Úřední věstník Evropské unie

L 85

České vydání

Právní předpisy

Ročník 61

28. března 2018

Obsah

[1] Text s významem pro EHP.

CS

Akty, jejichž název není vytištěn tučně, se vztahují ke každodennímu řízení záležitostí v zemědělství a obecně platí po omezenou dobu.

Názvy všech ostatních aktů jsou vytištěny tučně a předchází jim hvězdička.

II

(Nelegislativní akty)

NAŘÍZENÍ

PROVÁDĚCÍ NAŘÍZENÍ KOMISE (EU) 2018/502

ze dne 28. února 2018,

kterým se mění prováděcí nařízení (EU) 2016/799, kterým se stanoví požadavky na konstrukci, zkoušení, montáž, provoz a opravy tachografů a jejich součástí

(Text s významem pro EHP)

EVROPSKÁ KOMISE,

s ohledem na Smlouvu o fungování Evropské unie,

s ohledem na nařízení Evropského parlamentu a Rady (EU) č. 165/2014 ze dne 4. února 2014 o tachografech v silniční dopravě ([1]), a zejména na článek 11 a čl. 12 odst. 7 uvedeného nařízení,

vzhledem k těmto důvodům:

(1) Nařízení (EU) č. 165/2014 zavedlo inteligentní tachografy, tj. digitální tachografy druhé generace, jejichž součástí je také napojení na globální družicový navigační systém („GNSS"), komunikační zařízení pro včasné dálkové odhalování a nepovinné rozhraní s inteligentními dopravními systémy.

(2) Technické požadavky na konstrukci, zkoušení, montáž, provoz a opravy tachografů a jejich součástí jsou stanoveny v prováděcím nařízení Komise (EU) 2016/799 ([2]).

(3) V souladu s články 8, 9 a 10 nařízení (EU) č. 165/2014 jsou tachografy namontované do vozidel poprvé registrovaných dne 15. června 2019 nebo po tomto dni tachografy inteligentní. Prováděcí nařízení (EU) 2016/799 musí být proto změněno tak, aby se technická ustanovení uvedená v těchto článcích použila od téhož dne.

(4) Za účelem dosažení souladu s článkem 8 nařízení (EU) č. 165/2014, který stanoví, že poloha vozidla se musí zaznamenávat každé tři hodiny celkové doby řízení, by mělo být prováděcí nařízení (EU) 2016/799 změněno tak, aby informace o poloze vozidla mohly být ukládány ve tříhodinových intervalech metrikou, jejíž výsledky nelze vynulovat, a aby se zabránilo záměně s „dobou nepřetržitého řízení", což je metrika s odlišnou funkcí.

(5) Celkem ve vozidle může být jediný celek nebo několik celků rozmístěných ve vozidle. Zařízení GNSS a zařízení vyhrazeného spojení krátkého dosahu (DSRC) by proto mohla být umístěna uvnitř nebo vně hlavní jednotky celku ve vozidle. Jsou-li umístěna vně této jednotky, mělo by být možné obě zařízení i hlavní jednotku celku ve vozidle typově schválit jako součásti, aby se postup schválení typu inteligentních tachografů přizpůsobil potřebám trhu.

(6) Pravidla pro ukládání událostí nesouladu času a nastavení času musí být upravena tak, aby bylo možné rozlišovat mezi automatickým nastavením času, k němuž dojde po možném pokusu o nedovolenou manipulaci nebo po poruše tachografu, a nastavením času, k němuž dojde z jiných důvodů, např. v důsledku údržby.

(7) Identifikátory dat by měly být schopny rozlišovat mezi daty staženými z inteligentního tachografu a daty staženými z tachografů starší generace.

([1]) Úř. věst. L 60, 28.2.2014, s. 1.

([2]) Prováděcí nařízení Komise (EU) 2016/799 ze dne 18. března 2016, kterým se provádí nařízení Evropského parlamentu a Rady (EU) č. 165/2014, kterým se stanoví požadavky na konstrukci, zkoušení, montáž, provoz a opravy tachografů a jejich součástí (Úř. věst. L 139, 26.5.2016, s. 1).

(8) Doba platnosti karty podniku musí být prodloužena ze dvou na pět let, aby byla uvedena do souladu s dobou platnosti karty řidiče.

(9) Popis některých závad a událostí, validace vložených údajů o místě počátku nebo ukončení denní pracovní doby, používání souhlasu řidiče pro rozhraní inteligentního dopravního systému (ITS), pokud jde o údaje přenášené celkem ve vozidle prostřednictvím sítě vozidla, a další technické otázky by měly být lépe definovány.

(10) Aby byla zajištěna aktuálnost certifikace plomb tachografů, je třeba je přizpůsobit novým normám bezpečnosti mechanických plomb, které jsou na tachografech používány.

(11) Toto nařízení se týká konstrukce, zkoušení, montáže a provozu systémů, které rovněž sestávají z rádiových zařízení, jež upravuje směrnice Evropského parlamentu a Rady 2014/53/EU [1]. Tato směrnice upravuje uvádění elektronických a elektrických zařízení využívajících rádiové vlny pro účely komunikace nebo rádiového určování na horizontální úrovni na trh a jejich uvádění do provozu, zejména s ohledem na elektrickou bezpečnost, kompatibilitu s jinými systémy, přístup k rádiovému spektru, přístup k tísňovým službám nebo doplňující ustanovení o přenesené pravomoci. Aby bylo zajištěno účinné využívání rádiového spektra, zabráněno škodlivým vysokofrekvenčním interferencím, zajištěna bezpečnost a elektromagnetická kompatibilita rádiového zařízení a aby bylo možné stanovit jakékoli další zvláštní požadavky v přenesené pravomoci, uvedená směrnice by neměla být tímto nařízením dotčena.

(12) Prováděcí nařízení (EU) 2016/799 by proto mělo být změněno.

(13) Opatření stanovená tímto nařízením jsou v souladu se stanoviskem výboru uvedeného v čl. 42 odst. 3 nařízení (EU) č. 165/2014,

PŘIJALA TOTO NAŘÍZENÍ:

Článek 1

Prováděcí nařízení (EU) 2016/799 se mění takto:

1) Článek 1 se mění takto:

a) druhý a třetí odstavec se nahrazují tímto:

„2. Konstrukce, zkoušení, montáž, kontrola, provoz a opravy inteligentních tachografů a jejich součástí musí splňovat technické požadavky stanovené v příloze IC tohoto nařízení.

3. Tachografy jiné než inteligentní musí nadále, pokud jde o jejich konstrukci, zkoušení, montáž, kontrolu, provoz a opravy, splňovat podle konkrétního případu požadavky stanovené buď v příloze I nařízení (EU) č. 165/2014, nebo v příloze IB nařízení Rady (EHS) č. 3821/85 (*).

(*) Nařízení Rady (EHS) č. 3821/85 ze dne 20. prosince 1985 o záznamovém zařízení v silniční dopravě (Úř. věst. L 370, 31.12.1985, s. 8).“;

b) doplňuje se nový odstavec 5, který zní:

„5. Tímto nařízením není dotčena směrnice Evropského parlamentu a Rady 2014/53/EU (*).

(*) Směrnice 2014/53/EU Evropského parlamentu a Rady ze dne 16. dubna 2014 o harmonizaci právních předpisů členských států týkajících se dodávání rádiových zařízení na trh a zrušení směrnice 1999/5/ES (Úř. věst. L 153, 22.5.2014, s. 62).“

2) Článek 2 se mění takto:

a) definice v bodě 3 se nahrazuje tímto:

„3) „dokumentací výrobce“ úplná dokumentace v elektronické nebo tištěné podobě, která obsahuje všechny informace poskytované výrobcem nebo jeho zmocněncem orgánu příslušnému pro schvalování typu pro účely schválení typu tachografu nebo jeho součásti, včetně osvědčení uvedených v čl. 12 odst. 3 nařízení (EU) č. 165/2014, provádění zkoušek definovaných v příloze IC tohoto nařízení, jakož i výkresy, fotografie a další příslušné doklady;“

[1] Směrnice Evropského parlamentu a Rady 2014/53/EU ze dne 16. dubna 2014 o harmonizaci právních předpisů členských států týkajících se dodávání rádiových zařízení na trh a zrušení směrnice 1999/5/ES (Úř. věst. L 153, 22.5.2014, s. 62).

b) definice v bodě 7 se nahrazuje tímto:

„7) „inteligentním tachografem“ nebo „tachografem druhé generace“ digitální tachograf, který splňuje požadavky článků 8, 9 a 10 nařízení (EU) č. 165/2014, jakož i přílohy IC tohoto nařízení;“

c) definice v bodě 8 se nahrazuje tímto:

„8) „součástí tachografu“ kterýkoli z těchto prvků: celek ve vozidle, snímač pohybu, záznamový list, vnější zařízení GNSS a vnější zařízení pro včasné dálkové odhalování;“

d) doplňuje se nová definice v bodě 10, která zní:

„10) „celkem ve vozidle“ tachograf s výjimkou snímače pohybu a kabelů připojujících snímač pohybu.

Může jím být jediný celek nebo několik celků rozmístěných ve vozidle, přičemž zahrnuje řídicí jednotku, datovou paměť, funkci měření času, dvě čtecí zařízení čipových karet pro řidiče a druhého řidiče, tiskárnu, zobrazení, konektory a zařízení pro vkládání uživatelských údajů, přijímač GNSS a zařízení pro dálkovou komunikaci.

Celek ve vozidle může sestávat z těchto součástí, které podléhají schválení typu:

— celku ve vozidle jakožto jediné součásti (včetně přijímače GNSS a zařízení pro dálkovou komunikaci),

— hlavní jednotky celku ve vozidle (včetně zařízení pro dálkovou komunikaci) a vnějšího zařízení GNSS,

— hlavní jednotky celku ve vozidle (včetně přijímače GNSS) a vnějšího zařízení pro dálkovou komunikaci,

— hlavní jednotky celku ve vozidle, vnějšího přijímače GNSS a vnějšího zařízení pro dálkovou komunikaci.

Pokud celek ve vozidle sestává z několika celků rozmístěných ve vozidle, je hlavní jednotkou celku ve vozidle celek obsahující řídicí jednotku, datovou paměť a funkci měření času.

Výraz „celek ve vozidle (VU)“ se používá pro označení „celku ve vozidle“ nebo „hlavní jednotky celku ve vozidle.““

3) V článku 6 se třetí pododstavec nahrazuje tímto:

„Příloha IC se však použije ode dne 15. června 2019, s výjimkou dodatku 16, který se použije ode dne 2. března 2016.“

4) Příloha IC se mění v souladu s přílohou I tohoto nařízení;

5) Příloha II se mění v souladu s přílohou II tohoto nařízení.

Článek 2

Vstup v platnost

Toto nařízení vstupuje v platnost dvacátým dnem po vyhlášení v *Úředním věstníku Evropské unie*.

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

V Bruselu dne 28. února 2018.

Za Komisi

předseda

Jean-Claude JUNCKER

PŘÍLOHA I

Příloha IC nařízení (EU) 2016/799 se mění takto:

1) Obsah se mění takto:

a) bod 3.12.5 se nahrazuje tímto:

„3.12.5. Místa a polohy, kde začíná nebo končí denní pracovní doba a/nebo kde je dosaženo tří hodin součtové doby řízení“;

b) bod 4.5.3.2.16 se nahrazuje tímto:

„4.5.3.2.16 Údaje o místech součtové tříhodinové doby řízení“;

c) bod 4.5.4.2.14 se nahrazuje tímto:

„4.5.4.2.14 Údaje o místech součtové tříhodinové doby řízení“;

d) bod 6.2 se nahrazuje tímto:

„6.2 Kontrola nových nebo opravených součástí“;

2) bod 1 se mění takto:

a) definice ll) se nahrazuje tímto:

„ll) „zařízením pro dálkovou komunikaci“ nebo „zařízením pro včasné dálkové odhalování“:

vybavení celku ve vozidle, které se užívá k provádění cílených silničních kontrol;“;

b) definice tt) se nahrazuje tímto:

„tt) „nastavením času“:

nastavení aktuálního času; toto nastavení lze provádět automaticky v pravidelných intervalech podle času z přijímače GNSS představujícího čas referenční nebo v režimu kalibrace;“

c) v definici yy) se první odrážka nahrazuje tímto:

„— zabudováno a užíváno pouze ve vozidlech typu M1 a N1 (podle definice v příloze II směrnice Evropského parlamentu a Rady 2007/46/ES (*) v platném znění),“;

d) doplňuje se nová definice fff), která zní:

„fff) „součtovou dobou řízení“:

hodnota vyjadřující celkový počet minut jízdy určitého vozidla.

Hodnota součtové doby řízení je součet minut volného chodu, který funkce monitorování činností řízení záznamového zařízení považuje za JÍZDU, a používá se pouze ke spuštění záznamu polohy vozidla pokaždé, když součtová doba řízení dosáhne násobku tří hodin. Sčítání je zahájeno zapnutím záznamového zařízení. Tuto hodnotu neovlivňuje žádná jiná podmínka jako „mimo působnost“ nebo „převoz lodí / převoz vlakem“.

Hodnota součtové doby řízení není určena k zobrazování, tisku ani stahování;“

3) v bodě 2.3 se poslední odrážka v odstavci 13 nahrazuje tímto:

„— celky ve vozidle mají normální dobu platnosti používání 15 let od data vstupu osvědčení celku ve vozidle v platnost, ale celky ve vozidle lze používat další tři měsíce pouze pro stahování údajů.“;

4) v bodě 2.4 se první pododstavec nahrazuje tímto:

„Bezpečnost systému má za cíl ochranu datové paměti takovým způsobem, aby se zabránilo neoprávněnému přístupu a manipulaci s údaji a aby takové pokusy byly odhaleny, ochranu integrity a pravosti údajů přenášených mezi snímačem pohybu a celkem ve vozidle, ochranu integrity a pravosti údajů přenášených mezi záznamovým zařízením a kartami tachografu, ochranu integrity a pravosti údajů přenášených mezi celkem ve vozidle a vnějším zařízením GNSS, ochranu důvěrnosti, integrity a pravosti údajů přenášených pomocí komunikace včasného dálkového odhalování pro kontrolní účely a ověřování integrity a pravosti stahovaných údajů.“;

5) v bodě 3.2 se druhá odrážka odstavce 27 nahrazuje tímto:

„— poloh, kde součtová doba řízení dosáhne násobku tří hodin;“

6) v bodě 3.4 se odstavec 49 nahrazuje tímto:

„49) První změna činnosti řidiče na režim PŘESTÁVKA/ODPOČINEK nebo POHOTOVOST, která nastane během 120 sekund po automatickém přepnutí do režimu PRÁCE v důsledku zastavení vozidla, musí být považována za změnu nastalou v průběhu zastávky vozidla (proto je možné zrušení změny na režim PRÁCE).“;

7) v bodě 3.6.1 se odstavec 59 nahrazuje tímto:

„59) Řidič pak vloží aktuální polohu vozidla, která je považována za dočasný vstup.

Za následujících podmínek se dočasné údaje vytvořené při posledním vyjmutí karty validují (tj. již se dále nepřepisují):

— vložení údaje o místě zahájení aktuální denní pracovní doby při ručním zadání podle požadavku 61,

— pokud držitel karty nezadá žádné místo, kde zahájil nebo ukončil pracovní dobu, další vložení údaje o místě zahájení aktuální denní pracovní doby při ručním zadání podle požadavku 61.

Za následujících podmínek se dočasné údaje vytvořené při posledním vyjmutí karty přepíší a nová hodnota se validuje:

— pokud držitel karty nezadá žádné místo, kde zahájil nebo ukončil pracovní dobu, další vložení údaje o místě ukončení aktuální denní pracovní doby při ručním zadání podle požadavku 61.“;

8) v bodě 3.6.2 se šestá a sedmá odrážka nahrazují těmito odrážkami:

„— místo ukončení předešlé denní pracovní doby a příslušný čas (čímž dojde k přepsání a validaci položky vytvořené při posledním vyjmutí karty),

— místo zahájení aktuální denní pracovní doby a příslušný čas (čímž dojde k validaci dočasných údajů vytvořených při posledním vyjmutí karty).“;

9) bod 3.9.15 se nahrazuje tímto:

„3.9.15 „Nesoulad času“

86) Tato událost nastane, **není-li zařízení v kalibračním režimu**, pokud celek ve vozidle zjistí mezi časem funkce měření času celku ve vozidle a časem pocházejícím z přijímače GNSS nesoulad delší než 1 minuta. Tato událost je zaznamenána společně s hodnotou vnitřních hodin celku ve vozidle a je zahrnuta do automatického nastavení času. Nastane-li událost nesouladu času, celek ve vozidle po dobu příštích 12 hodin jiné události nesouladu času nevytvoří. Tato událost nenastane v případě, že přijímač GNSS po dobu 30 či více dnů nezjistil žádný platný signál GNSS.“;

10) v bodě 3.9.17 se doplňuje nová odrážka, která zní:

„— závada rozhraní ITS (v příslušných případech)“;

11) bod 3.10 se mění takto:

i) znění před tabulkou v odstavci 89 nahrazuje tímto:

„Záznamové zařízení musí zjistit závady v průběhu integrovaných zkoušek a autotestů v souladu s touto tabulkou:“;

ii) v tabulce se doplňuje nový řádek, který zní:

„Rozhraní ITS (volitelné)	Správná funkce“	

12) v bodě 3.12 se druhá odrážka nahrazuje tímto:

„— se průměrným počtem poloh za den rozumí nejméně 6 poloh, ve kterých začíná denní pracovní doba, 6 poloh, kdy součtová doba řízení dosáhne násobku tří hodin, a 6 poloh, ve kterých končí denní pracovní doba, takže „365 dnů“ obsahuje minimálně 6570 poloh,“;

13) bod 3.12.5 se mění takto:

a) nadpis a odstavec 108 se nahrazují tímto:

„3.12.5. Místa a polohy, kde začíná nebo končí denní pracovní doba a/nebo kde je dosaženo tří hodin součtové doby řízení

108) Záznamové zařízení musí zaznamenávat a ukládat do své datové paměti:

— místa a polohy, kde řidič a/nebo druhý řidič začíná svou denní pracovní dobu,

— polohy, kde součtová doba řízení dosáhne násobku tří hodin,

— místa a polohy, kde řidič a/nebo druhý řidič končí svou denní pracovní dobu.“;

b) v odstavci 110 se čtvrtá odrážka nahrazuje tímto:

„— typ vložených údajů (začátek a konec nebo tři hodiny součtové doby řízení),“;

c) odstavec 111 se nahrazuje tímto:

„111) Datová paměť musí být schopna uchovat místa a polohy, ve kterých denní pracovní doba začíná a končí a/nebo ve kterých je dosaženo tří hodin součtové doby řízení, minimálně po dobu 365 dnů.“;

14) v bodě 3.12.7 se odstavec 116 nahrazuje tímto:

„116) Záznamové zařízení musí zaznamenávat a uchovávat ve své datové paměti okamžitou rychlost vozidla a odpovídající datum a čas v každé sekundě po dobu nejméně posledních 24 hodin, kdy bylo vozidlo v pohybu.“;

15) tabulka v bodě 3.12.8 se mění takto:

a) mezi položky „Chybí informace o poloze z přijímače GNSS“ a „Chyba údajů o pohybu vozidla“ se vkládá tato položka:

„Chyba komunikace s vnějším zařízením GNSS	— nejdelší událost v každém z posledních deseti dnů výskytu — pět nejdelších událostí za posledních 365 dnů	— datum a čas začátku události — datum a čas konce události — typ, číslo, vydávající členský stát a generace všech karet vložených na začátku a/nebo na konci události — počet podobných událostí v tentýž den“

b) položka „Časový konflikt“ se nahrazuje tímto:

„Časový konflikt	— nejzávažnější událost v každém z posledních deseti dnů výskytu (tj. případy s největším rozdílem mezi datem a časem záznamového zařízení a datem a časem GNSS) — pět nejzávažnějších událostí za posledních 365 dnů	— datum a čas záznamového zařízení — datum a čas GNSS — typ, číslo, vydávající členský stát a generace všech karet vložených na začátku a/nebo na konci události — počet podobných událostí v tentýž den“

16) v bodě 3.20 se odstavec 200 nahrazuje tímto:

„200) Záznamové zařízení může být rovněž vybaveno standardními rozhraními, která umožňují, aby údaje zaznamenané nebo vytvořené tachografem používalo externí zařízení v provozním nebo kalibračními režimu.

V dodatku 13 je specifikováno a standardizováno volitelné rozhraní ITS. Mohou být používána i další podobná rozhraní celku ve vozidle, pokud zcela odpovídají požadavkům dodatku 13 z hlediska minimálního výčtu údajů, zabezpečení a souhlasu řidiče.

Souhlas řidiče se nevztahuje na data přenášená ze záznamového zařízení do sítě vozidla. Jsou-li osobní údaje přenesené do sítě vozidla dále zpracovávány mimo síť vozidla, výrobce vozidla odpovídá za to, že proces zpracování osobních údajů je v souladu s nařízením (EU) 2016/679 („obecné nařízení o ochraně osobních údajů“).

Souhlas řidiče se nevztahuje ani na data tachografu stahovaná do vzdáleného podniku (požadavek 193), jelikož tento proces je monitorován přístupovým právem ke kartě podniku.

Pro údaje ITS zprostředkované tímto rozhraním platí tyto požadavky:

— tyto údaje jsou souborem vybraných stávajících údajů ze slovníku dat tachografu (dodatek 1),

— dílčí soubor těchto vybraných údajů je označen jako „osobní údaje“,

— dílčí soubor „osobní údaje“ je k dispozici pouze v případě, že je vydán ověřitelný souhlas řidiče s tím, že jeho osobní údaje mohou opustit síť vozidla,

— pomocí příkazů v menu může být souhlas řidiče kdykoli vydán nebo zamítnut, je-li vložena karta řidiče,

— soubor a dílčí soubor údajů bude předáván pomocí bezdrátového protokolu Bluetooth v prostoru kabiny řidiče s obnovovací frekvencí 1 minuty,

— spárování vnějšího zařízení s rozhraním ITS bude chráněno vyhrazeným a náhodným kódem PIN obsahujícím minimálně 4 číslice, zaznamenaným a dostupným pomocí zobrazovací jednotky každého celku ve vozidle,

— přítomnost rozhraní ITS nesmí za žádných okolností narušovat nebo ovlivňovat správnou funkci a bezpečnost celku ve vozidle.

Další údaje mohou být také k dispozici kromě tohoto souboru vybraných stávajících údajů považovaných za minimální výčet, nelze-li je považovat za osobní údaje.

Záznamové zařízení musí být schopno informovat o stavu souhlasu řidiče ostatní platformy v síti vozidla.

Je-li zapnuto zapalování vozidla, musí být uvedené údaje neustále vysílány.“;

17) v bodě 3.23 se odstavec 211 nahrazuje tímto:

„211) Nastavení času vnitřních hodin celku ve vozidle se provádí automaticky každých 12 hodin. Pokud tato změna nastavení není možná, protože signál GNSS není k dispozici, provede se nastavení času, jakmile má celek ve vozidle podle stavu zapalování vozidla přístup k platnému času poskytovanému přijímačem GNSS. Časový odkaz pro automatické nastavení času vnitřních hodin celku ve vozidle se odvozuje od přijímače GNSS.“;

18) v bodě 3.26 se odstavce 225 a 226 nahrazují tímto:

„225) Na každou samostatnou součást záznamového zařízení musí být připevněn popisný štítek, na němž jsou uvedeny tyto údaje:

— název a adresa výrobce,

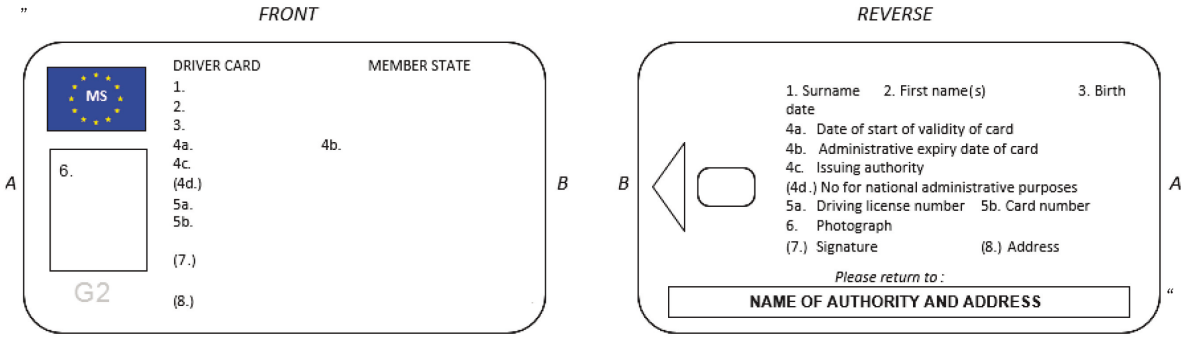
— katalogové číslo součásti podle výrobce a rok výroby,

— výrobní číslo,

— značka schválení typu.

226) Pokud není k dispozici dostatečný prostor pro zobrazení všech výše uvedených údajů, musí být na popisném štítku uvedeny alespoň: název nebo logo výrobce a katalogové číslo součásti.“;

19) v bodě 4.1 se výkres přední a zadní strany karty řidiče nahrazuje tímto:



20) v bodě 4.5.3.1.8 se první odrážka v odstavci 263 nahrazuje tímto:

„— chyba karty (v případě, že tato karta je předmětem chyby),“;

21) v bodě 4.5.3.2.8 se první odrážka v odstavci 288 nahrazuje tímto:

„— chyba karty (v případě, že tato karta je předmětem chyby),“;

22) bod 4.5.3.2.16 se nahrazuje tímto:

„4.5.3.2.16 Údaje o místech součtové tříhodinové doby řízení

305) Karta řidiče musí být schopna uchovat následující údaje vztahující se k poloze vozidla, kde součtová doba řízení dosáhne násobku tří hodin:

— datum a čas, kdy součtová doba řízení dosáhne násobku tří hodin,

— polohu vozidla,

— přesnost GNSS, datum a čas, kdy byla poloha zjištěna,

— stav počitadla ujetých kilometrů.

306) Karta řidiče musí být schopna uchovat nejméně 252 takových záznamů.“;

23) bod 4.5.4.2.14 se nahrazuje tímto:

„4.5.4.2.14 Údaje o místech součtové tříhodinové doby řízení

353) Karta dílny musí být schopna uchovat následující údaje vztahující se k poloze vozidla, kde součtová doba řízení dosáhne násobku tří hodin:

— datum a čas, kdy součtová doba řízení dosáhne násobku tří hodin,

— polohu vozidla,

— přesnost GNSS, datum a čas, kdy byla poloha zjištěna,

— stav počitadla ujetých kilometrů.

354) Karta dílny musí být schopna uchovat nejméně 18 takových záznamů.“;

24) v bodě 5.2 se odstavec 396 nahrazuje tímto:

„396) Štítek musí obsahovat alespoň tyto údaje:

— jméno, adresu nebo firemní značku schváleného montéra nebo dílny,

— charakteristický koeficient vozidla ve tvaru „w = … imp/km“,

— konstantu záznamového zařízení ve tvaru „k = … imp/km“,

— účinný obvod pneumatik na kolech ve tvaru „l = … mm“,

— rozměr pneumatiky,

— datum změření charakteristického koeficientu vozidla a účinného obvodu pneumatik na kolech,

— identifikační číslo vozidla,

— přítomnost (či nepřítomnost) vnějšího zařízení GNSS,

— v příslušných případech výrobní číslo vnějšího zařízení GNSS,

— výrobní číslo případného zařízení pro dálkovou komunikaci,

— výrobní číslo všech příslušných plomb,

— část vozidla, v níž je případně zabudován adaptér,

— část vozidla, v níž je zabudován snímač pohybu, pokud není připojen k převodové skříni nebo není používán adaptér,

— popis barvy kabelu mezi adaptérem a částí vozidla zajišťující přicházející impulsy,

— výrobní číslo vloženého snímače pohybu adaptéru.“;

25) bod 5.3 se mění takto:

a) za odstavec 398 se vkládá nový odstavec 398a, který zní:

„398a Výše uvedené plomby musí být certifikovány v souladu s normou EN 16882:2016.“;

b) v odstavci 401 se druhý pododstavec nahrazuje tímto:

„Toto jedinečné identifikační číslo je definováno jako: MMNNNNNNNN provedené neodstranitelným značením, přičemž MM je jedinečná identifikace výrobce (registrační databázi spravuje EK) a NNNNNNNN alfanumerické číslo plomby, které je jedinečné v doméně výrobců.“;

c) odstavec 403 se nahrazuje tímto:

„403) Výrobci plomb musí být registrováni v příslušné databázi, jakmile si nechají model plomby certifikovat podle normy EN 16882:2016, a musí zveřejnit identifikační čísla svých plomb postupem stanoveným Evropskou komisí.“;

d) odstavec 404 se nahrazuje tímto:

„404) Schválené dílny a výrobci vozidel musí v rámci nařízení (EU) č. 165/2014 používat pouze plomby certifikované podle normy EN 16882:2016 od výrobců uvedených ve výše zmíněné databázi.“;

26) bod 6.2 se nahrazuje tímto:

„6.2 Kontrola nových nebo opravených součástí

407) U každého jednotlivého zařízení, ať již nového nebo opraveného, musí být zkontrolována správná funkčnost a přesnost odečtů a záznamů, a to v rámci limitů stanovených v bodech 3.2.1, 3.2.2, 3.2.3 a 3.3.“;

27) v bodě 6.3 se odstavec 408 nahrazuje tímto:

„408) Po namontování záznamového zařízení do vozidla musí celá instalace (včetně záznamového zařízení) vyhovovat ustanovením vztahujícím se k maximálním tolerancím stanoveným v bodech 3.2.1, 3.2.2, 3.2.3 a 3.3. Celá instalace musí být zaplombována v souladu s bodem 5.3 a zkalibrována.“;

28) bod 8.1 se mění takto:

a) v bodě 8.1 se znění uvozující odstavec 425 nahrazuje tímto:

„Pro účely této kapitoly se „záznamovým zařízením“ rozumí „záznamové zařízení nebo jeho součásti“. Schválení typu není vyžadováno pro kabel(y) spojující snímač pohybu s celkem ve vozidle, vnější zařízení GNSS s celkem ve vozidle nebo vnější zařízení pro dálkovou komunikaci s celkem ve vozidle. Papír používaný záznamovým zařízením je považován za součást záznamového zařízení.

Kterýkoli výrobce může požádat o schválení typu součásti nebo součástí záznamového zařízení s jakoukoli jinou součástí či součástmi záznamového zařízení, pokud každá součást splňuje požadavky této přílohy. Případně mohou výrobci rovněž požádat o schválení typu záznamového zařízení.

Jak je popsáno v definici uvedené v čl. 2 bodě 10 tohoto nařízení, existují různé varianty montáže součástí celků ve vozidle. Bez ohledu na montáž součástí celku ve vozidle nejsou externí anténa a (případně) anténní rozdvojka připojené k přijímači GNSS nebo k zařízení pro dálkovou komunikaci součástí schválení typu celku ve vozidle.

Výrobci, kteří obdrželi schválení typu pro záznamové zařízení, však musí vést veřejně dostupný seznam antén a rozdvojek kompatibilních s každým typově schváleným celkem ve vozidle, vnějším zařízením GNSS a vnějším zařízením pro dálkovou komunikaci.“;

b) odstavec 427 se nahrazuje tímto:

„427) Orgány členských států příslušné pro schvalování typu nevydají osvědčení o schválení typu, pokud neobdrží:

— osvědčení o bezpečnosti (vyžaduje-li ho tato příloha),

— osvědčení o funkčnosti

— a osvědčení o interoperabilitě (vyžaduje-li ho tato příloha)

k záznamovému zařízení nebo kartě, která je předmětem žádosti o schválení typu.“;

29) dodatek 1 se mění takto:

a) obsah se mění takto:

i) bod 2.63 se nahrazuje tímto:

„2.63 Vyhrazeno pro budoucí použití“;

ii) bod 2.78 se nahrazuje tímto:

„2.78 GNSSAccumulatedDriving“;

iii) bod 2.79 se nahrazuje tímto:

„2.79 GNSSAccumulatedDrivingRecord“;

iv) bod 2.111 se nahrazuje tímto:

„2.111 NoOfGNSSADRecords“;

v) bod 2.160 se nahrazuje tímto:

„2.160 Vyhrazeno pro budoucí použití“;

vi) bod 2.203 se nahrazuje tímto:

„2.203 VuGNSSADRecord“;

vii) bod 2.204 se nahrazuje tímto:

„2.204 VuGNSSADRecordArray“;

viii) bod 2.230 se nahrazuje tímto:

„2.230 Vyhrazeno pro budoucí použití“;

ix) bod 2.231 se nahrazuje tímto:

„2.231 Vyhrazeno pro budoucí použití“;

b) v bodě 2 se před bod 2.1 vkládá nový pododstavec, který zní:

„U typů dat karty používaných pro aplikace 1. a 2. generace je v tomto dodatku uvedena velikost pro aplikaci 2. generace. Má se za to, že velikost pro aplikaci 1. generace již čtečka zná. Čísla požadavků v příloze IC týkajících se těchto typů dat zahrnují aplikace 1. i 2. generace.“;

c) bod 2.19 se nahrazuje tímto:

„2.19. **CardEventData**

1. generace:

Informace uložené na kartě řidiče nebo kartě dílny týkající se událostí souvisejících s držitelem karty (příloha IC požadavky 260 a 318).

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

CardEventData je posloupnost záznamů cardEventRecords seřazená vzestupně podle hodnot EventFaultType (kromě záznamů souvisejících s pokusy o narušení zabezpečení, které jsou seskupeny v poslední sadě v posloupnosti).

cardEventRecords je sada záznamů o událostech daného typu (nebo kategorie v případě pokusů o narušení zabezpečení).

2. generace:

Informace uložené na kartě řidiče nebo kartě dílny týkající se událostí souvisejících s držitelem karty (příloha IC požadavky 285 a 341).

```
CardEventData ::= SEQUENCE SIZE(11) OF {
  cardEventRecords                    SET SIZE(NoOfEventsPerType) OF
                                      CardEventRecord
}
```

CardEventData je posloupnost záznamů cardEventRecords seřazená vzestupně podle hodnot EventFaultType (kromě záznamů souvisejících s pokusy o narušení zabezpečení, které jsou seskupeny v poslední sadě v posloupnosti).

cardEventRecords je sada záznamů o událostech daného typu (nebo kategorie v případě pokusů o narušení zabezpečení)“.

d) bod 2.30 se nahrazuje tímto:

„2.30 **CardRenewalIndex**

Index obnovy karty (definice i)).

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

Přiřazení hodnoty: (viz kapitolu 7 této přílohy).

„0“ První vydání.

Posloupnost: „0, …, 9, A, …, Z“ “;

e) v bodě 2.61 se znění za nadpisem „2. generace“ nahrazuje tímto:

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

Kromě prvků 1. generace se používají tyto datové prvky:

noOfGNSSADRecords je počet záznamů o součtové době řízení dle GNSS, které lze na kartu uložit.

noOfSpecificConditionRecords je počet záznamů o zvláštní podmínce, které lze na kartu uložit.

noOfCardVehicleUnitRecords je počet záznamů o použitých celcích ve vozidle, které lze na kartu uložit.“;

f) bod 2.63 se nahrazuje tímto:

„2.63 **Vyhrazeno pro budoucí použití**“;

g) v bodě 2.67 se znění za nadpisem „2. generace“ nahrazuje tímto:

„Používají se stejné hodnoty jako v 1. generaci s těmito doplňky:

```
--GNSS Facility                 (8),
--Remote Communication Module   (9),
--ITS interface module          (10),
--Plaque                        (11),--may be used in SealRecord
--M1/N1 Adapter                 (12),--may be used in SealRecord
--European Root CA (ERCA)       (13),
--Member State CA (MSCA)        (14),
--External GNSS connection      (15),--may be used in SealRecord
--Unused                        (16),--used in SealDataVu
--Driver Card (Sign)            (17),--only to be used in the CHA
                                field of a signing certificate
--Workshop Card (Sign)          (18), --only to be used in the CHA
                                field of a signing certificate
--Vehicle Unit (Sign)           (19), --only to be used in the CHA
                                field of a signing certificate
--RFU                           (20..255)
```

Poznámka 1: Hodnoty 2. generace pro štítek, adaptér a vnější připojení GNSS, jakož i hodnoty 1. generace pro celek ve vozidle a snímač pohybu lze v příslušných případech použít v záznamu SealRecord.

Poznámka 2: V poli CardHolderAuthorisation (CHA) certifikátu 2. generace se hodnoty (1), (2) a (6) vykládají jako hodnoty označující certifikát pro vzájemné ověření pravosti pro příslušný typ zařízení. K označení příslušného certifikátu pro vytvoření digitálního podpisu se musí použít hodnoty (17), (18) nebo (19).“;

h) v bodě 2.70 se znění za nadpisem „2. generace“ nahrazuje tímto:

„2. generace:

'0x'H	všeobecné události,
'00'H	žádné další podrobnosti,
'01'H	vložení neplatné karty,
'02'H	konflikt karet,
'03'H	časový přesah,
'04'H	jízda bez náležité karty,
'05'H	vložení karty během řízení,
'06'H	poslední relace karty nebyla korektně uzavřena,
'07'H	překročení povolené rychlosti,
'08'H	přerušení napájení,
'09'H	chyba údajů o pohybu vozidla,
'0A'H	nesoulad údajů o pohybu vozidla,
'0B'H	časový nesoulad (GNSS vůči vnitřním hodinám VU),
'0C'H	chyba komunikace se zařízením pro dálkovou komunikaci,
'0D'H	chybí informace o poloze z přijímače GNSS,
'0E'H	chyba komunikace s vnějším zařízením GNSS,
'0F'H	vyhrazeno pro budoucí použití,
'1x'H	události pokusů o narušení zabezpečení souvisejících s celkem ve vozidle,
'10'H	žádné další podrobnosti,
'11'H	chyba ověření pravosti snímače pohybu,
'12'H	chyba ověření pravosti karty tachografu,
'13'H	neoprávněná výměna snímače pohybu,
'14'H	chyba integrity vstupních dat karty,
'15'H	chyba integrity uložených uživatelských dat,
'16'H	vnitřní chyba přenosu dat,
'17'H	neoprávněné otevření krytu,
'18'H	poškození technického vybavení,
'19'H	detekce nedovolené manipulace s GNSS,
'1A'H	chyba ověření pravosti vnějšího zařízení GNSS,
'1B'H	skončila platnost certifikátu vnějšího zařízení GNSS,
'1C'H to '1F'H	vyhrazeno pro budoucí použití,
'2x'H	události pokusů o narušení zabezpečení souvisejících se snímačem,
'20'H	žádné další podrobnosti,
'21'H	chyba ověření pravosti,
'22'H	chyba integrity uložených dat,
'23'H	vnitřní chyba přenosu dat,
'24'H	neoprávněné otevření krytu,
'25'H	poškození technického vybavení,
'26'H to '2F'H	vyhrazeno pro budoucí použití,
'3x'H	závady záznamového zařízení,
'30'H	žádné další podrobnosti,
'31'H	interní závada celku ve vozidle,
'32'H	závada tiskárny,
'33'H	závada displeje,
'34'H	závada stahování,
'35'H	závada snímače,
'36'H	vnitřní přijímač GNSS,
'37'H	vnější zařízení GNSS,
'38'H	zařízení pro dálkovou komunikaci,
'39'H	rozhraní ITS,
'3A'H to '3F'H	vyhrazeno pro budoucí použití,
'4x'H	závady karty,
'40'H	žádné další podrobnosti,
'41'H to '4F'H	vyhrazeno pro budoucí použití,
'50'H to '7F'H	vyhrazeno pro budoucí použití,
'80'H to 'FF'H	specifické pro výrobce.“;

i) bod 2.71 se nahrazuje tímto:

„2.71 **ExtendedSealIdentifier**

2. generace:

Rozšířený identifikátor plomby jednoznačně identifikuje plombu (příloha IC požadavek 401).

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

manufacturerCode je kód výrobce plomby.

sealIdentifier je identifikátor plomby, který je jednoznačný pro výrobce.“;

j) body 2.78 a 2.79 se nahrazují tímto:

„2.78 **GNSSAccumulatedDriving**

2. generace:

Informace uložené na kartě řidiče nebo kartě dílny týkající se polohy vozidla dle GNSS, pokud součtová doba řízení dosáhne násobku tří hodin (příloha IC požadavky 306 a 354).

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

gnssADPointerNewestRecord je index naposledy aktualizovaného záznamu o součtové době řízení dle GNSS.

Přiřazení hodnoty je číslo odpovídající čítači záznamů o součtové době řízení dle GNSS, začínající hodnotou ‘0’ pro první výskyt záznamu o součtové době řízení dle GNSS ve struktuře.

gnssAccumulatedDrivingRecords je sada záznamů obsahujících datum a čas, kdy součtová doba řízení dosáhne násobku tří hodin, a informace o poloze vozidla.

2.79 **GNSSAccumulatedDrivingRecord**

2. generace:

Informace uložené na kartě řidiče nebo kartě dílny týkající se polohy vozidla dle GNSS, pokud součtová doba řízení dosáhne násobku tří hodin (příloha IC požadavky 305 a 353).

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

timeStamp je datum a čas, kdy součtová doba řízení dosáhne násobku tří hodin.

gnssPlaceRecord obsahuje informace týkající se polohy vozidla.

vehicleOdometerValue je stav počitadla ujetých kilometrů, kdy součtová doba řízení dosáhne násobku tří hodin.“;

k) bod 2.86 se nahrazuje tímto:

„2.86 **KeyIdentifier**

Jednoznačný identifikátor veřejného klíče použitý k odkazu na klíč a výběru klíče. Rovněž identifikuje držitele klíče.

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

První volba je vhodná k odkazu na veřejný klíč celku ve vozidle, karty tachografu nebo vnějšího zařízení GNSS.

Druhá volba je vhodná k odkazu na veřejný klíč celku ve vozidle (pokud výrobní číslo celku ve vozidle není známo v době vystavení certifikátu).

Třetí volba je vhodná k odkazu na veřejný klíč členského státu.“;

l) bod 2.92 se nahrazuje tímto:

„2.92 **MAC**

2. generace:

Kryptografický kontrolní součet délky 8, 12 nebo 16 bajtů odpovídající sadám šifer uvedeným v dodatku 11.

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

m) bod 2.111 se nahrazuje tímto:

„2.111 **NoOfGNSSADRecords**

2. generace:

Počet záznamů o součtové době řízení dle GNSS, které lze na kartu uložit.

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

Přiřazení hodnoty: viz dodatek 2.“;

n) v bodě 2.120 se přiřazení hodnoty ‘16H’ nahrazuje tímto:

„`'16'H` VuGNSSADRecord “;

o) bod 2.160 se nahrazuje tímto:

„2.160 **Vyhrazeno pro budoucí použití**“;

p) bod 2.162 se nahrazuje tímto:

„2.162 **TimeReal**

Kód pro kombinované pole data a času, kde datum a čas jsou vyjádřeny jako počet sekund uplynutých od 00h:00m:00s dne 1. ledna 1970 v časovém pásmu UTC.

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

Přiřazení hodnoty – oktetové uspořádání: počet sekund od půlnoci 1. ledna 1970 v časovém pásmu UTC.

Nejvyšší možný údaj data/času je v roce 2106.“;

q) bod 2.179 se nahrazuje tímto:

„2.179 **VuCardRecord**

2. generace:

Informace uložené v celku ve vozidle o použité kartě tachografu (příloha IC požadavek 132).

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

cardNumberAndGenerationInformation je celé číslo karty a generace použité karty (datový typ 2.74).

cardExtendedSerialNumber se načte ze souboru EF_ICC pod hlavním souborem (MF) karty.

cardStructureVersion se načte ze souboru EF_Application_Identification pod DF_Tachograph_G2.

cardNumber se načte ze souboru EF_Identification pod DF_Tachograph_G2.“;

r) body 2.203 a 2.204 se nahrazují tímto:

„2.203 **VuGNSSADRecord**

2. generace:

Informace uložené v celku ve vozidle týkající se polohy vozidla dle GNSS, pokud součtová doba řízení dosáhne násobku tří hodin (příloha IC požadavky 108 a 110).

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

timeStamp je datum a čas, kdy součtová doba řízení dosáhne násobku tří hodin.

cardNumberAndGenDriverSlot identifikuje kartu vloženou v otvoru pro kartu řidiče, včetně její generace.

cardNumberAndGenCodriverSlot identifikuje kartu vloženou v otvoru pro kartu druhého řidiče, včetně její generace.

gnssPlaceRecord obsahuje informace týkající se polohy vozidla.

vehicleOdometerValue je stav počitadla ujetých kilometrů, kdy součtová doba řízení dosáhne násobku tří hodin.

2.204 **VuGNSSADRecordArray**

2. generace:

Informace uložené v celku ve vozidle týkající se polohy vozidla dle GNSS, pokud součtová doba řízení dosáhne násobku tří hodin (příloha IC požadavky 108 a 110).

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

recordType označuje typ záznamu (VuGNSSADRecord).

Přiřazení hodnoty: viz RecordType.

recordSize je velikost záznamu VuGNSSADRecord v bajtech.

noOfRecords je počet záznamů v sadě záznamů.

records je sada záznamů o součtové době řízení dle GNSS.“;

s) body 2.230 a 2.231 se nahrazují tímto:

„2.230 Vyhrazeno pro budoucí použití.

2.231 Vyhrazeno pro budoucí použití.“;

t) v bodě 2.234 se znění za nadpisem „2. generace“ nahrazuje tímto:

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

Kromě prvků 1. generace se používají tyto datové prvky:

noOfGNSSADRecords je počet záznamů o součtové době řízení dle GNSS, které lze na kartu uložit.

noOfSpecificConditionRecords je počet záznamů o zvláštní podmínce, které lze na kartu uložit.

noOfCardVehicleUnitRecords je počet záznamů o použitých celcích ve vozidle, které lze na kartu uložit.“;

30) dodatek 2 se mění takto:

a) v bodě 1.1 se vkládají tyto zkratky:

„CHA autorizace držitele certifikátu

DO datový objekt“;

b) bod 3.3 se mění takto:

i) odstavec TCS_24 se nahrazuje tímto:

„TCS_24 Uvedené bezpečnostní podmínky mohou být spojeny takto:

AND: všechny bezpečnostní podmínky musí být splněny,

OR: alespoň jedna bezpečnostní podmínka musí být splněna.

Pravidla přístupu pro systém souborů, tj. pro příkazy SELECT, READ BINARY a UPDATE BINARY, jsou stanovena v kapitole 4. Pravidla přístupu pro zbývající příkazy jsou stanovena v následujících tabulkách. Výraz „nepoužije se“ je uveden v případě, že příkaz nemusí být podporován. V takovém případě může být příkaz podporován či nikoli, ale podmínka přístupu je mimo působnost.“;

ii) v odstavci TCS_25 se tabulka nahrazuje tímto:

„Příkaz	Karta řidiče	Karta dílny	Kontrolní karta	Karta podniku
External Authenticate				
— pro ověření pravosti 1. generace	ALW	ALW	ALW	ALW
— pro ověření pravosti 2. generace	ALW	PWD	ALW	ALW
Internal Authenticate	ALW	PWD	ALW	ALW
General Authenticate	ALW	ALW	ALW	ALW
Get Challenge	ALW	ALW	ALW	ALW
MSE:SET AT	ALW	ALW	ALW	ALW
MSE:SET DST	ALW	ALW	ALW	ALW
Process DSRC Message	Nepoužije se	Nepoužije se	Nepoužije se	Nepoužije se
PSO: Compute Digital Signature	ALW OR SM-MAC-G2	ALW OR SM-MAC-G2	Nepoužije se	Nepoužije se
PSO: Hash	Nepoužije se	Nepoužije se	ALW	Nepoužije se

Příkaz	Karta řidiče	Karta dílny	Kontrolní karta	Karta podniku
PERFORM HASH of FILE	ALW OR SM-MAC-G2	ALW OR SM-MAC-G2	Nepoužije se	Nepoužije se
PSO: Verify Certificate	ALW	ALW	ALW	ALW
PSO: Verify Digital Signature	Nepoužije se	Nepoužije se	ALW	Nepoužije se
Verify	Nepoužije se	ALW	Nepoužije se	Nepoužije se“

iii) v odstavci TCS_26 se tabulka nahrazuje tímto:

„Příkaz	Karta řidiče	Karta dílny	Kontrolní karta	Karta podniku
External Authenticate				
— pro ověření pravosti 1. generace	Nepoužije se	Nepoužije se	Nepoužije se	Nepoužije se
— pro ověření pravosti 2. generace	ALW	PWD	ALW	ALW
Internal Authenticate	Nepoužije se	Nepoužije se	Nepoužije se	Nepoužije se
General Authenticate	ALW	ALW	ALW	ALW
Get Challenge	ALW	ALW	ALW	ALW
MSE:SET AT	ALW	ALW	ALW	ALW
MSE:SET DST	ALW	ALW	ALW	ALW
Process DSRC Message	Nepoužije se	ALW	ALW	Nepoužije se
PSO: Compute Digital Signature	ALW OR SM-MAC-G2	ALW OR SM-MAC-G2	Nepoužije se	Nepoužije se
PSO: Hash	Nepoužije se	Nepoužije se	ALW	Nepoužije se
PERFORM HASH of FILE	ALW OR SM-MAC-G2	ALW OR SM-MAC-G2	Nepoužije se	Nepoužije se
PSO: Verify Certificate	ALW	ALW	ALW	ALW
PSO: Verify Digital Signature	Nepoužije se	Nepoužije se	ALW	Nepoužije se
Verify	Nepoužije se	ALW	Nepoužije se	Nepoužije se“

iv) v odstavci TCS_27 se tabulka nahrazuje tímto:

„Příkaz	Karta řidiče	Karta dílny	Kontrolní karta	Karta podniku
External Authenticate				
— pro ověření pravosti 1. generace	Nepoužije se	Nepoužije se	Nepoužije se	Nepoužije se
— pro ověření pravosti 2. generace	ALW	PWD	ALW	ALW
Internal Authenticate	Nepoužije se	Nepoužije se	Nepoužije se	Nepoužije se
General Authenticate	ALW	ALW	ALW	ALW
Get Challenge	ALW	ALW	ALW	ALW
MSE:SET AT	ALW	ALW	ALW	ALW
MSE:SET DST	ALW	ALW	ALW	ALW
Process DSRC Message	Nepoužije se	Nepoužije se	Nepoužije se	Nepoužije se
PSO: Compute Digital Signature	Nepoužije se	Nepoužije se	Nepoužije se	Nepoužije se
PSO: Hash	Nepoužije se	Nepoužije se	Nepoužije se	Nepoužije se
PERFORM HASH of FILE	Nepoužije se	Nepoužije se	Nepoužije se	Nepoužije se
PSO: Verify Certificate	ALW	ALW	ALW	ALW
PSO: Verify Digital Signature	Nepoužije se	Nepoužije se	Nepoužije se	Nepoužije se
Verify	Nepoužije se	ALW	Nepoužije se	Nepoužije se“

c) v bodě 3.4 se odstavec TCS_29 nahrazuje tímto:

„TCS_29 V každé zprávě s odpovědí jsou vrácena stavová slova SW1 SW2, která označují stav zpracování příkazu.

SW1	SW2	Význam
90	00	Normální zpracování
61	XX	Normální zpracování XX = počet dostupných bajtů odpovědi
62	81	Zpracování s varováním. Část vrácených dat může být poškozena.
63	00	Chyba ověření pravosti (varování)
63	CX	Chybné CHV (kód PIN). „X“ poskytuje stav čítače zbývajících pokusů.

SW1	SW2	Význam
64	00	Chyba provádění – stav paměti nezávislé na napájení nezměněn. Chyba integrity.
65	00	Chyba provádění – stav paměti nezávislé na napájení změněn.
65	81	Chyba provádění – stav paměti nezávislé na napájení změněn – porucha paměti.
66	88	Chyba zabezpečení: chybný kryptografický kontrolní součet (při bezpečném předávání zpráv) nebo chybný certifikát (při ověřování certifikátu) nebo chybný kryptogram (při externím ověřování pravosti) nebo chybný podpis (při ověřování podpisu)
67	00	Chybná délka (chybná hodnota Lc nebo Le)
68	83	Očekáván poslední příkaz řetězce
69	00	Zakázaný příkaz (žádná dostupná odpověď v T=0)
69	82	Bezpečnostní status nesplněn
69	83	Metoda ověření pravosti zablokována
69	85	Podmínky použití nesplněny
69	86	Nedovolený příkaz (žádný aktuální EF)
69	87	Chybí očekávané datové objekty bezpečného předávání zpráv.
69	88	Chybné datové objekty bezpečného předávání zpráv
6A	80	Chybné parametry v datovém poli
6A	82	Soubor nenalezen
6A	86	Chybné parametry P1-P2
6A	88	Odkazovaná data nenalezena
6B	00	Chybné parametry (offset mimo EF)
6C	XX	Chybná délka, SW2 udává přesnou délku. Není vráceno žádné datové pole.
6D	00	Kód instrukce není podporován nebo je neplatný.
6E	00	Třída není podporována.
6F	00	- Jiné chyby kontroly

Mohou být vrácena další stavová slova definovaná v normě ISO/IEC 7816-4, pokud jejich chování není výslovně uvedeno v tomto dodatku.

Volitelně mohou být vrácena například tato stavová slova:

6881: Logický kanál není podporován.

6882: Bezpečné předávání zpráv není podporováno.“;

d) v bodě 3.5.1.1 se poslední odrážka v odstavci TCS_38 nahrazuje tímto:

„— Je-li vybraná aplikace považována za poškozenou (v atributech souboru je detekována chyba integrity), je vrácen stav zpracování „**6400**“ nebo „**6500**“.“;

e) v bodě 3.5.1.2 se poslední odrážka v odstavci TCS_41 nahrazuje tímto:

„— Je-li vybraný soubor považován za poškozený (v atributech souboru je detekována chyba integrity), je vrácen stav zpracování „**6400**“ nebo „**6500**“.“;

f) v bodě 3.5.2.1 se šestá odrážka v odstavci TCS_43 nahrazuje tímto:

„— Je-li v atributech souboru zjištěna chyba integrity, karta považuje soubor za poškozený a neopravitelný a je vrácen stav zpracování „**6400**“ nebo „**6500**“.“;

g) bod 3.5.2.1.1 se mění takto:

i) v odstavci TCS_45 se tabulka nahrazuje tímto:

„Bajt	Délka	Hodnota	Popis
#1	1	„81h“	T_{PV}: tag pro otevřená data
#2	L	„NNh“ nebo „81 NNh“	L_{PV}: délka vrácených dat (= původní Le). L jsou 2 bajty, jestliže L_{PV} > 127 bajtů.
#(2+L)-#(1+L+NN)	NN	„XX..XXh“	Otevřená data
#(2+L+NN)	1	„99h“	Tag pro stav zpracování (SW1-SW2) – volitelný pro bezpečné předávání zpráv 1. generace
#(3+L+NN)	1	„02h“	Délka stavu zpracování – volitelná pro bezpečné předávání zpráv 1. generace
#(4+L+NN) - #(5+L+NN)	2	„XX XXh“	Stav zpracování nechráněné APDU odpovědi – volitelný pro bezpečné předávání zpráv 1. generace
#(6+L+NN)	1	„8Eh“	TCC: tag pro kryptografický kontrolní součet
#(7+L+NN)	1	„XXh“	LCC: délka následujícího kryptografického kontrolního součtu „04h“ pro bezpečné předávání zpráv 1. generace (viz dodatek 11 část A) „08h“, „0Ch“ nebo „10h“ v závislosti na délce klíče AES pro bezpečné předávání zpráv 2. generace (viz dodatek 11 část B)

„Bajt	Délka	Hodnota	Popis
#(8+L+NN)-#(7+M+L+NN)	M	„XX..XXh“	Kryptografický kontrolní součet
SW	2	„XXXXh“	Stavová slova (SW1, SW2)“

ii) v odstavci TCS_46 se tabulka nahrazuje tímto:

„Bajt	Délka	Hodnota	Popis
#1	1	„87h“	$T_{PI\ CG}$: tag pro šifrovaná data (kryptogram)
#2	L	„MMh“ nebo „81 MMh“	$L_{PI\ CG}$: délka vrácených šifrovaných dat (v důsledku doplnění odlišná od původního Le příkazu). L je 2 bajty, jestliže LPI CG > 127 bajtů.
#(2+L)-#(1+L+MM)	MM	„01XX..XXh“	Šifrovaná data: indikátor doplnění a kryptogram
#(2+L+MM)	1	„99h“	Tag pro stav zpracování (SW1-SW2) – volitelný pro bezpečné předávání zpráv 1. generace
#(3+L+MM)	1	„02h“	Délka stavu zpracování – volitelná pro bezpečné předávání zpráv 1. generace
#(4+L+MM) - #(5+L+MM)	2	„XX XXh“	Stav zpracování nechráněné APDU odpovědi – volitelný pro bezpečné předávání zpráv 1. generace
#(6+L+MM)	1	„8Eh“	TCC: tag pro kryptografický kontrolní součet
#(7+L+MM)	1	„XXh“	LCC: délka následujícího kryptografického kontrolního součtu „04h“ pro bezpečné předávání zpráv 1. generace (viz dodatek 11 část A) „08h“, „0Ch“ nebo „10h“ v závislosti na délce klíče AES pro bezpečné předávání zpráv 2. generace (viz dodatek 11 část B)
#(8+L+MM)-#(7+N+L+MM)	N	„XX..XXh“	Kryptografický kontrolní součet
SW	2	„XXXXh“	Stavová slova (SW1, SW2)“

h) v bodě 3.5.2.2 se šestá odrážka v odstavci TCS_50 nahrazuje tímto:

„— Je-li v atributech souboru zjištěna chyba integrity, karta považuje soubor za poškozený a neopravitelný a je vrácen stav zpracování „**6400**“ nebo „**6500**“.“;

i) v bodě 3.5.2.3 se odstavec TCS_52 mění takto:

i) poslední řádek tabulky se nahrazuje tímto:

„Le	1	„XXh“	Podle specifikace v ISO/IEC 7816-4“

ii) vkládá se nová věta, která zní:

„Je-li T=0, karta předpokládá hodnotu Le = „00h“, jestliže není použito bezpečné předávání zpráv.

Je-li T=1, je vrácen stav zpracování „6700“, jestliže Le = „01h“.“;

j) v bodě 3.5.2.3 se šestá odrážka v odstavci TCS_53 nahrazuje tímto:

„— Je-li v atributech souboru zjištěna chyba integrity, karta považuje soubor za poškozený a neopravitelný a je vrácen stav zpracování „**6400**“ nebo „**6500**“.“;

k) v bodě 3.5.3.2 se šestá odrážka v odstavci TCS_63 nahrazuje tímto:

„— Je-li v atributech souboru zjištěna chyba integrity, karta považuje soubor za poškozený a neopravitelný a je vrácen stav zpracování „**6400**“ nebo „**6500**“.“;

l) v bodě 3.5.5 se odstavec TCS_72 nahrazuje tímto:

„TCS_72 Kód PIN zadaný uživatelem musí být v kódování ASCII a IFD jej zprava doplní bajty „FFh“ na délku 8 bajtů, viz rovněž datový typ WorkshopCardPIN v dodatku 1.“;

m) v bodě 3.5.8 se odstavec TCS_95 nahrazuje tímto:

„TCS_95 Jestliže je příkaz INTERNAL AUTHENTICATE úspěšný, aktuální klíč relace 1. generace, pokud existuje, se vymaže a není nadále k dispozici. Aby byl k dispozici nový klíč relace 1. generace, musí být úspěšně proveden příkaz EXTERNAL AUTHENTICATE pro mechanismus ověření pravosti 1. generace.

Poznámka: klíče relace 2. generace viz dodatek 11 odstavce CSM_193 a CSM_195. Jsou-li vytvořeny klíče relace 2. generace a karta tachografu přijme otevřený příkaz INTERNAL AUTHENTICATE APDU, přeruší relaci bezpečného předávání zpráv 2. generace a zlikviduje klíče relace 2. generace.“;

n) v bodě 3.5.9 se odstavec TCS_97 nahrazuje tímto:

„TCS_97 Variantu příkazu pro vzájemné ověření pravosti druhé generace celku ve vozidle a karty lze provést v MF, DF Tachograph a DF Tachograph_G2, viz rovněž TCS_34. Jestliže je tento příkaz EXTERNAL AUTHENTICATE 2. generace úspěšný, aktuální klíč relace 1. generace, pokud existuje, se vymaže a není nadále k dispozici.

Poznámka: klíče relace 2. generace viz dodatek 11 odstavce CSM_193 a CSM_195. Jsou-li vytvořeny klíče relace 2. generace a karta tachografu přijme otevřený příkaz EXTERNAL AUTHENTICATE APDU, přeruší relaci bezpečného předávání zpráv 2. generace a zlikviduje klíče relace 2. generace.“;

o) v bodě 3.5.10 se v tabulce v odstavci TCS_101 doplňuje nový řádek, který zní:

„5 + L + 1	1	‘00h’	Podle specifikace v ISO/IEC 7816-4“

p) v bodě 3.5.11.2.3 se v odstavci TCS_114 doplňují nové pododstavce, které znějí:

„— Je-li currentAuthenticatedTime karty pozdější než datum skončení platnosti zvoleného veřejného klíče, je vrácen stav zpracování „**6A88**“.

Poznámka: Použije-li se pro ověření pravosti celku ve vozidle příkaz MSE: SET AT, je klíčem, na který se odkazuje, veřejný klíč VU_MA. Karta nastaví k použití veřejný klíč VU_MA, který odpovídá odkazu na držitele certifikátu (CHR) uvedenému v datovém poli příkazu, pokud jej má v paměti (karta dokáže veřejné klíče VU_MA identifikovat pomocí pole CHA certifikátu). Karta na tento příkaz vrátí „6A 88“, pokud je k dispozici pouze veřejný klíč VU_Sign nebo pokud není k dispozici žádný veřejný klíč celku ve vozidle. Viz definice pole CHA v dodatku 11 a datového typu equipmentType v dodatku 1.

Podobně v případě příkazu MSE: SET DST s odkazem na EQT (tj. celek ve vozidle nebo kartu) poslaného na kontrolní kartu je podle CSM_234 klíčem, na který se odkazuje, vždy klíč EQT_Sign, který se musí použít k ověření digitálního podpisu. Podle obrázku 13 v dodatku 11 bude na kontrolní kartě vždy uložen příslušný veřejný klíč EQT_Sign. V některých případech může být na kontrolní kartě uložen odpovídající veřejný klíč EQT_MA. Kontrolní karta vždy nastaví k použití veřejný klíč EQT_Sign, když obdrží příkaz MSE: SET DST.“;

q) bod 3.5.13 se mění takto:

i) odstavec TCS_121 se nahrazuje tímto:

„TCS_121 Dočasně uložená hodnota hash souboru se smaže, pokud je pomocí příkazu PERFORM HASH of FILE vypočítána nová hodnota hash souboru, pokud je zvolen DF a pokud je resetována karta tachografu.“;

ii) odstavec TCS_123 se nahrazuje tímto:

„TCS_123 Aplikace tachografu 2. generace podporuje algoritmus SHA-2 (SHA-256, SHA-384 nebo SHA-512), specifikovaný sadami šifer v dodatku 11 části B pro podpisový klíč karty Card_Sign.“;

iii) tabulka v odstavci TCS_124 se nahrazuje tímto:

„Bajt	Délka	Hodnota	Popis
CLA	1	„80h“	CLA
INS	1	„2Ah“	Provedení bezpečnostní operace
P1	1	„90h“	Tag: Hash
P2	1	„00h“	Algoritmus je implicitně znám. Pro aplikaci tachografu 1. generace: SHA-1 Pro aplikaci tachografu 2. generace: algoritmus SHA-2 (SHA-256, SHA-384 nebo SHA-512) definovaný sadou šifer v dodatku 11 části B pro podpisový klíč karty Card_Sign“

r) bod 3.5.14 se mění takto:

znění pod nadpisem až k odstavci TCS_126 se nahrazuje tímto:

„Tento příkaz se používá pro výpočet digitálního podpisu dříve vypočtené hodnoty hash (viz PERFORM HASH OF FILE, bod 3.5.13).

Tento příkaz musí podporovat jen karta řidiče a karta dílny v DF Tachograph a DF Tachograph_G2.

Ostatní typy karet tachografu mohou, ale nemusí tento příkaz implementovat. Pokud jde o aplikaci tachografu 2. generace, mají podpisový klíč 2. generace pouze karta řidiče a karta dílny, ostatní typy karet nemohou tento příkaz úspěšně provést a ukončí jej s vhodným chybovým kódem.

Příkaz může, ale nemusí být přístupný v MF. Pokud příkaz v MF přístupný není, skončí vhodným chybovým kódem.

Tento příkaz je v souladu s normou ISO/IEC 7816-8. Jeho použití je ale ve srovnání se související normou omezené.“;

s) bod 3.5.15 se mění takto:

i) tabulka v odstavci TCS_133 se nahrazuje tímto:

„Bajt	Délka	Hodnota	Popis
CLA	1	„00h“	CLA
INS	1	„2Ah“	Provedení bezpečnostní operace
P1	1	„00h“	
P2	1	„A8h“	Tag: datové pole obsahuje datové objekty relevantní pro ověření
Lc	1	„XXh“	Délka Lc následujícího datového pole
#6	1	„9Eh“	Tag pro digitální podpis
#7 nebo #7-#8	L	„NNh“ nebo „81 NNh“	Délka digitálního podpisu (L je 2 bajty, pokud je digitální podpis delší než 127 bajtů): 128 bajtů kódovaných podle dodatku 11 části A pro aplikaci tachografu 1. generace v závislosti na zvolené křivce pro aplikaci tachografu 2. generace (viz dodatek 11 část B).
#(7+L)-#(6+L+NN)	NN	„XX..XXh“	Obsah digitálního podpisu“

ii) v odstavci TCS_134 se doplňuje nová odrážka, která zní:

„— Jestliže vybraný veřejný klíč (použitý k ověření digitálního podpisu) má CHA.LSB (CertificateHolderAuthorisation.equipmentType), který není vhodný pro ověření digitálního podpisu podle dodatku 11, je vrácen stav zpracování „**6985**“.“;

t) bod 3.5.16 se mění takto:

i) v tabulce v odstavci TCS_138 se doplňuje nový řádek, který zní:

„5 + L + 1	1	„00h“	Podle specifikace v ISO/IEC 7816-4“

ii) v odstavci TCS_139 se doplňuje nový pododstavec, který zní:

„— „**6985**“ označuje, že časové razítko (4 bajty) uvedené v datovém poli příkazu je dřívější než hodnota cardValidityBegin nebo pozdější než hodnota cardExpiryDate.“;

u) bod 4.2.2 se mění takto:

i) v datové struktuře v odstavci TCS_154 se řádky od DF Tachograph G2 do EF CardMA_Certificate a řádky od EF GNSS_Places do konce tohoto odstavce nahrazují tímto:

”

Soubor / datový prvek	Počet záznamů	Velikost (bajty) Min	Max	Výchozí hodnoty
DF Tachograph_G2		*20268*	*40316*	
EF Application_Identification		*17*	*17*	
DriverCardApplicationIdentification		*17*	*17*	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfEventsPerType		1	1	{00}
noOfFaultsPerType		1	1	{00}
activityStructureLength		2	2	{00 00}
noOfCardVehicleRecords		2	2	{00 00}
noOfCardPlaceRecords		2	2	{00 00}
noOfGNSSADRecords		2	2	{00 00}
noOfSpecificConditionRecords		2	2	{00 00}
noOfCardVehicleUnitRecords		2	2	{00 00}
EF CardMA_Certificate		*204*	*341*	

...

EF GNSS_Places		*4538*	*6050*	
GNSSContinuousDriving		*4538*	*6050*	
gnssADPointerNewestRecord		2	2	{00 00}
gnssAccumulatedDrivingRecords		4536	6048	
GNSSContinuousDrivingRecord	n_8	*18*	*18*	
timeStamp		4	4	{00..00}
gnssPlaceRecord		14	14	
timeStamp		4	4	{00..00}
gnssAccuracy		1	1	{00}
geoCoordinates		6	6	{00..00}
vehicleOdometerValue		3	3	{00..00}

“

ii) v odstavci TCS_155 se položka NoOfGNSSCDRecords v tabulce nahrazuje tímto:

„n_8	NoOfGNSSADRecords	252	336“

v) v bodě 4.3.1 se znění odpovídající zkratce SC4 v odstavci TCS_156 nahrazuje tímto:

„**SC4** Pro příkaz READ BINARY se sudým bajtem INS:

(SM-C-MAC-G1 AND SM-R-ENC-MAC-G1) OR

(SM-C-MAC-G2 AND SM-R-ENC-MAC-G2)

Pro příkaz READ BINARY s lichým bajtem INS (je-li podporován): NEV“;

w) bod 4.3.2 se mění takto:

i) v datové struktuře v odstavci TCS_162 se řádky od DF Tachograph G2 do EF CardMA_Certificate, řádky od EF Calibration do extendedSealIdentifier a řádky od EF GNSS_Places do vehicleOdometerValue nahrazují tímto:

”

Soubor / datový prvek	Počet záznamů	Velikost (bajty) Min	Max	Výchozí hodnoty
DF Tachograph_G2	*1878*		*49787*	
EF Application_Identification	*19*		*19*	
WorkshopCardApplicationIdentificatio	*19*		*19*	
typeOfTachographCardId	1		1	{00}
cardStructureVersion	2		2	{00 00}
noOfEventsPerType	1		1	{00}
noOfFaultsPerType	1		1	{00}
activityStructureLength	2		2	{00 00}
noOfCardVehicleRecords	2		2	{00 00}
noOfCardPlaceRecords	2		2	{00 00}
noOfCalibrationRecords	2		2	{00 00}
noOfGNSSADRecords	2		2	{00 00}
noOfSpecificConditionRecords	2		2	{00 00}
noOfCardVehicleUnitRecords	2		2	{00 00}
EF CardMA_Certificate	*204*		*341*	
...				
EF Calibration		*15668*	*45394*	
WorkshopCardCalibrationData		*15668*	*45394*	
calibrationTotalNumber		2	2	{00 00}
calibrationPointerNewestRecord		2	2	{00}
calibrationRecords		*15664*	*45390*	
WorkshopCardCalibrationRecord	n_5	*178*	*178*	
calibrationPurpose		1	1	{00}
vehicleIdentificationNumber		17	17	{20..20}
vehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
wVehicleCharacteristicConstant		2	2	{00 00}
kConstantOfRecordingEquipment		2	2	{00 00}
lTyreCircumference		2	2	{00 00}
tyreSize		15	15	{20..20}
authorisedSpeed		1	1	{00}
oldOdometerValue		3	3	{00..00}
newOdometerValue		3	3	{00..00}
oldTimeValue		4	4	{00..00}
newTimeValue		4	4	{00..00}
nextCalibrationDate		4	4	{00..00}
vuPartNumber		16	16	{20..20}
vuSerialNumber		8	8	{00..00}
sensorSerialNumber		8	8	{00..00}
sensorGNSSSerialNumber		8	8	{00..00}
rcmSerialNumber		8	8	{00..00}
vuAbility		1	1	{00}
sealDataCard		56	56	
noOfSealRecords		1	1	{00}
SealRecords		55	55	
SealRecord	5	11	11	
equipmentType		1	1	{00}
extendedSealIdentifier		10	10	{00..00}

...

EF GNSS_Places		*326*	*434*	
└GNSSContinuousDriving		*326*	*434*	
├gnssADPointerNewestRecord		2	2	{00 00}
└gnssAccumulatedDrivingRecords		324	432	
└GNSSContinuousDrivingRecord	n_8	*18*	*18*	
├timeStamp		4	4	{00..00}
└gnssPlaceRecord		14	14	
├timeStamp		4	4	{00..00}
├gnssAccuracy		1	1	{00}
├geoCoordinates		6	6	{00..00}
vehicleOdometerValue		3	3	{00..00}

“

ii) položka NoOfGNSSCDRecords v tabulce v odstavci TCS_163 se nahrazuje tímto:

„n_8	NoOfGNSSADRecords	18	24“

31) v dodatku 3 se bod 2 mění takto:

a) za řádek s piktogramy „místo začátku denní pracovní doby“ a „místo konce denní pracovní doby“ se vkládá nový řádek, který zní:

„ poloha po třech hodinách součtové doby řízení“;

b) kombinace piktogramů „nastavení času (dílnou)“ se nahrazuje tímto:

„ časový konflikt nebo nastavení času (dílnou)“;

c) na seznam Události se přidávají tyto kombinace piktogramů:

„ chybí informace o poloze z přijímače GNSS nebo chyba komunikace s vnějším zařízením GNSS;

chyba komunikace se zařízením pro dálkovou komunikaci“;

32) dodatek 4 se mění takto:

a) bod 2 se mění takto:

i) blok číslo 11.4 se nahrazuje tímto:

„11.4 *Zadání místa začátku a/nebo konce denní pracovní doby*

pi=piktogram místa začátku/konce, čas, země, region, zeměpisná délka zaznamenané polohy, zeměpisná šířka zaznamenané polohy, časové razítko, kdy byla poloha stanovena, stav počitadla ujetých kilometrů	pihh:mm Cou Reg lon ±DDD°MM.M’ lat ± DD°MM.M’ hh:mm x xxx xxx **km**“

ii) blok číslo 11.5 se nahrazuje tímto:

„11.5 *Polohy po třech hodinách součtové doby řízení*
pi=poloha po třech hodinách součtové doby řízení,

čas,
zeměpisná délka zaznamenané polohy,
zeměpisná šířka zaznamenané polohy,
časové razítko, kdy byla poloha stanovena,
stav počitadla ujetých kilometrů

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

b) v bodě 3.1 se pozice 11.5 formátu denního výtisku nahrazuje tímto:

„11.5	Polohy po třech hodinách součtové doby řízení v chronologickém pořadí“

c) v bodě 3.2 se formát denního výtisku nahrazuje tímto:

„1	Datum a čas vytištění dokumentu
2	Typ výtisku
3	Identifikace držitele karty (pro všechny karty vložené do VU, + GEN)
4	Identifikace vozidla (z nějž se výtisk pořizuje)
5	Identifikace VU (VU, z nějž se výtisk pořizuje, + GEN)
6	Poslední kalibrace tohoto VU
7	Poslední kontrola tohoto tachografu
9	Oddělovač činností řidiče
10	Oddělovač otvoru pro kartu řidiče (otvor č. 1)
10a	Na začátku tohoto dne platila podmínka „mimo působnost“
10.1 / 10.2 / 10.3 / 10.3a / 10.4	Činnosti v chronologickém pořadí (otvor pro kartu řidiče)
10	Oddělovač otvoru pro kartu druhého řidiče (otvor č. 2)
10a	Na začátku tohoto dne platila podmínka „mimo působnost“
10.1 / 10.2 / 10.3 / 10.3a / 10.4	Činnosti v chronologickém pořadí (otvor pro kartu druhého řidiče)
11	Oddělovač denního souhrnu
11.1	Souhrn dob bez karty v otvoru pro kartu řidiče
11.4	Zadaná místa v chronologickém pořadí
11.5	Polohy po třech hodinách součtové doby řízení v chronologickém pořadí
11.7	Celkové doby trvání činností
11.2	Souhrn dob bez karty v otvoru pro kartu druhého řidiče
11.4	Zadaná místa v chronologickém pořadí
11.5	Polohy po třech hodinách součtové doby řízení v chronologickém pořadí

11.8	Celkové doby trvání činností
11.3	Souhrn činností řidiče při zahrnutí obou otvorů pro kartu
11.4	Místa zadaná tímto řidičem v chronologickém pořadí
11.5	Polohy po třech hodinách součtové doby řízení v chronologickém pořadí
11.9	Celkové doby trvání činností tohoto řidiče
13.1	Oddělovač událostí a závad
13.4	Záznamy událostí/závad (posledních 5 událostí nebo závad uložených nebo probíhajících ve VU)
22.1	Místo kontroly
22.2	Podpis kontrolora
22.3	Čas začátku (místo, kde může řidič bez karty uvést,
22.4	Čas konce která období se ho týkají)
22.5	Podpis řidiče“

d) v bodě 3.7 se odstavec PRT_014 nahrazuje tímto:

„PRT_014 Výtisk historie vložených karet musí mít následující formát:

1	Datum a čas vytištění dokumentu
2	Typ výtisku
3	Identifikace držitelů karty (pro všechny karty vložené do VU)
23	Karta naposledy vložená do VU
23.1	Vložené karty (až 88 záznamů)
12.3	Oddělovač závad“

33) dodatek 7 se mění takto:

a) bod 1.1 se nahrazuje tímto:

„1.1 **Oblast působnosti**

Data mohou být stažena na externí paměťové médium:

— z celku ve vozidle inteligentním vyhrazeným zařízením (IDE) připojeným k celku ve vozidle,

— z karty tachografu pomocí IDE vybaveného kartovým rozhraním (IFD),

— z karty tachografu prostřednictvím celku ve vozidle pomocí IDE připojeného k celku ve vozidle.

Aby bylo možné zkontrolovat pravost a integritu stažených dat uložených na externí paměťové médium, stahují se data s připojeným podpisem v souladu s dodatkem 11 „Společné bezpečnostní mechanismy“. Rovněž se stahuje identifikace zdrojového zařízení (VU nebo karty) a jeho bezpečnostní certifikáty (členského státu a zařízení). Ověřovatel dat musí mít nezávisle získaný důvěryhodný evropský veřejný klíč.

Data stažená z celku ve vozidle se opatří podpisem v souladu s dodatkem 11 „Společné bezpečnostní mechanismy“ částí B („Systém tachografu druhé generace“), vyjma případů, kdy kontrolu řidičů provádí kontrolní orgán, který nepatří do EU, za použití kontrolní karty první generace a kdy se data opatří podpisem v souladu dodatkem 11 „Společné bezpečnostní mechanismy“ částí A („Systém tachografu první generace“), v souladu s dodatkem 15 Migrace požadavkem MIG_015.

Tento dodatek tudíž stanoví dva typy stahování dat z celku ve vozidle:

— stahování dat z celku ve vozidle typu 2. generace, poskytující datovou strukturu 2. generace a opatřené podpisem v souladu s dodatkem 11 „Společné bezpečnostní mechanismy“ částí B,

— stahování dat z celku ve vozidle typu 1. generace, poskytující datovou strukturu 1. generace a opatřené podpisem v souladu s dodatkem 11 „Společné bezpečnostní mechanismy“ částí A.

Podobně existují dva typy stahování dat z karet řidiče druhé generace vložených do celku ve vozidle, jak je uvedeno v bodech 3 a 4 tohoto dodatku.“;

b) bod 2.2.2 se mění takto:

i) tabulka se nahrazuje tímto:

„Struktura zprávy	Max. 4 bajty Hlavička				Max. 255 bajtů Data			1 bajt Kontrolní součet
IDE -> **<- VU**	FMT	TGT	SRC	LEN	SID	DS_ / TRTP	DATA	CS
Start Communication Request	81	EE	F0		81			E0
Positive Response Start Communication	80	F0	EE	03	C1		EA, 8F	9B
Start Diagnostic Session Request	80	EE	F0	02	10	81		F1
Positive Response Start Diagnostic	80	F0	EE	02	50	81		31
Link Control Service								
Verify Baud Rate (stage 1)								
9 600 Bd	80	EE	F0	04	87		01,01,01	EC
19 200 Bd	80	EE	F0	04	87		01,01,02	ED
38 400 Bd	80	EE	F0	04	87		01,01,03	EE
57 600 Bd	80	EE	F0	04	87		01,01,04	EF
115 200 Bd	80	EE	F0	04	87		01,01,05	F0
Positive Response Verify Baud Rate	80	F0	EE	02	C7		01	28
Transition Baud Rate (stage 2)	80	EE	F0	03	87		02,03	ED
Request Upload	80	EE	F0	0A	35		00,00,00,00-,00,FF,FF,FF,FF	99
Positive Response Request Upload	80	F0	EE	03	75		00,FF	D5
Transfer Data Request								
Overview	80	EE	F0	02	36	01 nebo 21		97
Activities	80	EE	F0	06	36	02 nebo 22	Date	CS
Events & Faults	80	EE	F0	02	36	03 nebo 23		99
Detailed Speed	80	EE	F0	02	36	04 nebo 24		9A
Technical Data	80	EE	F0	02	36	05 nebo 25		9B
Card download	80	EE	F0	02	36	06	Slot	CS

Struktura zprávy	Max. 4 bajty Hlavička				Max. 255 bajtů Data			1 bajt Kontrolní součet
IDE -> **<- VU**	FMT	TGT	SRC	LEN	SID	DS_ / TRTP	DATA	CS
Positive Response Transfer Data	80	F0	EE	Len	76	TREP	Data	CS
Request Transfer Exit	80	EE	F0	01	37			96
Positive Response Request Transfer Exit	80	F0	EE	01	77			D6
Stop Communication Request	80	EE	F0	01	82			E1
Positive Response Stop Communication	80	F0	EE	01	C2			21
Acknowledge sub message	80	EE	F0	Len	83		Data	CS
Negative responses								
General reject	80	F0	EE	03	7F	Sid Req	10	CS
Service not supported	80	F0	EE	03	7F	Sid Req	11	CS
Sub function not supported	80	F0	EE	03	7F	Sid Req	12	CS
Incorrect Message Length	80	F0	EE	03	7F	Sid Req	13	CS
Conditions not correct or Request sequence error	80	F0	EE	03	7F	Sid Req	22	CS
Request out of range	80	F0	EE	03	7F	Sid Req	31	CS
Upload not accepted	80	F0	EE	03	7F	Sid Req	50	CS
Response pending	80	F0	EE	03	7F	Sid Req	78	CS
Data not available	80	F0	EE	03	7F	Sid Req	FA	CS“

ii) v části Poznámky za tabulkou se doplňují nové odrážky, které znějí:

„— TRTP 21 až 25 se použijí pro požadavky na stahování dat z VU 2. generace, TRTP 01 až 05 se použijí pro požadavky na stahování dat z VU 1. generace, které může VU akceptovat pouze v rámci kontroly řidičů prováděné kontrolním orgánem, který nepatří do EU, za použití kontrolní karty první generace,

— TRTP 11 až 19 a 31 až 39 jsou vyhrazeny pro specifické požadavky výrobce na stahování.“;

c) bod 2.2.2.9 se mění takto:

i) odstavec DDP_011 se nahrazuje tímto:

„DDP_011 Zprávu Transfer Data Request posílá IDE, aby informovalo VU, jaký typ dat se má stahovat. Jednobajtový parametr TRTP udává typ přenosu.

Existuje šest typů přenosu dat. V případě stahování dat z VU lze pro každý přenos dat použít dvě různé hodnoty TRTP:

Typ přenosu dat	Hodnota TRTP pro stahování dat z VU typu 1. generace	Hodnota TRTP pro stahování dat z VU typu 2. generace
přehled (*Overview*)	01	21
činnosti v daný den (*Activities of a specified date*)	02	22
události a chyby (*Events and faults*)	03	23
podrobnosti o rychlosti (*Detailed speed*)	04	24
technická data (*Technical data*)	05	25

Typ přenosu dat	Hodnota TRTP
stahování z karty (*Card download*)	06“

ii) odstavec DDP_054 se nahrazuje tímto:

„DDP_054 IDE v rámci relace stahování povinně žádá o přenos dat přehledu (TRTP 01 nebo 21), neboť jedině tak lze zajistit, že ve staženém souboru budou zaznamenány certifikáty VU (a bude možné ověřit digitální podpis).

Ve druhém případě (TRTP 02 nebo 22) zpráva *Transfer Data Request* obsahuje kalendářní den (ve formátu `TimeReal`), za který se mají data stáhnout.“;

d) v bodě 2.2.2.10 se odstavec DDP_055 nahrazuje tímto:

„DDP_055 V prvním případě (TREP 01 nebo 21) VU pošle data, která operátorovi IDE pomohou vybrat data, která chce dále stáhnout. Informace obsažené v této zprávě jsou:

— bezpečnostní certifikáty,

— identifikace vozidla,

— aktuální datum a čas VU,

— minimální a maximální datum, za které lze data stáhnout(data VU),

— indikace přítomnosti karet ve VU,

— předešlé stažení dat podnikem,

— zámky podniku,

— předešlé kontroly.“;

e) v bodě 2.2.2.16 se poslední odrážka v odstavci DDP_018 nahrazuje tímto:

„— FA Data not available (data nejsou k dispozici)

Datový objekt požadavku na přenos dat není ve VU k dispozici (např. není vložená žádná karta, požadavek na stažení dat z VU typu 1. generace je mimo rámec kontroly řidiče kontrolním orgánem, který nepatří do EU, …).“;

f) bod 2.2.6.1 se mění takto:

i) v odstavci DDP_029 se první pododstavec nahrazuje tímto:

„Datové pole zprávy *Positive Response Transfer Data Overview* musí obsahovat následující data v uvedeném pořadí, přičemž se použije SID 76 hex, TREP 01 nebo 21 hex a patřičné rozdělení do dílčích zpráv a jejich počítání:“;

ii) nadpis „Datová struktura 1. generace“ se nahrazuje tímto:

„Datová struktura 1. generace (TREP 01 hex)“;

iii) nadpis „Datová struktura 2. generace“ se nahrazuje tímto:

„Datová struktura 2. generace (TREP 21 hex)“;

g) bod 2.2.6.2 se mění takto:

i) v odstavci DDP_030 se první pododstavec nahrazuje tímto:

„Datové pole zprávy *Positive Response Transfer Data Activities* musí obsahovat následující data v uvedeném pořadí, přičemž se použije SID 76 hex, TREP 02 nebo 22 hex a patřičné rozdělení do dílčích zpráv a jejich počítání:“;

ii) nadpis „Datová struktura 1. generace“ se nahrazuje tímto:

„Datová struktura 1. generace (TREP 02 hex)“;

iii) nadpis „Datová struktura 2. generace“ se nahrazuje tímto:

„Datová struktura 2. generace (TREP 22 hex)“;

iv) položka VuGNSSCDRecordArray pod nadpisem „Datová struktura 2. generace (TREP 22 hex)“ se nahrazuje tímto:

„VuGNSSADRecordArray	Polohy vozidla dle GNSS, když součtová doba řízení vozidla dosáhne násobku tří hodin. Pokud je tato sekce prázdná, odešle se hlavička pole s noOfRecords = 0.“

h) bod 2.2.6.3 se mění takto:

i) v odstavci DDP_031 se první pododstavec nahrazuje tímto:

„Datové pole zprávy *Positive Response Transfer Data Events and Faults* musí obsahovat následující data v uvedeném pořadí, přičemž se použije SID 76 hex, TREP 03 nebo 23 hex a patřičné rozdělení do dílčích zpráv a jejich počítání:“;

ii) nadpis „Datová struktura 1. generace“ se nahrazuje tímto:

„Datová struktura 1. generace (TREP 03 hex)“;

iii) nadpis „Datová struktura 2. generace“ se nahrazuje tímto:

„Datová struktura 2. generace (TREP 23 hex)“;

iv) položka VuTimeAdjustmentGNSSRecordArray pod nadpisem „Datová struktura 2. generace (TREP 23 hex)“ se zrušuje;

i) bod 2.2.6.4 se mění takto:

i) v odstavci DDP_032 se první pododstavec nahrazuje tímto:

„Datové pole zprávy *Positive Response Transfer Data Detailed Speed* musí obsahovat následující data v uvedeném pořadí, přičemž se použije SID 76 hex, TREP 04 nebo 24 hex a patřičné rozdělení do dílčích zpráv a jejich počítání:“;

ii) nadpis „Datová struktura 1. generace“ se nahrazuje tímto:

„Datová struktura 1. generace (TREP 04)“;

iii) nadpis „Datová struktura 2. generace“ se nahrazuje tímto:

„Datová struktura 2. generace (TREP 24)“;

j) bod 2.2.6.5 se mění takto:

i) v odstavci DDP_033 se první pododstavec nahrazuje tímto:

„Datové pole zprávy *Positive Response Transfer Data Technical Data* musí obsahovat následující data v uvedeném pořadí, přičemž se použije SID 76 hex, TREP 05 nebo 25 hex a patřičné rozdělení do dílčích zpráv a jejich počítání:“;

ii) nadpis „Datová struktura 1. generace“ se nahrazuje tímto:

„Datová struktura 1. generace (TREP 05)“;

iii) nadpis „Datová struktura 2. generace“ se nahrazuje tímto:

„Datová struktura 2. generace (TREP 25)“;

k) v bodě 3.3 se odstavec DDP_035 nahrazuje tímto:

„DDP_035 Stahování z karty tachografu zahrnuje následující kroky:

— Stažení společných informací karty v elementárních souborech (EF) `ICC` a `IC`. Tyto informace jsou nepovinné a nejsou zabezpečeny digitálním podpisem.

— (U karet tachografu první a druhé generace) stažení EF v rámci `Tachograph DF`:

— Stažení EF `Card_Certificate` a `CA_Certificate`. Tyto informace nejsou zabezpečeny digitálním podpisem.

Tyto soubory musí být povinně staženy v rámci každé relace stahování.

— Stažení EF s dalšími daty aplikace (v rámci `Tachograph DF`) kromě EF `Card_Download`. Tyto informace jsou zabezpečeny digitálním podpisem za použití mechanismů v souladu s dodatkem 11 „Společné bezpečnostní mechanismy“ částí A.

— V každé relaci stahování musí být povinně staženy alespoň EF `Application_Identification` a `Identification`.

— Při stahování z karty řidiče musí být rovněž povinně staženy tyto EF:

— `Events_Data`,

— `Faults_Data`,

— Driver_Activity_Data,

— Vehicles_Used,

— Places,

— Control_Activity_Data,

— Specific_Conditions,

— (Pouze u karet tachografu druhé generace) kromě případů, kdy stahování z karty řidiče vložené do VU provádí během kontroly řidičů kontrolní orgán, který nepatří do EU, za použití kontrolní karty první generace, stažení EF v rámci Tachograph_G2 DF DF:

— Stažení EF CardSignCertificate, CA_Certificate a Link_Certificate (je-li k dispozici). Tyto informace nejsou zabezpečeny digitálním podpisem.

Tyto soubory musí být povinně staženy v rámci každé relace stahování.

— Stažení EF s dalšími daty aplikace (v rámci Tachograph_G2 DF DF) kromě EF Card_Download. Tyto informace jsou zabezpečeny digitálním podpisem za použití mechanismů v souladu s dodatkem 11 „Společné bezpečnostní mechanismy“ částí B.

— V každé relaci stahování musí být povinně staženy alespoň EF Application_Identification a Identification.

— Při stahování z karty řidiče musí být rovněž povinně staženy tyto EF:

— Events_Data,

— Faults_Data,

— Driver_Activity_Data,

— Vehicles_Used,

— Places,

— Control_Activity_Data,

— Specific_Conditions,

— VehicleUnits_Used,

— GNSS Places.

— Při stahování z karty řidiče aktualizujte datum LastCardDownload v EF Card_Download v DF Tachograph a případně Tachograph_G2 .

— Při stahování z karty dílny vynulujte počítadlo kalibrací v EF Card_Download v DF Tachograph a případně Tachograph_G2 .

— Při stahování z karty dílny se nestahuje EF `Sensor_Installation_Data` v DF `Tachograph` a případně `Tachograph_G2` .“;

l) v bodě 3.3.2 se první pododstavec odstavce DDP_037 nahrazuje tímto:

„Sekvence stahování EF ICC, IC, Card_Certificate (nebo CardSignCertificate pro DF Tachograph_G2), CA_Certificate a Link_Certificate (pouze pro DF Tachograph_G2) je následující:“;

m) v bodě 3.3.3 se tabulka nahrazuje tímto:

„Karta	Směr	IDE/IFD	Význam/poznámky
	⇦	**Select File**	
OK	⇨		
	⇦	**Perform Hash of File**	— Vypočte hodnotu hash dat obsažených ve vybraném souboru pomocí předepsaného hašovacího algoritmu podle dodatku 11 části A nebo B. Tento příkaz není příkazem ISO.
Výpočet hodnoty hash souboru a dočasné uložení hodnoty hash			
OK	⇨		
	⇦	**Read Binary**	Pokud soubor obsahuje více dat, než pojme vyrovnávací paměť čtečky nebo karty, je třeba příkaz opakovat, dokud není přečten celý soubor.
Data souboru **OK**	⇨	Uložení přijatých dat na ESM	Podle bodu **3.4** Data storage format
	⇦	**PSO: Compute Digital Signature**	
Provedení bezpečnostní operace *Compute Digital Signature* (výpočet digitálního podpisu) pomocí dočasně uložené hodnoty hash			
Podpis **OK**	⇨	Připojení dat k datům dříve uloženým na ESM	Podle bodu **3.4** Data storage format“

n) v bodě 3.4.2 se odstavec DDP_046 nahrazuje tímto:

„DDP_046 Podpis se uloží jako následující objekt TLV bezprostředně za objekt TLV, který obsahuje data souboru.

Definice	Význam	Délka
FID (2 bajty) || „00“	Tag pro EF (FID) v DF Tachograph nebo pro společné informace karty	3 bajty
FID (2 bajty) || „01“	Tag pro podpis EF (FID) v DF Tachograph	3 bajty
FID (2 bajty) || „02“	Tag pro EF (FID) v DF Tachograph_G2	3 bajty
FID (2 bajty) || „03“	Tag pro podpis EF (FID) v DF Tachograph_G2	3 bajty
xx xx	Délka pole s hodnotou	2 bajty

Příklad stažených dat v souboru na ESM:

Tag	Délka	Hodnota
00 02 00	00 11	— Data EF ICC
C1 00 00	00 C2	— Data EF Card_Certificate
		— …
05 05 00	0A 2E	Data EF Vehicles_Used (v DF Tachograph)
05 05 01	00 80	Podpis EF Vehicles_Used (v DF Tachograph)
05 05 02	0A 2E	Data EF Vehicles_Used v DF Tachograph_G2
05 05 03	xx xx	Podpis EF Vehicles_Used v DF Tachograph_G2 “

o) v bodě 4 se odstavec DDP_049 nahrazuje tímto:

„DDP_049 Karty řidiče první generace: data se stahují pomocí protokolu pro stahování dat první generace a stažená data mají stejný formát jako data stažená z celku ve vozidle první generace.

Karty řidiče druhé generace: VU poté stáhne data z celé karty, soubor po souboru, v souladu s protokolem pro stahování z karty definovaným v odstavci 3 a přepošle všechna data přijatá z karty do IDE v patřičném formátu souboru TLV (viz bod 3.4.2) a zapouzdřená ve zprávě *Positive Response Transfer Data*.“;

34) v dodatku 8 se v bodě 2 pododstavec pod nadpisem „Odkazy“ nahrazuje tímto:

„ISO 14230-2: Road Vehicles – Diagnostic Systems – Keyword Protocol 2000 – Part 2: Data Link Layer.

First edition: 1999 (Silniční vozidla – Diagnostické systémy – Protokol klíčových slov 2000 – Část 2: Spojová vrstva. První vydání: 1999).“;

35) dodatek 9 se mění takto:

a) v obsahu se bod 6 nahrazuje tímto:

„6 ZKOUŠKY VNĚJŠÍHO ZAŘÍZENÍ PRO DÁLKOVOU KOMUNIKACI“;

b) v bodě 1.1 se první odrážka nahrazuje tímto:

„— **osvědčení bezpečnosti**, které vychází ze specifikací *Common Criteria*, vůči bezpečnostnímu cíli, který je plně v souladu s dodatkem 10 této přílohy,“;

c) v bodě 2 se tabulka funkčních zkoušek celku ve vozidle nahrazuje tímto:

„Č.	Zkouška	Popis	Související požadavky
1	**Administrativní šetření**		
1.1	Dokumentace	Správnost dokumentace	
1.2	Výsledky zkoušek výrobce	Výsledky zkoušek výrobce provedených při integraci. Předložení písemných dokladů.	88, 89, 91
2	**Vizuální kontrola**		
2.1	Shoda s dokumentací		
2.2	Identifikace/značení		224 až 226
2.3	Materiály		219 až 223
2.4	Plomby		398, 401 až 405
2.5	Vnější rozhraní		
3	**Funkční zkoušky**		
3.1	Poskytované funkce		02, 03, 04, 05, 07, 382
3.2	Provozní režimy		09 až 11*, 134, 135
3.3	Přístupová práva k funkcím a datům		12* 13*, 382, 383, 386 až 389
3.4	Sledování vkládání a vyjímání karet		15, 16, 17, 18, 19*, 20*, 134
3.5	Měření rychlosti a vzdálenosti		21 až 31
3.6	Měření času (zkouška při 20 °C)		38 až 43
3.7	Sledování činností řidiče		44 až 53, 134
3.8	Sledování stavu řízení		54, 55, 134
3.9	Ruční vkládání		56 až 62
3.10	Správa zámků podniku		63 až 68
3.11	Sledování kontrolních činností		69, 70
3.12	Detekce událostí a/nebo závad		71 až 88, 134

Č.	Zkouška	Popis	Související požadavky
3.13	Identifikační údaje zařízení		93*, 94*, 97, 100
3.14	Údaje o vložení a vyjmutí karty řidiče		102* až 104*
3.15	Údaje o činnostech řidiče		105* až 107*
3.16	Údaje o místech a polohách		108* až 112*
3.17	Údaje počitadla ujetých kilometrů		113* až 115*
3.18	Podrobné údaje o rychlosti		116*
3.19	Údaje o událostech		117*
3.20	Údaje o závadách		118*
3.21	Kalibrační údaje		119* až 121*
3.22	Údaje o nastavení času		124*, 125*
3.23	Údaje o kontrolních činnostech		126*, 127*
3.24	Údaje o zámcích podniku		128*
3.25	Údaje o stahování dat		129*
3.26	Údaje o zvláštních podmínkách		130*, 131*
3.27	Záznam a ukládání dat na kartách tachografu		136, 137, 138*, 139*, 141*, 142, 143 144, 145, 146*, 147*, 148*, 149, 150
3.28	Zobrazení		90, 134, 151 až 168, PIC_001, DIS_001
3.29	Tisk		90, 134, 169 až 181, PIC_001, PRT_001 až PRT_014
3.30	Varování		134, 182 až 191, PIC_001
3.31	Stahování dat na externí paměťová média		90, 134, 192 až 196
3.32	Dálková komunikace pro cílené silniční kontroly		197 až 199
3.33	Výstup dat do dalších vnějších zařízení		200, 201
3.34	Kalibrace		202 až 206*, 383, 384, 386 až 391
3.35	Silniční kontrola kalibrace		207 až 209
3.36	Nastavení času		210 až 212*
3.37	Neovlivnění přídavnými funkcemi		06, 425

Č.	Zkouška	Popis	Související požadavky
3.38	Rozhraní snímače pohybu		02, 122
3.39	Vnější zařízení GNSS		03, 123
3.40	Ověřit, že celek ve vozidle detekuje, zaznamenává a ukládá události a/nebo závady definované jeho výrobcem, když spárovaný snímač pohybu reaguje na magnetická pole, která narušují detekci pohybu vozidla.		217
3.41	Sada šifer a standardizované parametry domény		CSM_48, CSM_50
4	**Zkoušky vlivů prostředí**		
4.1	Teplota	Ověřit funkčnost podle těchto zkoušek: Zkouška podle ISO 16750-4, kapitoly 5.1.1.2: provozní zkouška při nízké teplotě (72 h při – 20 °C) Tato zkouška odkazuje na IEC 60068-2-1: Zkoušení vlivů prostředí– Část 2-1: Zkoušky– Zkouška A: Chlad Zkouška podle ISO 16750-4, kapitoly 5.1.2.2: provozní zkouška při vysoké teplotě (72 h při 70 °C) Tato zkouška odkazuje na IEC 60068-2-2: Zkoušení vlivů prostředí – Část 2-2: Zkoušky – Zkouška B: Suché teplo Zkouška podle ISO 16750-4, kapitoly 5.3.2: Rychlá změna teploty se stanovenou dobou přechodu (– 20 °C/70 °C, 20 cyklů, prodleva 2 h při každé teplotě) Při nižší teplotě, při vyšší teplotě a během teplotních cyklů lze provádět omezený soubor zkoušek (z těch, které jsou definovány v části 3 této tabulky).	213
4.2	Vlhkost	Ověřit, že celek ve vozidle vydrží cyklickou zkoušku vlhkostí (zkouška teplem) podle IEC 60068-2-30 – Zkouška Db, šest 24hodinových cyklů, každý se změnou teploty od + 25 °C do + 55 °C a relativní vlhkostí 97 % při + 25 °C a 93 % při + 55 °C	214
4.3	Mechanické vlivy	1. Sinusové vibrace: Ověřit, že celek ve vozidle vydrží sinusové vibrace s těmito parametry: konstantní výchylka mezi 5 a 11 Hz: max. 10 mm, konstantní zrychlení mezi 11 a 300 Hz: 5 g. Tento požadavek se ověřuje podle IEC 60068-2-6 – Zkouška Fc o délce nejméně 3 × 12 hod (12 hod na každou osu). ISO 16750-3 nevyžaduje zkoušku sinusovými vibracemi u zařízení umístěných v odpružené kabině vozidla.	219

Č.	Zkouška	Popis	Související požadavky
		2. Náhodné vibrace: Zkouška podle ISO 16750-3, kapitoly 4.1.2.8: Zkouška VIII: Užitkové vozidlo, odpružená kabina vozidla Zkouška náhodnými vibracemi, 10...2 000 Hz, efektivní vertikální zrychlení 21,3 m/s^2, efektivní podélné zrychlení 11,8 m/s^2, efektivní příčné zrychlení 13,1 m/s^2, 3 osy, 32 h na osu, včetně teplotního cyklu -20...70 °C. Tato zkouška odkazuje na IEC 60068-2-64: Zkoušení vlivů prostředí– Část 2-64: Zkoušky – Zkouška Fh: Širokopásmové náhodné vibrace a návod 3. Rázy: mechanický půlsinusový ráz o velikosti 3 g podle ISO 16750. Výše uvedené zkoušky se provádějí na různých vzorcích typu testovaného zařízení.	
4.4	Ochrana proti vodě a cizím tělesům	Zkouška podle ISO 20653: *Road vehicles – Degree of protection (IP code) – Protection of electrical equipment against foreign objects, water and access* (beze změny parametrů); minimální hodnota IP 40	220, 221
4.5	Ochrana proti přepětí	Ověřit, že celek ve vozidle vydrží tato napájecí napětí: verze pro napětí 24 V: 34 V při + 40 °C, 1 hod. verze pro napětí 12 V: 17 V při + 40 °C, 1 hod.(ISO 16750-2)	216
4.6	Ochrana proti záměně polarity	Ověřit, že celek ve vozidle vydrží přepólování napájecího napětí (ISO 16750-2)	216
4.7	Ochrana proti zkratu	Ověřit, že vstupní a výstupní signály jsou chráněny proti zkratu vůči napájení a uzemnění (ISO 16750-2)	216
5	**Zkoušky elektromagnetické kompatibility**		
5.1	Vyzařované emise a citlivost	Soulad s předpisem EHK č. 10	218
5.2	Elektrostatický výboj	Soulad s ISO 10605:2008 + technická oprava: 2010 + AMD1:2014: +/- 4 kV pro kontakt a +/- 8 kV pro výboj vzduchem	218

Č.	Zkouška	Popis	Související požadavky
5.3	Odolnost proti rušení vedenému napájecími vodiči	Verze pro napětí 24 V: soulad s ISO 7637-2 + předpisem EHK č. 10 rev. 3: impuls 1a: Vs = – 450 V, Ri = 50 Ω impuls 2a: Vs = + 37 V, Ri = 2 Ω impuls 2b: Vs = + 20 V, Ri = 0,05 Ω impuls 3a: Vs = – 150 V, Ri = 50 Ω impuls 3b: Vs = + 150 V, Ri = 50 Ω impuls 4: Vs = – 16 V, Va = -12 V, t6 = 100 ms impuls 5: Vs = + 120 V, Ri = 2,2 Ω, td = 250 ms Verze pro napětí 12 V: soulad s ISO 7637-1 + předpisem EHK č. 10 rev. 3: impuls 1: Vs = – 75 V, Ri = 10 Ω impuls 2a: Vs = + 37 V, Ri = 2 Ω impuls 2b: Vs = + 10 V, Ri = 0,05 Ω impuls 3a: Vs = – 112 V, Ri = 50 Ω impuls 3b: Vs = + 75 V, Ri = 50 Ω impuls 4: Vs = – 6 V, Va = – 5 V, t6 = 15 ms impuls 5: Vs = + 65 V, Ri = 3 Ω, td = 100 ms Impuls 5 se zkouší jen u celků ve vozidle určených k montáži ve vozidlech, která nejsou vybavena žádnou vnější společnou ochranou proti odpojení zátěže. Návrh týkající se odpojení zátěže viz ISO 16750-2, 4. vydání, kapitola 4.6.4.	218“

d) bod 6 se nahrazuje tímto:

„6 ZKOUŠKA VNĚJŠÍHO ZAŘÍZENÍ PRO DÁLKOVOU KOMUNIKACI

Č.	Zkouška	Popis	Související požadavky
1.	**Administrativní šetření**		
1.1	Dokumentace	Správnost dokumentace	
2.	**Vizuální kontrola**		
2.1	Shoda s dokumentací		
2.2	Identifikace/značení		225, 226
2.3	Materiály		219 až 223
3.	**Funkční zkoušky**		
3.1	Dálková komunikace pro cílené silniční kontroly		4, 197 až 199

Č.	Zkouška	Popis	Související požadavky
3.2	Zaznamenávání a ukládání údajů do datové paměti		91
3.3	Komunikace s celkem ve vozidle		Dodatek 14 odstavce DSC_66 až DSC_70, DSC_71 až DSC_76
4.	**Zkoušky vlivů prostředí**		
4.1	Teplota	Ověřit funkčnost podle těchto zkoušek: Zkouška podle ISO 16750-4, kapitoly 5.1.1.2: provozní zkouška při nízké teplotě (72 h při – 20 °C) Tato zkouška odkazuje na IEC 60068-2-1: Zkoušení vlivů prostředí– Část 2-1: Zkoušky– Zkouška A: Chlad Zkouška podle ISO 16750-4, kapitoly 5.1.2.2: provozní zkouška při vysoké teplotě (72 h při 70 °C) Tato zkouška odkazuje na IEC 60068-2-2: Zkoušení vlivů prostředí – Část 2-2: Zkoušky – Zkouška B: Suché teplo Zkouška podle ISO 16750-4, kapitoly 5.3.2: Rychlá změna teploty se stanovenou dobou přechodu (– 20 °C/70 °C, 20 cyklů, prodleva 1 h při každé teplotě) Při nižší teplotě, při vyšší teplotě a během teplotních cyklů lze provádět omezený soubor zkoušek (z těch, které jsou definovány v bodě 3 této tabulky).	213
4.2	Ochrana proti vodě a cizím tělesům	Zkouška podle ISO 20653: *Road vehicles – Degree of protection (IP code) – Protection of electrical equipment against foreign objects, water and access* (cílová hodnota IP40)	220, 221
5	**Zkoušky elektromagnetické kompatibility**		
5.1	Vyzařované emise a citlivost	Soulad s předpisem EHK č. 10	218
5.2	Elektrostatický výboj	Soulad s ISO 10605:2008 + technická oprava: 2010 + AMD1:2014: +/- 4 kV pro kontakt a +/- 8 kV pro výboj vzduchem	218

Č.	Zkouška	Popis	Související požadavky
5.3	Odolnost proti rušení vedenému napájecími vodiči	Verze pro napětí 24 V: soulad s ISO 7637-2 + předpisem EHK č. 10 rev. 3: impuls 1a: Vs = – 450 V, Ri = 50 Ω impuls 2a: Vs = + 37 V, Ri = 2 Ω impuls 2b: Vs = + 20 V, Ri = 0,05 Ω impuls 3a: Vs = – 150 V, Ri = 50 Ω impuls 3b: Vs = + 150 V, Ri = 50 Ω impuls 4: Vs = – 16 V, Va = – 12 V, t6 = 100 ms impuls 5: Vs = + 120 V, Ri = 2,2 Ω, td = 250 ms Verze pro napětí 12 V: soulad s ISO 7637-1 + předpisem EHK č. 10 rev. 3: impuls 1: Vs = – 75 V, Ri = 10 Ω impuls 2a: Vs = + 37 V, Ri = 2 Ω impuls 2b: Vs = + 10 V, Ri = 0,05 Ω impuls 3a: Vs = – 112 V, Ri = 50 Ω impuls 3b: Vs = + 75 V, Ri = 50 Ω impuls 4: Vs = – 6 V, Va = -5 V, t6 = 15 ms impuls 5: Vs = + 65 V, Ri = 3 Ω, td = 100 ms Impuls 5 se zkouší jen u celků ve vozidle určených k montáži ve vozidlech, která nejsou vybavena žádnou vnější společnou ochranou proti odpojení zátěže. Návrh týkající se odpojení zátěže viz ISO 16750-2, 4. vydání, kapitola 4.6.4.	218“

e) v bodě 8 o zkouškách interoperability se tabulka nahrazuje tímto:

„Č.	Zkouška	Popis
	8.1 Zkoušky interoperability celků ve vozidle a karet tachografu	
1	Vzájemné ověření pravosti	Ověřit, že vzájemné ověření pravosti mezi celkem ve vozidle a kartou tachografu probíhá normálně.
2	Zkoušky zápisu/čtení	Provést typický scénář činností s celkem ve vozidle. Scénář je přizpůsoben typu zkoušené karty a zahrnuje zápis do co největšího počtu elementárních souborů na kartě. Ověřit stažením z celku ve vozidle, že všechny příslušné záznamy byly řádně provedeny. Ověřit stažením z karty, že všechny příslušné záznamy byly řádně provedeny. Ověřit pomocí denních výtisků, že všechny příslušné záznamy lze řádně přečíst.

Č.	Zkouška	Popis
	8.2 Zkoušky interoperability celků ve vozidle a snímačů pohybu	
1	Párování	Ověřit, že párování mezi celky ve vozidle a snímači pohybu probíhá normálně.
2	Zkoušky činnosti	Provést typický scénář činností se snímačem pohybu. Scénář zahrnuje normální činnost a vytvoření co největšího počtu událostí nebo závad. Ověřit stažením z celku ve vozidle, že všechny příslušné záznamy byly řádně provedeny. Ověřit stažením z karty, že všechny příslušné záznamy byly řádně provedeny. Ověřit pomocí denního výtisku, že všechny příslušné záznamy lze řádně přečíst.
	8.3 Zkoušky interoperability celků ve vozidle a vnějších zařízení GNSS (v příslušných případech)	
1	Vzájemné ověření pravosti	Ověřit, že vzájemné ověření pravosti (vazba) mezi celkem ve vozidle a vnějším modulem GNSS probíhá normálně.
2	Zkoušky činnosti	Provést typický scénář činností s vnějším zařízením GNSS. Scénář zahrnuje normální činnost a vytvoření co největšího počtu událostí nebo závad. Ověřit stažením z celku ve vozidle, že všechny příslušné záznamy byly řádně provedeny. Ověřit stažením z karty, že všechny příslušné záznamy byly řádně provedeny. Ověřit pomocí denního výtisku, že všechny příslušné záznamy lze řádně přečíst.“

36) dodatek 11 se mění takto:

a) v bodě 8.2.3 se odstavec CSM_49 nahrazuje tímto:

„CSM_49 Celky ve vozidle, karty tachografu a vnější zařízení GNSS musí podporovat algoritmy SHA-256, SHA-384 a SHA-512 stanovené v [SHS].“;

b) v bodě 9.1.2 se první pododstavec v odstavci CSM_58 nahrazuje tímto:

„CSM_58 Kdykoli ERCA generuje nový evropský kořenový pár klíčů, vytvoří spojovací certifikát pro nový evropský veřejný klíč a podepíše jej předchozím evropským soukromým klíčem. Doba platnosti spojovacího certifikátu je 17 let plus 3 měsíce. To je také znázorněno na obrázku 1 v bodě 9.1.7.“;

c) v bodě 9.1.4 se odstavec CSM_72 nahrazuje tímto:

„CSM_72 Pro každý VU musí být generovány dva jedinečné páry klíčů ECC označené jako VU_MA a VU_Sign. Tento úkol zajišťují výrobci VU. Při každém generování páru klíčů VU zašle strana generující klíč svému MSCA veřejný klíč, aby mohla obdržet příslušný certifikát VU podepsaný MSCA. Soukromý klíč užívá pouze celek ve vozidle.“;

d) bod 9.1.5 se mění takto:

i) odstavec CSM_83 se nahrazuje tímto:

„CSM_83 Pro každou kartu tachografu musí být generován jedinečný pár klíčů ECC, označený jako Card_MA. Pro každou kartu řidiče a každou kartu dílny musí být navíc generován druhý jedinečný pár klíčů ECC, označený jako Card_Sign. Tento úkol mohou zajišťovat výrobci karet nebo personalizátoři karet. Při každém generování páru klíčů karty zašle strana generující klíč svému MSCA veřejný klíč, aby mohla obdržet příslušný certifikát karty podepsaný MSCA. Soukromý klíč užívá pouze karta tachografu.“;

ii) odstavec CSM_88 se nahrazuje tímto:

„CSM_88 Doba platnosti certifikátu Card_MA je následující:

— pro karty řidiče: 5 let

— pro karty podniku: 5 let

— pro kontrolní karty: 2 roky

— pro karty dílny: 1 rok“;

iii) v odstavci CSM_91 se doplňuje nová odrážka, která zní:

„— dále pouze pro kontrolní karty, karty podniku a karty dílny a pouze v případě, že takové karty byly vydány v prvních třech měsících doby platnosti nového certifikátu EUR: certifikát EUR, který je o dvě generace starší, pokud existuje.

Poznámka k poslední odrážce: Například v prvních třech měsících platnosti certifikátu ERCA(3) (viz obrázek 1) musí uvedené karty obsahovat certifikát ERCA(1). To je nutné k zajištění toho, aby tyto karty mohly být používány ke stahování dat z celků ve vozidle ERCA(1), jejichž běžná patnáctiletá životnost plus tříměsíční období pro stahování dat vyprší během těchto tří měsíců; viz příloha IC požadavek 13 poslední odrážka.“;

e) bod 9.1.6 se mění takto:

i) odstavec CSM_93 se nahrazuje tímto:

„CSM_93 Pro každé vnější zařízení GNSS musí být generován jedinečný pár klíčů ECC, označený jako EGF_MA. Tento úkol musí zajišťovat výrobci vnějšího zařízení GNSS. Při každém generování páru klíčů EGF_MA zašle strana generující klíč svému MSCA veřejný klíč, aby mohla obdržet příslušný certifikát EGF_MA podepsaný MSCA. Soukromý klíč užívá pouze vnější zařízení GNSS.“;

ii) odstavec CSM_95 se nahrazuje tímto:

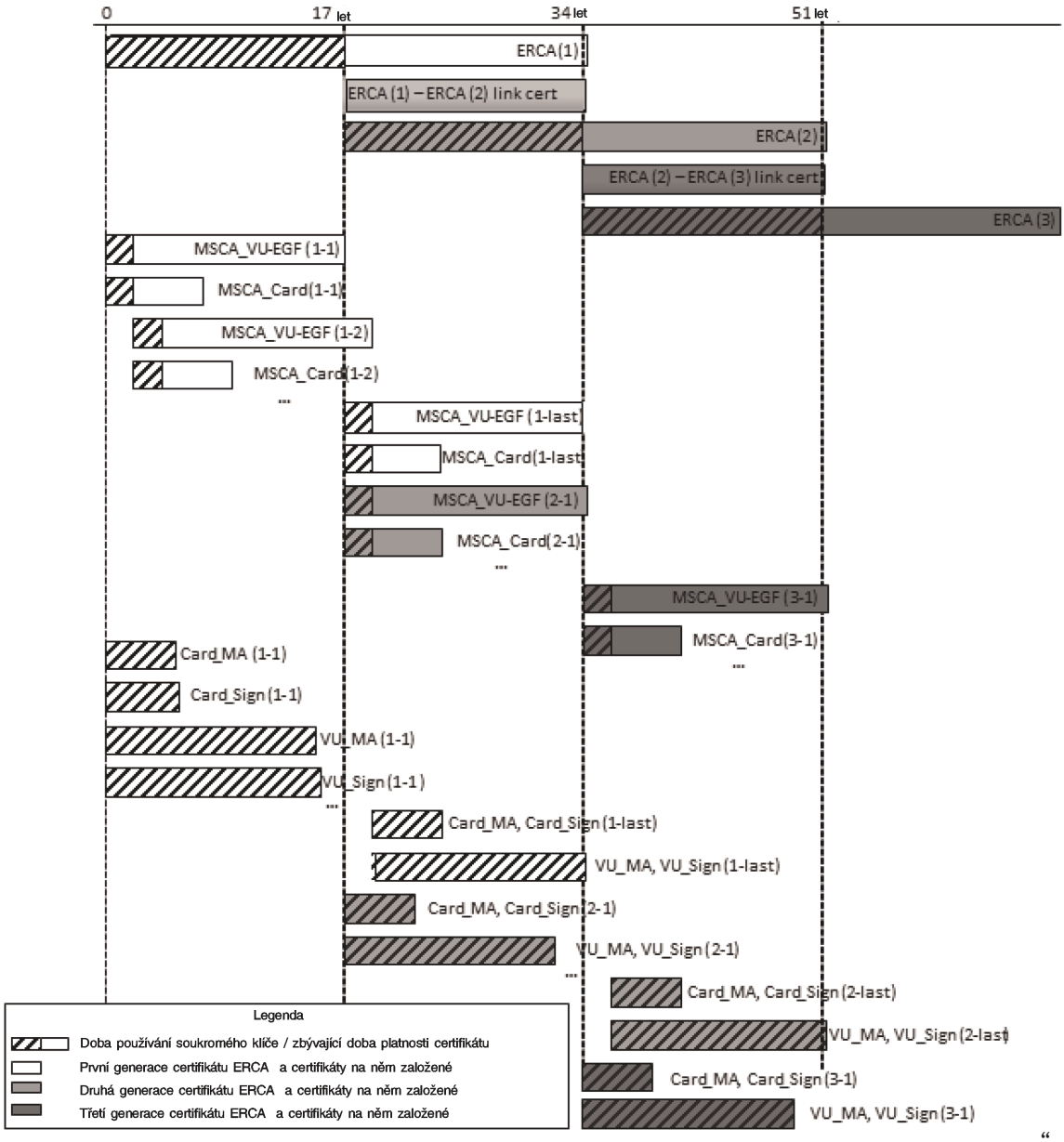
„CSM_95 Vnější zařízení GNSS musí užívat svůj pár klíčů EGF_MA obsahující soukromý klíč EGF_MA.SK a veřejný klíč EGF_MA.PK výhradně pro vzájemné ověřování pravosti a odsouhlasení klíče relace vůči celkům ve vozidle podle pokynů v bodě 11.4 tohoto dodatku.“;

f) bod 9.1.7 se mění takto:

i) obrázek 1 se nahrazuje tímto:

„Obrázek 1

Vydávání a používání různých generací kořenových certifikátů ERCA, spojovacích certifikátů ERCA, certifikátů MSCA a certifikátů zařízení



“

ii) v poznámkách k obrázku 1 se odstavec 6 nahrazuje tímto:

„6 Z důvodu úspory místa je rozdíl doby platnosti mezi certifikáty Card_MA a Card_Sign uveden pouze pro první generaci.“;

g) bod 9.2.1.1 se mění takto:

i) v odstavci CSM_106 se první odrážka nahrazuje tímto:

„— Pro 128-bitové hlavní klíče snímače pohybu: CV = ‘B6 44 2C 45 0E F8 D3 62 0B 7A 8A 97 91 E4 5D 83’“;

ii) v odstavci CSM_107 se první pododstavec nahrazuje tímto:

„Každý výrobce snímačů pohybu musí generovat náhodný a jedinečný párovací klíč K_P pro každý snímač pohybu a odeslat každý párovací klíč certifikačnímu orgánu svého členského státu. MSCA musí každý párovací klíč samostatně zašifrovat pomocí hlavního klíče snímače pohybu K_M a vrátit zašifrovaný klíč výrobci snímačů pohybu. Pro každý zašifrovaný klíč musí MSCA oznámit výrobci snímačů pohybu číslo verze příslušného K_M.“;

iii) odstavec CSM_108 se nahrazuje tímto:

„CSM_108 Každý výrobce snímačů pohybu musí generovat jedinečné sériové číslo pro každý snímač pohybu a odeslat všechna sériová čísla certifikačnímu orgánu svého členského státu. MSCA musí každé sériové číslo samostatně zašifrovat pomocí identifikačního klíče K_{ID} a vrátit zašifrované sériové číslo výrobci snímačů pohybu. Pro každé zašifrované sériové číslo musí MSCA oznámit výrobci snímačů pohybu číslo verze příslušného K_{ID}.“;

h) bod 9.2.2.1 se mění takto:

i) odstavec CSM_123 se nahrazuje tímto:

„CSM_123 Pro každý celek ve vozidle musí výrobce celku ve vozidle vytvořit jedinečné sériové číslo VU a na požádání je zaslat certifikačnímu orgánu svého členského státu, aby mohl získat sadu dvou klíčů DSRC vyhrazených příslušným VU. Sériové číslo VU musí mít datový typ `VuSerialNumber`.

Poznámka:

— Toto sériové číslo VU se musí shodovat s prvkem vuSerialNumber identifikace VuIdentification, viz dodatek 1, a s odkazem na držitele certifikátu v certifikátech VU.

— Sériové číslo VU nemusí být v okamžiku, kdy výrobce celku ve vozidle požádá o klíče DSRC vyhrazené příslušnému VU, známo. V takovém případě výrobce VU místo toho zašle jedinečný identifikátor žádosti o certifikát, který použil v žádosti o certifikáty VU; viz CSM_153. Tento identifikátor žádosti o certifikát je tudíž rovnocenný odkazu na držitele certifikátu v certifikátech VU.“;

ii) v odstavci CSM_124 se požadavek na informace v kroku 2 nahrazuje tímto:

„info = sériové číslo VU nebo identifikátor žádosti o certifikát, jež jsou uvedeny v odstavci CSM_123“;

iii) odstavec CSM_128 se nahrazuje tímto:

„CSM_128 MSCA musí vést záznamy o všech klíčích DSRC vyhrazených příslušným VU, které generoval, jejich číslech verze a sériových číslech VU nebo identifikátorech žádosti o certifikát, které byly použity při jejich odvozování.“;

i) v bodě 9.3.1 se první pododstavec v odstavci CSM_135 nahrazuje tímto:

„Pro kódování datových objektů v certifikátech musí být použita zvláštní kódovací pravidla (DER) podle [ISO 8825-1]. V tabulce 4 je uvedeno kompletní kódování certifikátů, včetně všech tagů a délek v bajtech.“;

j) v bodě 9.3.2.3 se odstavec CSM_141 nahrazuje tímto:

„CSM_141 Autorizace držitele certifikátu se používá k identifikaci typu certifikátu. Obsahuje šest nejdůležitějších bajtů ID aplikace tachografu kaskádově spojených s typem zařízení, čím je udán typ zařízení, pro něž je certifikát určen. V případě certifikátu VU, karty řidiče nebo karty dílny se typ zařízení používá také k rozlišení mezi certifikátem pro vzájemné ověření pravosti a certifikátem pro vytváření digitálních podpisů (viz bod 9.1 a dodatek 1, datový typ EquipmentType).“;

k) v bodě 9.3.2.5 se v odstavci CSM_146 doplňuje nový pododstavec, který zní:

„*Poznámka:* Pro certifikát karty musí být hodnota CHR rovna hodnotě cardExtendedSerialNumber v EF_ICC; viz dodatek 2. Pro certifikát EGF musí být hodnota CHR rovna hodnotě sensorGNSSSerialNumber v EF_ICC; viz dodatek 14. Pro certifikát VU musí být hodnota CHR rovna prvku vuSerialNumber identifikace VuIdentification, viz dodatek 1, pokud výrobce v okamžiku podání žádosti o certifikát nezná specifické sériové číslo výrobce.“;

l) v bodě 9.3.2.6 se odstavec CSM_148 nahrazuje tímto:

„CSM_148 Datum účinnosti certifikátu musí označovat počáteční datum a délku doby platnosti certifikátu.“;

m) bod 9.3.3 se mění takto:

i) v odstavci CSM_151 se první pododstavec nahrazuje tímto:

„Při podání žádosti o certifikát musí MSCA zaslat ERCA tyto údaje:“;

ii) odstavec CSM_153 se nahrazuje tímto:

„CSM_153 Výrobce zařízení musí zaslat MSCA v žádosti o certifikát tyto údaje, které MSCA umožní vytvořit odkaz na držitele nového certifikátu zařízení:

— případně (viz CSM_154) sériové číslo pro zařízení, které je pro výrobce jedinečné, typ zařízení a měsíc výroby. V ostatních případech jedinečný identifikátor žádosti o certifikát,

— měsíc a rok výroby zařízení nebo žádosti o certifikát.

Výrobce musí zajistit správnost těchto údajů a vložení certifikátu, který mu MSCA vrátí, do určeného zařízení.“;

n) bod 10.2.1 se mění takto:

i) v odstavci CSM_157 se znění před poznámkami k obrázku 4 nahrazuje tímto:

„Celky ve vozidle musí pro ověření řetězce certifikátů karty tachografu užívat protokol popsaný na obrázku 4. U každého certifikátu přečteného z karty VU ověří, zda jsou údaje v poli autorizace držitele certifikátu (CHA) správné:

— V poli CHA certifikátu karty musí být uveden certifikát karty pro vzájemné ověření pravosti (viz dodatek 1, datový typ EquipmentType).

— V poli CHA certifikátu Card.CA musí být uveden MSCA.

— V poli CHA certifikátu Card.Link musí být uveden ERCA.“;

ii) v odstavci CSM_159 se doplňuje nová věta, která zní:

„Zatímco uložení všech ostatních typů certifikátů není povinné, nový spojovací certifikát předložený kartou VU uložit musí.“;

o) bod 10.2.2 se mění takto:

i) v odstavci CSM_161 se znění před obrázkem 5 nahrazuje tímto:

„Karty tachografu musí pro ověření řetězce certifikátů VU používat protokol popsaný na obrázku 5. U každého certifikátu, který VU předloží, karta ověří, zda jsou údaje v poli autorizace držitele certifikátu (CHA) správné:

— V poli CHA certifikátu VU.Link musí být uveden ERCA.

— V poli CHA certifikátu VU.CA musí být uveden MSCA.

— V poli CHA certifikátu VU musí být uveden certifikát VU pro vzájemné ověření pravosti (viz dodatek 1, datový typ EquipmentType).“;

ii) odstavec CSM_165 se nahrazuje tímto:

„CSM_165 Je-li příkaz MSE: Set AT úspěšný, karta nastaví uvedený VU.PK pro následující použití během ověřování pravosti vozidla a přechodně uloží Comp(VU.PKeph). Jsou-li před odsouhlasením klíče relace zaslány dva nebo více úspěšných příkazů MSE: Set AT, karta uloží pouze poslední přijatý Comp(VU.PKeph). Karta resetuje Comp(VU.PKeph) po úspěšném provedení příkazu GENERAL AUTHENTICATE.“;

p) bod 10.3 se mění takto:

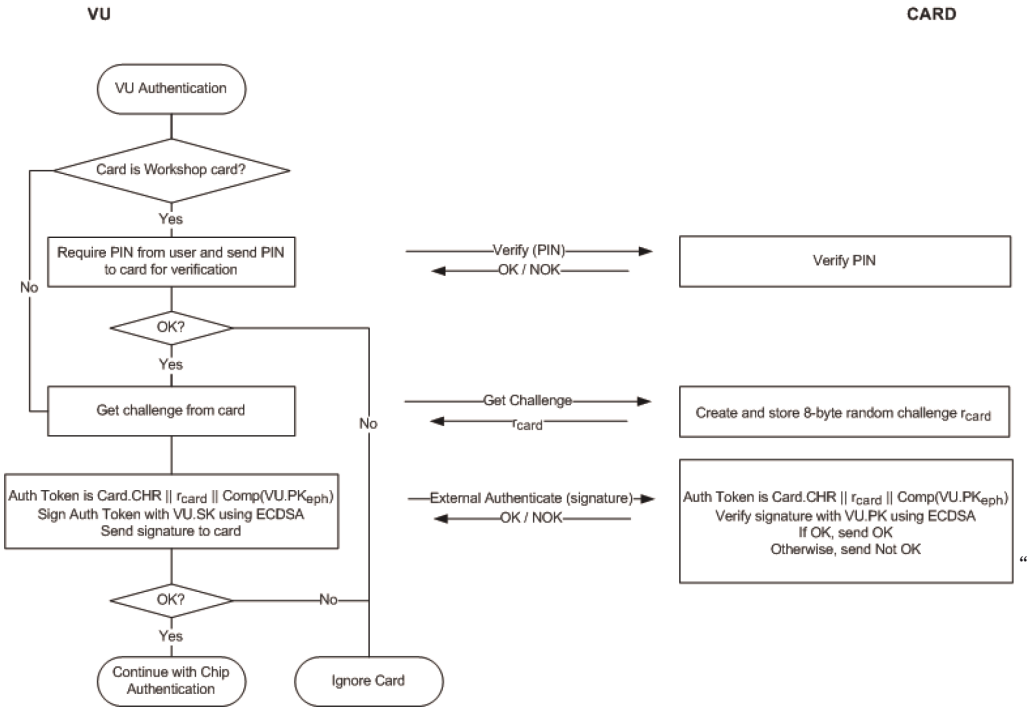
i) v odstavci CSM_170 se první pododstavec nahrazuje tímto:

„Kromě samotného podpisu výzvy karty musí VU do podpisu vložit odkaz na držitele certifikátu zjištěný z certifikátu karty.“;

ii) v odstavci CSM_171 se obrázek 6 nahrazuje tímto:

„*Obrázek 6*

Protokol ověřování pravosti VU



“

iii) odstavec CSM_174 se nahrazuje tímto:

„CSM_174 Po přijetí podpisu VU v příkazu EXTERNAL AUTHENTICATE musí karta

— vypočítat ověřovací token kaskádovým spojením Card.CHR, výzvu karty rcard a identifikátor přechodného veřejného klíče Comp(VU.PKeph) celku ve vozidle,

— ověřit podpis VU pomocí algoritmu ECDSA, pomocí hašovacího algoritmu spojeného s velikostí klíče páru klíčů VU_MA key celku ve vozidle podle CSM_50, ve spojení s VU.PK a vypočítaným ověřovacím tokenem.“;

q) v bodě 10.4 se odstavec CSM_176 mění takto:

i) druhý pododstavec se nahrazuje tímto:

„2. VU zašle kartě veřejný bod $VU.PK_{eph}$ svého přechodného páru klíčů. Tento veřejný bod musí být konvertován na oktetový řetězec podle [TR-03111]. Musí být použit nekomprimovaný kódovací formát. Jak je uvedeno v CSM_164, VU generoval tento přechodný pár klíčů před ověřením řetězce certifikátů VU. VU zaslal identifikátor přechodného veřejného klíče $Comp(VU.PK_{eph})$ kartě, která jej uložila.“;

ii) druhý pododstavec se nahrazuje tímto:

„6. Pomocí K_{MAC} karta vypočítá ověřovací token pro přechodný veřejný bod VU: $T_{PICC} = CMAC(K_{MAC}, VU.PK_{eph})$. Veřejný bod musí být ve formátu použitém v celku ve vozidle (viz druhý pododstavec výše). Karta zašle N_{PICC} a T_{PICC} celku ve vozidle.“;

r) v bodě 10.5.2 se odstavec CSM_191 nahrazuje tímto:

„CSM_191 Všechny datové objekty určené k šifrování musí být podle [ISO 7816-4] doplněny indikátorem doplňkového obsahu ‘01’. Pro výpočet MAC se datové objekty v APDU doplní podle [ISO 7816-4].

Poznámka: Doplňování pro bezpečné předávání zpráv se vždy provádí pomocí vrstvy bezpečného předávání zpráv, nikoli pomocí algoritmů CMAC nebo CBC.

Shrnutí a příklady

Příkaz APDU s použitým bezpečným předáváním zpráv má v závislosti na příslušném nezabezpečeném příkazu následující strukturu (DO je datový objekt):

Případ 1: CLA INS P1 P2 || Lc’ || DO „8E“ || Le

Případ 2: CLA INS P1 P2 || Lc’ || DO „97“ || DO„8E“ || Le

Případ 3 (sudý bajt INS): CLA INS P1 P2 || Lc’ || DO „81“ || DO„8E“ || Le

Případ 3 (lichý bajt INS): CLA INS P1 P2 || Lc’ || DO „B3“ || DO„8E“ || Le

Případ 4 (sudý bajt INS): CLA INS P1 P2 || Lc’ || DO „81“ || DO„97“ || DO„8E“ || Le

Případ 4 (lichý bajt INS): CLA INS P1 P2 || Lc’ || DO „B3“ || DO„97“ || DO„8E“ || Le

kde Le = ‘00’ nebo ‘00 00’ v závislosti na tom, zda jsou použita krátká pole délky nebo rozšířená pole délky; viz [ISO 7816-4].

Odpověď APDU s použitým bezpečným předáváním zpráv má v závislosti na příslušné nezabezpečené odpovědi následující strukturu:

Případ 1 nebo 3: DO „99“ || DO „8E“ || SW1SW2

Případ 2 nebo 4 (sudý bajt INS) bez šifrování: DO „81“ || DO „99“ || DO „8E“ || SW1SW2

Případ 2 nebo 4 (sudý bajt INS) se šifrováním: DO „87“ || DO „99“ || DO „8E“ || SW1SW2

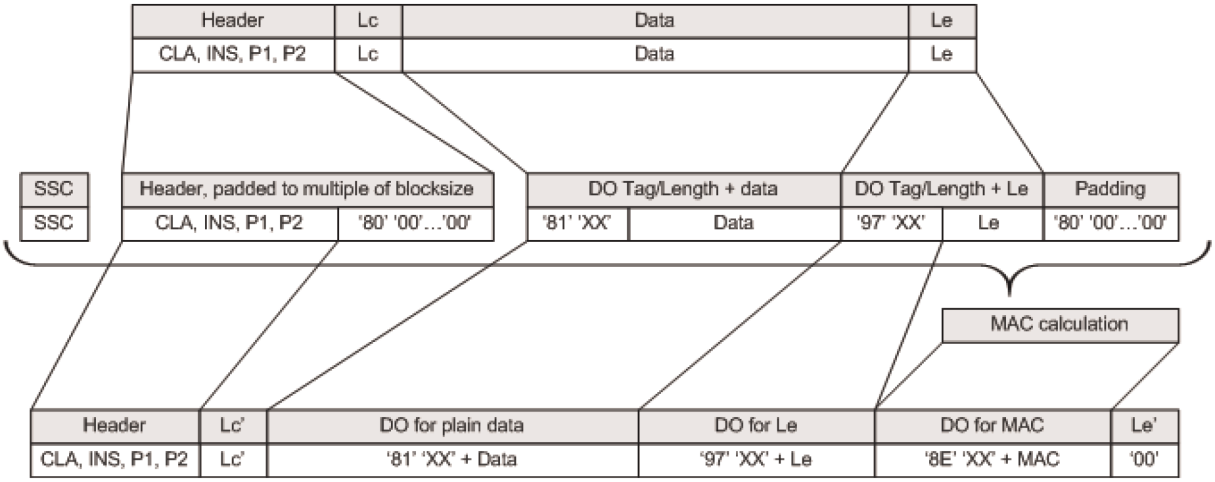
Případ 2 nebo 4 (lichý bajt INS) bez šifrování: DO „B3“ || DO „99“ || DO „8E“ || SW1SW2

Poznámka: Případ 2 nebo 4 (lichý bajt INS) se šifrováním se v komunikaci mezi VU a kartou nikdy nepoužívá.

Níže jsou uvedeny tři příklady transformace APDU pro příkazy se sudým kódem INS. Obrázek 8 znázorňuje případ 4 příkazu APDU s ověřenou pravostí, obrázek 9 znázorňuje případ 1 / případ 3 odpovědi APDU s ověřenou pravostí a obrázek 10 znázorňuje případ 2 / případ 4 odpovědi APDU se šifrováním a ověřenou pravostí.

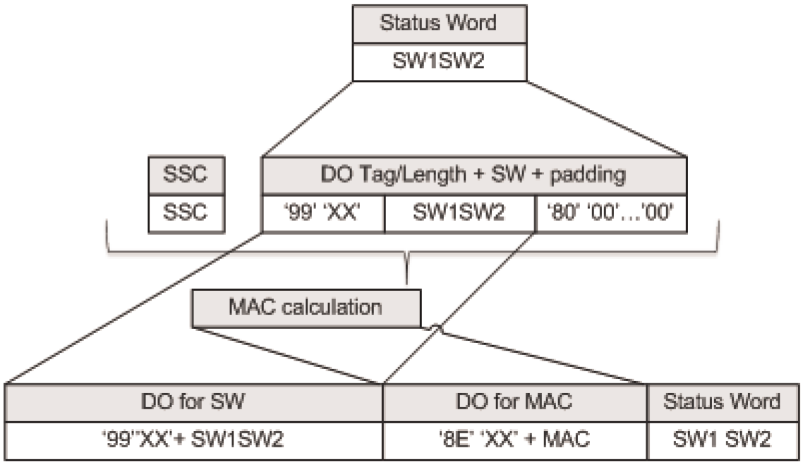
Obrázek 8

Transformace případu 4 příkazu APDU s ověřenou pravostí



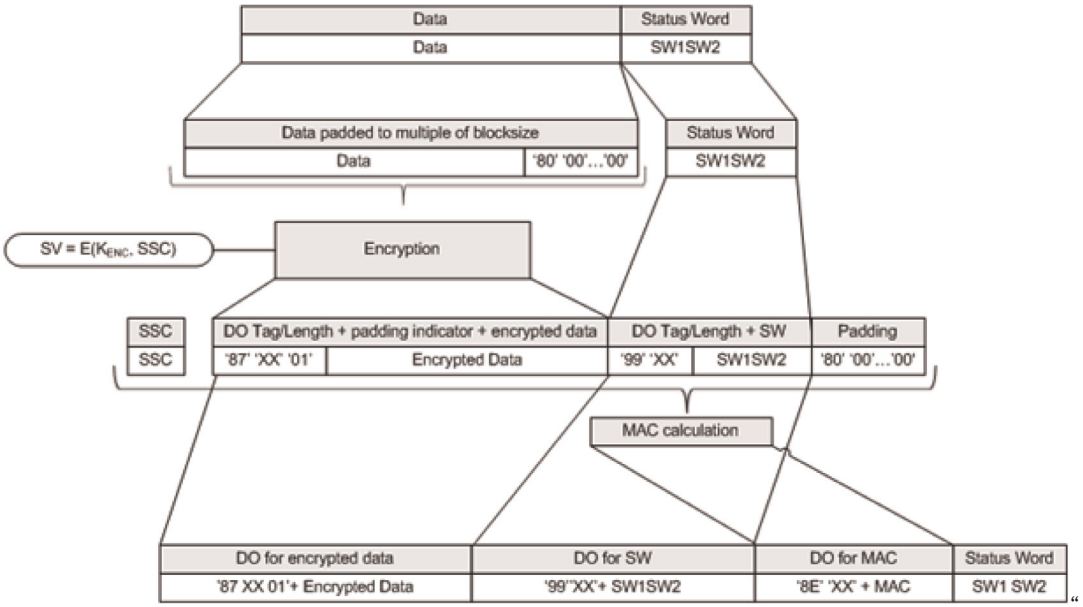
Obrázek 9

Transformace případu 1 / případu 3 odpovědi APDU s ověřenou pravostí



Obrázek 10

Transformace případu 2 / případu 4 odpovědi APDU se šifrováním a ověřenou pravostí



“

s) v bodě 10.5.3 se odstavec CSM_193 nahrazuje tímto:

„CSM_193 Karta tachografu přeruší aktuální relaci bezpečného předávání zpráv pouze v případě, že je splněna některá z těchto podmínek:

— přijme otevřený příkaz APDU,

— detekuje chybu bezpečného předávání zpráv v příkazu APDU:

— chybí očekávaný datový objekt bezpečného předávání zpráv, pořadí datových objektů je nesprávné nebo je zařazen neznámý datový objekt,

— datový objekt bezpečného předávání zpráv je nesprávný, např. hodnota MAC nebo struktura TLV je nesprávná,

— je odpojena od napájení nebo resetována,

— VU zahájí proces ověření pravosti VU,

— je dosaženo mezního počtu příkazů a příslušných odpovědí v rámci aktuální relace. Pro příslušnou kartu tuto mezní hodnotu stanoví její výrobce s ohledem na bezpečnostní požadavky použitého hardwaru s maximální hodnotou 240 příkazů a příslušných odezev SM na relaci.“;

t) bod 11.3.2 se mění takto:

i) v odstavci CSM_208 se první pododstavec nahrazuje tímto:

„Během párování s VU musí vnější zařízení GNSS používat protokol uvedený na obrázku 5 (bod 10.2.2) pro ověření řetězců certifikátů VU.“;

ii) odstavec CSM_210 se nahrazuje tímto:

„CSM_210 Jakmile vnější zařízení GNSS ověří certifikát VU_MA, musí jej uložit pro použití během normálního provozu; viz bod 11.3.3.“;

u) v bodě 11.3.3 se první pododstavec v odstavci CSM_211 nahrazuje tímto:

„Během normálního provozu musí celek ve vozidle a EGF používat protokol uvedený na obrázku 11 pro ověření dočasné platnosti uloženého certifikátu EGF_MA a pro nastavení veřejného klíče VU_MA pro následné ověření pravosti VU. Během normálního provozu se žádné další vzájemné ověření řetězců certifikátů neprovádí.“;

v) v bodě 12.3 se tabulka 6 nahrazuje tímto:

„Tabulka 6

Počet bajtů otevřeného textu a šifrovaných dat na instrukci podle [ISO 16844-3]

Instrukce	Požadavek/ odpověď	Popis dat	Počet bajtů otevřených dat podle [ISO 16844-3]	Počet bajtů otevřených dat s použitím klíčů AES	Počet bajtů otevřených dat s použitím klíčů AES s bitovou délkou		
					128	192	256
10	požadavek	Data ověření pravosti + číslo souboru	8	8	16	16	16
11	odpověď	Data ověření pravosti + obsah souboru	16 nebo 32, podle souboru	16 nebo 32, podle souboru	32 / 48	32 / 48	32 / 48
41	požadavek	Sériové číslo MoS	8	8	16	16	16
41	odpověď	Párovací klíč	16	16 / 24 / 32	16	32	32
42	požadavek	Klíč relace	16	16 / 24 / 32	16	32	32
43	požadavek	Párovací informace	24	24	32	32	32
50	odpověď	Párovací informace	24	24	32	32	32
70	požadavek	Data ověření pravosti	8	8	16	16	16
80	odpověď	Hodnota čítače MoS + data ověření pravosti	8	8	16	16	16“

w) v bodě 13.1 se požadavek týkající se sériového čísla VU v odstavci CSM_224 nahrazuje tímto:

„**Sériové číslo VU** sériové číslo VU nebo identifikátor žádosti o certifikát (datový typ VuSerialNumber nebo CertificateRequestID) – viz CSM_123“;

x) v bodě 13.3 se druhá odrážka v odstavci CSM_228 nahrazuje tímto:

„2. Kontrolní karta použije uvedený hlavní klíč DSRC ve spojení se sériovým číslem VU nebo identifikátorem žádosti o certifikát v bezpečnostních datech DSRC pro odvození klíčů DSRC příslušného celku ve vozidle K_VU_{DSRC}_ENC a K_VU_{DSRC}_MAC, jak je uvedeno v CSM_124.“;

y) bod 14.3 se mění takto:

i) v odstavci CSM_234 se znění před poznámkami k obrázku 13 nahrazuje tímto:

„IDE může ověřovat podpis stahovaných dat samostatně nebo může k tomuto účelu použít kontrolní kartu. V případě, že použije kontrolní kartu, provede se ověření podpisu podle Figure 13. Pro ověření dočasné platnosti certifikátu předloženého IDE kontrolní karta použije svůj interní aktuální čas, jak je uvedeno v odstavci CSM_167. Kontrolní karta svůj aktuální čas aktualizuje, je-li datum účinnosti certifikátu s původním platným zdrojem času pozdější než aktuální čas karty. Karta jako platný zdroj času přijme pouze tyto certifikáty:

— spojovací certifikáty ERCA druhé generace,

— certifikáty MSCA druhé generace,

— certifikáty VU_Sign nebo Card_Sign druhé generace vydané stejnou zemí jako vlastní certifikát kontrolní karty.

V případě, že ověří podpis samostatně, prokázání pravosti a platnost všech certifikátů v řetězci certifikátů datového souboru a podpis dat podle podpisového schématu uvedeného v [DSS]. V obou případech je u každého certifikátu přečteného z datového souboru potřeba ověřit, zda je pole autorizace držitele certifikátu (CHA) správné:

— V poli CHA certifikátu EQT musí být uveden certifikát VU, případně karty pro připojení podpisu (viz dodatek 1, datový typ EquipmentType).

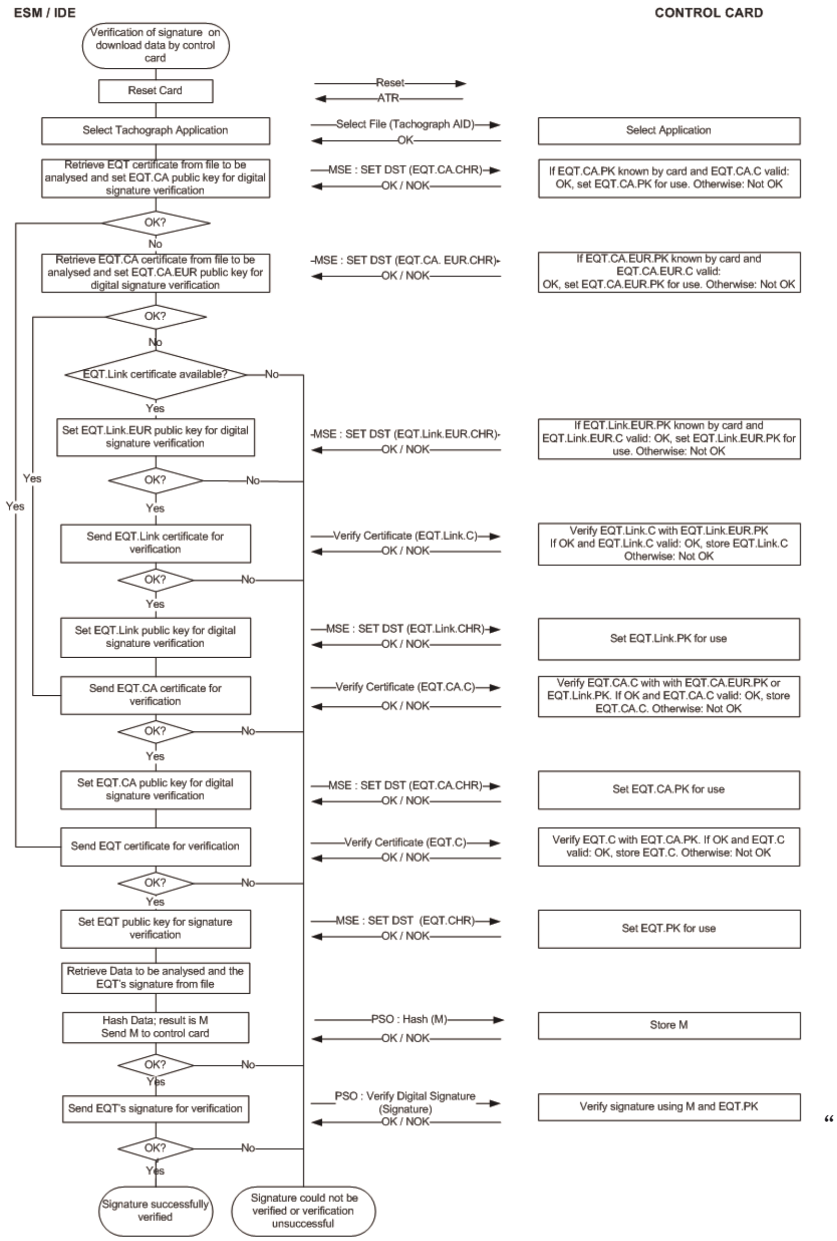
— V poli CHA certifikátu EQT.CA musí být uveden MSCA.

— V poli CHA certifikátu EQT.Link musí být uveden ERCA.“;

ii) obrázek 13 se nahrazuje tímto:

„*Obrázek 13*

Protokol pro ověření podpisu staženého datového souboru



“

37) dodatek 12 se mění takto:

a) bod 3 se mění takto:

i) v odstavci GNS_4 se druhý pododstavec za obrázkem 2 nahrazuje tímto:

„Rozlišení polohy je založeno na výše popsaném formátu věty RMC. První část polí č. 3 a 5 představuje stupně. Zbytek představuje minuty vyjádřené na tři desetinná místa. Rozlišení je tedy 1/1000 minuty nebo 1/60000 stupně (protože jedna minuta je 1/60 stupně).“;

ii) odstavec GNS_5 se nahrazuje tímto:

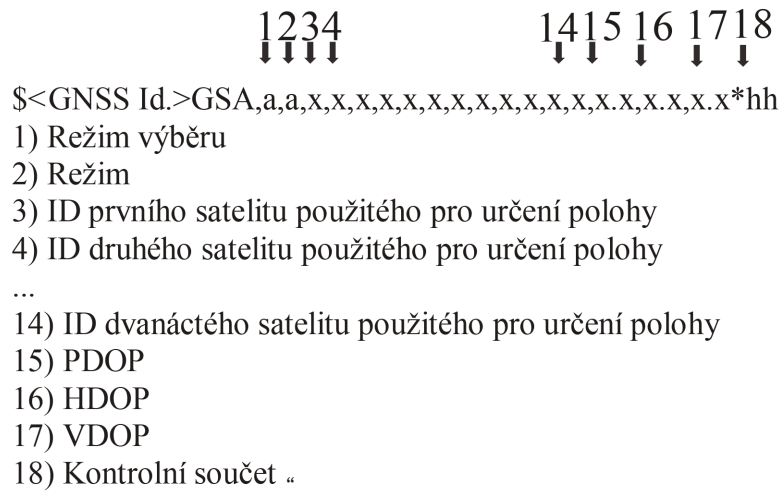
„GNS_5 Celek ve vozidle ukládá v databázi VU informace o poloze, pokud jde o zeměpisnou šířku a délku, s rozlišením 1/10 minuty nebo 1/600 stupně, jak popisuje dodatek 1 pro typ GeoCoordinates.

Ke zjišťování a zaznamenávání dostupnosti a přesnosti signálu může celek ve vozidle používat příkaz GSA (GPS DOP a aktivní družice). K indikaci úrovně přesnosti zaznamenaných údajů o poloze se používá zejména parametr HDOP (viz část 4.2.2). Celek ve vozidle ukládá hodnotu parametru horizontální přesnosti (HDOP) vypočítanou jako minimum z hodnot HDOP shromážděných z dostupných systémů GNSS.

ID systému GNSS označuje příslušné ID NMEA pro každou konstelaci GNSS a systém s družicovým rozšířením (SBAS).

Obrázek 3

Struktura věty GSA



iii) odstavec GNS_6 se nahrazuje tímto:

„GNS_6 Věta GSA se ukládá s číslem záznamu ‘02’ až ‘06’ “;

b) bod 4.2.1 se mění takto:

i) odstavec GNS_16 se nahrazuje tímto:

„GNS_16 V komunikačním protokolu nejsou podporována rozšířená pole délky.“;

ii) odstavec GNS_18 se nahrazuje tímto:

„GNS_18 Pokud jde o funkce 1) shromažďování a distribuce údajů GNSS, 2) shromažďování konfiguračních dat vnějšího zařízení GNSS a 3) protokol správy, bezpečnostní přijímač-vysílač GNSS simuluje inteligentní kartu s architekturou systému souborů tvořenou hlavním souborem (MF), vyhrazeným souborem (DF) s identifikátorem aplikace stanoveným v dodatku 1 kapitole 6.2 ('FF 44 54 45 47 4D') a s třemi elementárními soubory (EF) obsahujícími certifikáty a jedním samostatným elementárním souborem (EF.EGF) s identifikátorem souboru rovným '2F2F', jak popisuje tabulka 1."

iii) odstavec GNS_20 se nahrazuje tímto:

„GNS_20 Bezpečnostní přijímač-vysílač GNSS používá pro ukládání dat paměť a musí být schopen provést nejméně 20 milionů cyklů zápisu/čtení. Kromě této podmínky jsou vnitřní konstrukce a implementace bezpečnostního přijímače-vysílače GNSS ponechány na uvážení výrobců.

Mapování čísel záznamů a dat je uvedeno v tabulce 1. Je třeba mít na paměti, že existuje pět vět GSA pro konstelace GNSS a systém s družicovým rozšířením (SBAS).";

c) v bodě 4.2.2 se pátý pododstavec v odstavci GNS_23 nahrazuje tímto:

„5. Procesor VU zkontroluje přijaté údaje a extrahuje informace (např. zeměpisnou šířku, délku, čas) z věty RMC NMEA. Věta RMC NMEA obsahuje informaci, zda je poloha platná. Není-li poloha platná, nejsou údaje o poloze dosud k dispozici a nelze je použít pro zaznamenání polohy vozidla. Je-li poloha platná, procesor VU rovněž extrahuje hodnoty HDOP z vět GSA NMEA a vypočítá minimální hodnotu z dostupných družicových systémů (tj. je-li poloha k dispozici).";

d) v bodě 4.4.1 se odstavec GNS_28 nahrazuje tímto:

„GNS_28 Pokud celek ve vozidle není schopen komunikovat s vnějším zařízením GNSS s vytvořenou vazbou nepřetržitě po dobu delší než 20 minut, VU generuje a zaznamená událost typu EventFaultType s hodnotou enum '0E'H Communication error with the external GNSS facility (chyba komunikace s vnějším zařízením GNSS) a s časovým razítkem s aktuálním časem. Událost se generuje, pouze pokud jsou splněny tyto dvě podmínky: a) inteligentní tachograf není v kalibračním režimu a b) vozidlo se pohybuje. V této souvislosti se chyba komunikace vyvolá, když bezpečnostní přijímač-vysílač VU neobdrží zprávu s odpovědí po zprávě s požadavkem, jak je popsáno v bodě 4.2.";

e) v bodě 4.4.2 se odstavec GNS_29 nahrazuje tímto:

„GNS_29 Při narušení vnějšího zařízení GNSS bezpečnostní přijímač-vysílač GNSS vymaže veškerý obsah své paměti, včetně kryptografického materiálu. Jak je popsáno v odstavcích GNS_25 a GNS_26, VU detekuje nedovolenou manipulaci, je-li status odpovědi '6690'. Celek ve vozidle poté generuje událost typu EventFaultType enum '19'H Tamper detection of GNSS (detekce nedovolené manipulace s GNSS). Případně může vnější zařízení GNSS přestat reagovat na externí požadavky."

f) v bodě 4.4.3 se odstavec GNS_30 nahrazuje tímto:

„GNS_30 Pokud bezpečnostní přijímač-vysílač GNSS neobdrží data z přijímače GNSS nepřetržitě po dobu delší než 3 hodiny, bezpečnostní přijímač-vysílač GNSS generuje zprávu s odpovědí na příkaz READ RECORD s číslem RECORD rovným '01' a s datovým polem obsahujícím 12 bajtů, které mají všechny hodnotu 0xFF. Po přijetí zprávy s odpovědí s touto hodnotou datového pole VU generuje a zaznamená událost typu EventFaultType enum '0D'H Absence of position information from GNSS receiver (chybí informace o poloze z přijímače GNSS) s časovým razítkem s aktuálním časem, avšak pouze v případě, že jsou splněny tyto dvě podmínky: a) inteligentní tachograf není v kalibračním režimu a b) vozidlo se pohybuje.";

g) v bodě 4.4.4 se znění v odstavci GNS_31 až po obrázek 4 nahrazuje tímto:

„Pokud celek ve vozidle zjistí, že certifikát EGF používaný pro vzájemné ověření pravosti již není platný, VU generuje a zaznamená událost záznamového zařízení typu EventFaultType enum *'1B'H External GNSS facility certificate expired* (skončila platnost certifikátu vnějšího zařízení GNSS) s časovým razítkem s aktuálním časem. VU nadále používá přijaté údaje GNSS o poloze.";

h) v bodě 5.2.1 se odstavec GNS_34 nahrazuje tímto:

„GNS_34 Pokud celek ve vozidle neobdrží data z přijímače GNSS nepřetržitě po dobu delší než 3 hodiny, VU generuje a zaznamená událost typu EventFaultType enum '0D'H Absence of position information from GNSS receiver (chybí informace o poloze z přijímače GNSS) s časovým razítkem s aktuálním časem, avšak pouze v případě, že jsou splněny tyto dvě podmínky: a) inteligentní tachograf není v kalibračním režimu a b) vozidlo se pohybuje.";

i) bod 6 se nahrazuje tímto:

„6. NESOULAD ČASU GNSS

Pokud celek ve vozidle zjistí rozdíl větší než 1 minuta mezi časem podle funkce pro měření času v celku ve vozidle a časem pocházejícím z přijímače GNSS, VU zaznamená událost typu EventFaultType enum *'0B'H Time conflict (GNSS versus VU internal clock)* (nesoulad času – GNSS vůči vnitřním hodinám VU). Po vyvolání události nesouladu času VU nekontroluje časový nesoulad po dobu následujících 12 hodin. Tato událost není vyvolána v případech, kdy přijímač GNSS během posledních 30 dnů nezjistil žádný platný signál GNSS.";

38) dodatek 13 se mění takto:

a) v bodě 2 se čtvrtý pododstavec nahrazuje tímto:

„Pro upřesnění tento dodatek nespecifikuje:

— činnost a správu, pokud jde o shromažďování *údajů* v celku ve vozidle (které jsou specifikovány jinde v *nařízení* nebo jsou jinak funkcí konstrukce výrobku),

— formu prezentace shromážděných údajů aplikaci ve vnějším zařízení,

— ustanovení o zabezpečení dat nad rámec toho, co poskytuje Bluetooth® (např. šifrování), pokud jde o obsah *údajů* (což je specifikováno jinde v *nařízení* [Dodatek 11 Společné bezpečnostní mechanismy]),

— protokoly Bluetooth® používané rozhraním ITS.";

b) v bodě 4.2 se třetí pododstavec nahrazuje tímto:

„Dostane-li se vnější zařízení poprvé do dosahu VU, lze iniciovat proces párování Bluetooth® (viz rovněž přílohu 2). Zařízení sdílejí své adresy, názvy, profily a společný tajný klíč, což jim umožní navázat spojení, kdykoli se v budoucnu k sobě přiblíží. Po dokončení tohoto kroku je vnější zařízení považováno za důvěryhodné a může iniciovat požadavky na stažení dat z tachografu. Nepočítá se s přidáním šifrovacích mechanismů nad rámec toho, co poskytuje Bluetooth®. Jsou-li však nezbytné dodatečné bezpečnostní mechanismy, lze tak učinit v souladu s dodatkem 11 Společné bezpečnostní mechanismy.";

c) bod 4.3 se mění takto:

i) první pododstavec se nahrazuje tímto:

„Z bezpečnostních důvodů VU vyžaduje systém ověření pomocí kódu PIN odděleně od párování Bluetooth. Pro účely ověření pravosti je každý VU schopen generovat kódy PIN tvořené nejméně 4 číslicemi. Vnější zařízení musí při každém párování s VU poskytnout správný kód PIN, než bude moci přijímat data.";

ii) třetí pododstavec za tabulkou 1 se nahrazuje tímto:

„Výrobce může nabízet možnost změny kódu PIN přímo prostřednictvím celku ve vozidle, avšak kód PUC nelze měnit. Změna kódu PIN, pokud je možná, vyžaduje zadání aktuálního kódu PIN přímo do VU.“;

d) v bodě 4.4 se druhý pododstavec za nadpisem „Datové pole“ nahrazuje tímto:

„Jsou-li data, která je třeba zpracovat, delší než dostupný prostor v jedné zprávě, rozdělí se do několika dílčích zpráv. Každá dílčí zpráva má stejnou hlavičku a SID, ale obsahuje dvoubajtový čítač, *Counter Current* (CC) a *Counter Max* (CM), který uvádí číslo dílčí zprávy. Aby byla možná kontrola chyb a přerušení přenosu, přijímající zařízení potvrzuje každou dílčí zprávu. Přijímající zařízení může přijmout dílčí zprávu, požádat o to, aby byla znovu přenesena, nebo požádat vysílající zařízení o opětovný start nebo o přerušení přenosu.“;

e) Příloha 1 se mění takto:

i) nadpis se nahrazuje tímto:

„1) SEZNAM ÚDAJŮ DOSTUPNÝCH PROSTŘEDNICTVÍM ROZHRANÍ ITS“;

ii) v tabulce v bodě 3 se za položku „Chybí informace o poloze z přijímače GNSS“ vkládá nová položka, která zní:

„Chyba komunikace s vnějším zařízením GNSS	— nejdelší událost v každém z posledních 10 dnů výskytu — 5 nejdelších událostí za posledních 365 dnů	— datum a čas začátku události, — datum a čas konce události — typ, číslo, vydávající členský stát a generace všech karet vložených na začátku a/nebo na konci události — počet podobných událostí v tentýž den“

iii) v bodě 5 se doplňuje nová odrážka, která zní:

„— závada rozhraní ITS (v příslušných případech)“;

f) v příloze 3 se specifikace v notaci ASN.1 mění takto:

i) za řádek 206 se vkládají nové řádky 206a až 206e, které znějí:

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

ii) řádky 262 až 264 se nahrazují tímto:

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

iii) řádek 275 se nahrazuje tímto:

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

iv) řádky 288 až 310 se nahrazují tímto:

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

v) řádky 362 a 363 se nahrazují tímto:

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

vi) za řádek 410 se vkládají nové řádky 410a a 410b, které znějí:

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

vii) za řádek 539 se vkládají nové řádky 539a až 539j, které znějí:

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

39) dodatek 14 se mění takto:

a) v obsahu se bod 5.5 nahrazuje tímto:

„5.5 Podpora pro směrnici (EU) 2015/719 ..... 490“;

b) v bodě 2 se třetí pododstavec nahrazuje tímto:

„V tomto scénáři je čas vyhrazený pro komunikaci omezený, protože *komunikace* je cílená a má krátký dosah. Stejné komunikační prostředky pro dálkové sledování tachografů (RTM) mohou navíc příslušné kontrolní orgány používat pro další aplikace (např. maximální hmotnosti a rozměry těžkých nákladních vozidel podle směrnice (EU) 2015/719) a tyto operace mohou být podle rozhodnutí příslušných kontrolních orgánů izolované nebo sekvenční.“;

c) bod 5.1 se mění takto:

i) v odstavci DSC_19 se dvanáctá odrážka nahrazuje tímto:

„— Anténa DSRC-VU musí být umístěna v místě, ve kterém umožňuje optimální komunikaci DSRC mezi vozidlem a přijímací silniční anténou, když je přijímač umístěn 15 metrů před vozidlem a ve výšce 2 metry a zaměřen na vodorovný a svislý střed čelního skla. U lehkých vozidel se umístí v horní části čelního skla. U všech ostatních vozidel se anténa DSRC umístí buď poblíž spodní nebo poblíž horní části čelního skla.“;

ii) v odstavci DSC_22 se první pododstavec nahrazuje tímto:

„Tvarový činitel antény není stanoven a je komerčním rozhodnutím, pokud namontované zařízení DSRC-VU splňuje požadavky na shodu podle části 5 níže. Anténa musí být umístěna v souladu s pokyny v DSC_19 a účinně podporovat případy použití popsané v bodech 4.1.2 a 4.1.3.“;

d) v bodě 5.4.3 se sekvence 7 nahrazuje tímto:

„7	REDCR	>	DSRC-VU	Posílá příkaz GET.request na údaje v jiném atributu (v případě potřeby).“

e) v bodě 5.4.4 se definice modulu ASN.1 v odstavci DCS_40 mění takto:

(i) první řádek sekvence pro `TachographPayload` se nahrazuje tímto:

„`tp15638VehicleRegistrationPlate LPN – Vehicle Registration Plate as per EN 15509`[1]“;

ii) doplňuje se nová poznámka pod čarou 1, která zní:

„1. Jestliže LPN obsahuje AlphabetIndicator LatinAlphabetNo2 nebo latinCyrillicAlphabet, speciální znaky se přemapují v silniční dotazovací jednotce za použití zvláštních pravidel podle přílohy E normy ISO/DIS 14 906,2“;

iii) horní index 2 v řádku, v němž je definováno časové razítko aktuálního záznamu, se zrušuje;

iv) definice modulu ASN.1 pro `RtmTransferAck` se nahrazuje tímto:

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

f) v bodě 5.4.5 se položka RTM12 v tabulce 14.3 nahrazuje tímto:

„**RTM12** **Porucha snímače**	VU vygeneruje celočíselnou hodnotu pro datový prvek RTM12. VU přiřadí proměnné sensorFault hodnotu: — 1, jestliže během posledních 10 dní zaznamenal událost typu '35H' Porucha snímače, — 2, jestliže během posledních 10 dní zaznamenal událost typu Porucha přijímače GNSS (interního nebo externího s hodnotami enum '36'H nebo '37'H), — 3, jestliže během posledních 10 dní zaznamenal událost typu '0E'H Chyba komunikace s vnějším zařízením GNSS, — 4, jestliže během posledních 10 dní zaznamenal poruchu snímače i poruchu přijímače GNSS, — 5, jestliže během posledních 10 dní zaznamenal poruchu snímače i událost Chyba komunikace s vnějším zařízením GNSS, — 6, jestliže během posledních 10 dní zaznamenal poruchu přijímače GNSS i událost Chyba komunikace s vnějším zařízením GNSS, — 7, jestliže během posledních 10 dní zaznamenal všechny tři poruchy snímače, JINAK přiřadí hodnotu 0, jestliže během posledních 10 dní nebyly zaznamenány žádné události.	– Porucha snímače – jeden oktet podle slovníku údajů	`sensorFault INTEGER (0..255),;` “

g) v bodě 5.4.6 se odstavec DSC_43 nahrazuje tímto:

„DSC_43 Pro všechny výměny DSRC jsou data šifrována pomocí PER (Packed Encoding Rules) UNALIGNED, kromě `TachographPayload` a `OwsPayload`;, které se šifrují pomocí OER (Octet Encoding Rules), definovaných v normě ISO/IEC 8825-7, Rec. ITU-T X.696.“;

h) v bodě 5.4.7 se ve čtvrtém sloupci tabulky 14.9 znění v buňce popisující `Rtm-ContextMark`; nahrazuje tímto:

„Identifikátor objektu podporované normy, části a verze. Příklad: ISO (1) norma (0) TARV (15638) část9 (9) verze 1 (1).

První oktet je 06H, což je identifikátor objektu. Druhý oktet je 06H, což je délka. Následujících 6 oktetů kóduje identifikátor objektu příkladu.“;

i) body 5.5 a 5.5.1 se nahrazují tímto:

„5.5 **Podpora pro směrnici (EU) 2015/719**

5.5.1 *Přehled*

DSC_59 Na podporu směrnice (EU) 2015/719 o maximálních hmotnostech a rozměrech těžkých nákladních vozidel je transakční protokol pro stahování dat OWS pomocí rozhraní 5,8 GHz DSRC stejný jako protokol používaný pro data RTM (viz 5.4.1); jediným rozdílem je, že identifikátor objektu, který se vztahuje k normě TARV, odpovídá normě ISO 15638 (TARV) části 20, týkající se WOB/OWS.“;

j) v bodě 5.6.1 se písmeno a) v odstavci DSC_68 nahrazuje tímto:

„a) Aby bylo možné uzavírat smlouvy na dodávky VU a DSRC-VU a rovněž různých sérií DSRC-VU s různými dodavateli, je spojení mezi VU a DSRC-VU, který není součástí VU, otevřeným standardním spojením. VU se s DSRC-VU spojuje buď“;

k) v bodě 5.7.1 se odstavec DSC_77 nahrazuje tímto:

„DSC_77 Již zabezpečená data jsou funkcí *VUSM* poskytnuta *DSRC-VU*. *VUSM* ověří, zda data zaznamenaná v *DSRC-VU* byla řádně zaznamenána. Zaznamenání a hlášení případných chyb v přenosu dat z *VU* do paměti *DSRC-VU* je zaznamenáno s typem EventFaultType a hodnotou enum nastavenou na ‘0C’H Chyba komunikace se zařízením pro dálkovou komunikaci s časovým razítkem.“;

40) dodatek 15 se mění takto:

a) v bodě 2.2 se první pododstavec nahrazuje tímto:

„Rozumí se, že karty tachografu první generace jsou interoperabilní s celky ve vozidle první generace v souladu s přílohou IB nařízení (EHS) č. 3821/85, zatímco karty tachografu druhé generace jsou interoperabilní s celky ve vozidle druhé generace v souladu s přílohou IC tohoto nařízení. Kromě toho se uplatní níže uvedené požadavky.“;

b) v bodě 2.4.1 se odstavec MIG_11 mění takto:

i) první odrážka se nahrazuje tímto:

„— nepodepsané elementární soubory EF ic a icc (volitelné),“;

ii) třetí odrážka se nahrazuje tímto:

„— ostatní elementární soubory EF s aplikačními daty (v rámci souboru DF Tachograph) vyžadované protokolem pro stahování dat z karet první generace. Tyto informace musí být zabezpečeny digitálním podpisem podle bezpečnostních mechanismů první generace.

Uvedené stahování nesmí zahrnovat elementární soubory EF s aplikačními daty, které jsou přítomny pouze na kartách řidiče (a kartách dílny) druhé generace (elementární soubory EF s aplikačními daty v rámci souboru DF Tachograph_G2).“;

c) v bodě 2.4.3 se odstavce MIG_014 a MIG_015 nahrazují tímto:

„MIG_014 Nad rámec kontroly řidičů kontrolními orgány, které nepatří do EU, se data musí stahovat z celků ve vozidle druhé generace pomocí bezpečnostních mechanismů druhé generace a protokolu pro stahování dat specifikovaného v dodatku 7 této přílohy.

MIG_015 Aby se umožnila kontrola řidičů kontrolními orgány, které nepatří do EU, lze také případně umožnit stahování dat z celků ve vozidle druhé generace pomocí bezpečnostních mechanismů první generace. Stahovaná data pak musí mít stejný formát jako data stahovaná z celku ve vozidle první generace. Tuto možnost lze zvolit pomocí příkazů v menu.“;

PŘÍLOHA II

Příloha II nařízení (EU) 2016/799 se mění takto:

1) v kapitole I bodě 1 se písmeno b) nahrazuje tímto:

„b) z čísla schválení, které odpovídá číslu osvědčení o schválení vystaveného pro prototyp záznamového zařízení nebo záznamového listu nebo karty tachografu a které se umístí kdekoli v bezprostřední blízkosti obdélníku.“;

2) v kapitole III se bod 5 nahrazuje tímto:

„5. Předloženo k schválení dne .....“;

3) v kapitole IV se bod 5 nahrazuje tímto:

„5. Předloženo k schválení dne .....“.

ISSN 1977-0626 (elektronické vydání)
ISSN 1725-5074 (papírové vydání)

Úřad pro publikace Evropské unie
2985 Lucemburk
LUCEMBURSKO

CS