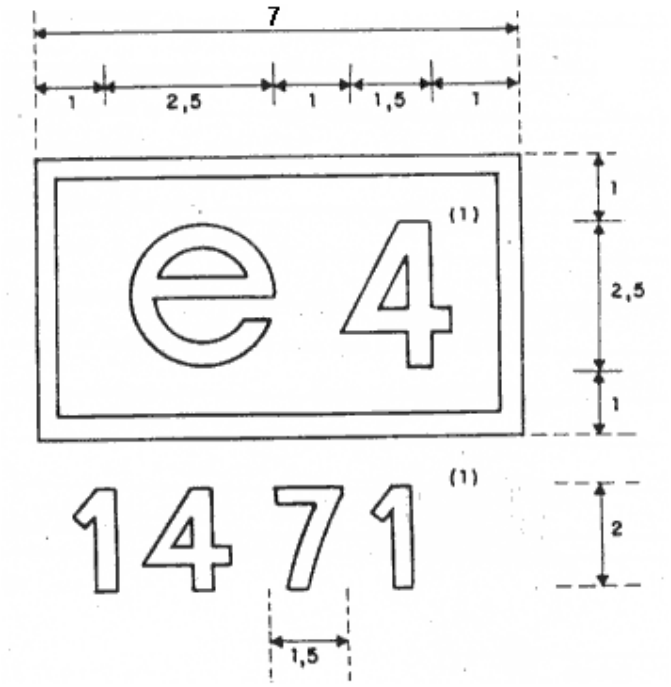
Belgicko	6,
Dánsko	18,
Nemecko	1,
Grécko	23,
Španielsko	9,
Francúzsko	2,
Írsko	24,
Taliansko	3,
Luxembursko	13,
Holandsko	4,
Portugalsko	21,
Spojené kráľovstvo	11,
Rakúsko	12,
Fínsko	17,
Švédsko	5,

a

- schvaľovacie číslo zodpovedajúce číslu schvaľovacieho osvedčenia udeleného pre prototyp záznamového zariadenia alebo záznamový list tachografovej karty, ktoré je umiestnený v ktoromkoľvek bode v tesnej blízkosti tohto obdĺžnika.

2. Schvaľovacia značka bude uvedená na popisnej doske každej sústavy zariadenia a na každom záznamovom liste a na každej tachografovej karte. Musí byť neodstrániteľná a musí vždy zostať zreteľne čitateľná.

3. Rozmery schvaľovacej značky načrtnuté nižšie sú vyjadrené v mm. Tieto rozmery sú minimálne. Pomery medzi rozmermi sa musia dodržať.



II. OSVEDČENIE O SCHVÁLENÍ PRE VÝROBKY, KTORÉ SPĹŇAJÚ POŽIADAVKY PRÍLOHY I

Štát ktorý udeľuje schválenie, vydá žiadateľovi osvedčenie o schválení, ktorého vzor je uvedený nižšie. V prípade informovania ostatných členských štátov o schváleniach, alebo v prípade vzniku situácie o odobratiach, členský štát by mal použiť kópiu daného osvedčenia.

OSVEDČENIE O SCHVÁLENÍ

Názov príslušného orgánu.....

Oznámenie týkajúce sa([6])
- schválenia typu záznamového zariadenia
- odobratia schválenia typu záznamového zariadenia
- schválenia modelového záznamového listu
- odobratia schválenia záznamového listu

Schválenie č. .....

1. Výrobná značka alebo obchodné označenie.....
2. Názov typu alebo modelu .....
3. Názov výrobcu .....
4. Adresa výrobcu .....
   .....
5. Predložený na schválenie dňa .....

[6] Nehodiace sa prečiarknuť

6. Testovaný v .....
7. Dátum a číslo protokolu o teste .....
8. Dátum schválenia .....
9. Dátum odobratia schválenia .....
10. Typ alebo typy záznamového zariadenia, na ktorých sa má záznam používať

    .....

    .....
11. Miesto .....
12. Dátum .....
13. Priložené popisné dokumenty .....

    .....

14. Poznámky

.....

(podpis)

III. SCHVAĽOVACIE OSVEDČENIE PRE VÝROBKY, KTORÉ SPĹŇAJÚ POŽIADAVKY PRÍLOHY I B

Štát, ktorý udelil schválenie vydá žiadateľovi schvaľovacie osvedčenie, ktorého vzor je uvedený nižšie. Na informovanie ostatných členských štátov o vydaných alebo odobratých schváleniach, použije členský štát kópie uvedeného osvedčenia.

SCHVAĽOVACIE OSVEDČENIE PRE VÝROBKY, KTORÉ SPĹŇAJÚ POŽIADAVKY PRÍLOHY I B

Názov príslušného orgánu .....

Oznámenie sa týka [3]:

schválenia

odobratia schválenia

vzoru záznamového zariadenia

komponentu záznamového zariadenia[4] .....

karty vodiča

dielenskej karty

podnikovej karty

kontrolnej karty

Schválenie číslo .....

1. Výrobná alebo obchodná značka .....
2. Názov modelu .....
3. Meno výrobcu .....

[3] Označiť krížikom príslušné okienka.

[4] Špecifikovať komponent, na ktorý sa oznámenie vzťahuje.

4. Adresa výrobcu .....
5. Predložené na schválenie pre .....
6. Skúšobňa(skúšobne) .....
7. Dátum a číslo skúšky(skúšok) .....
8. Dátum schválenia .....
9. Dátum odobratia schválenia .....
10. Vzorka komponentu(komponentov) záznamového zariadenia, pre ktoré je komponentu určený ..
11. Miesto .....
12. Dátum .....
13. Priložené popisné dokumenty .....

---

14. Poznámky (vrátane prípadná poloha plomb)

.....
podpis