Úřední věstník L 139

Evropské unie

Svazek 59

České vydání **Právní předpisy** 26. května 2016

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) 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

(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 digitální tachografy druhé generace, tzv. inteligentní tachografy, jejichž součástí je také napojení na globální družicový navigační systém („GNSS“), komunikační zařízení pro včasné dálkové odhalování a rozhraní s inteligentními dopravními systémy. Měly by být stanoveny specifikace technických požadavků na konstrukci inteligentních tachografů.

(2) Zařízení pro včasné dálkové odhalování stanovené v čl. 9 odst. 4 nařízení (EU) č. 165/2014 by mělo kontrolorům při silniční kontrole předávat údaje z digitálního tachografu a informace týkající se hmotností a hmotností na nápravu úplné soupravy vozidel (tahače a přívěsů nebo návěsů) v souladu se směrnicí Evropského parlamentu a Rady 96/53/ES ([2]). To by mělo umožnit účinnou a rychlou kontrolu vozidel ze strany kontrolních orgánů při nižším počtu elektronických zařízení v kabině vozidla.

(3) V souladu se směrnicí 96/53/ES by zařízení pro včasné dálkové odhalování mělo používat normy CEN DSRC ([3]) uvedené ve směrnici, a to v kmitočtovém pásmu 5 795–5 805 MHz. Vzhledem k tomu, že se toto kmitočtové pásmo používá i pro elektronický výběr mýtného, neměli by kontroloři zařízení pro včasné dálkové odhalování používat v prostorech určených pro výběr mýtného, aby se předešlo interferencím mezi aplikacemi pro výběr mýtného a pro kontrolu.

(4) Aby se vyřešila současná slabá místa v oblasti bezpečnosti, měly by spolu s inteligentními tachografy být zavedeny nové bezpečnostní mechanismy pro zachování úrovně bezpečnosti digitálních tachografů. Jedním z takových slabých míst je absence dat o konci doby platnosti digitálních certifikátů. Pro dosažení souladu s osvědčenými postupy v otázkách bezpečnosti se doporučuje digitální certifikáty bez dat o konci doby platnosti nepoužívat. Běžná doba provozní platnosti celků ve vozidle by měla být 15 let, počínaje dnem vydání digitálních certifikátů pro celek ve vozidle. Celky ve vozidle by po uvedené době platnosti měly být vyměněny.

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

([2]) Směrnice Rady 96/53/ES ze dne 25. července 1996, kterou se pro určitá silniční vozidla provozovaná v rámci Společenství stanoví maximální přípustné rozměry pro vnitrostátní a mezinárodní provoz a maximální přípustné hmotnosti pro mezinárodní provoz (Úř. věst. L 235, 17.9.1996, s. 59).

([3]) Normy Evropského výboru pro normalizaci (CEN) týkající se vyhrazených spojení krátkého dosahu EN 12253, EN 12795, EN 12834, EN 13372 a ISO 14906.

(5) Zajištění zabezpečených a spolehlivých informací o poloze je základním prvkem účinného fungování inteligentních tachografů. Je proto vhodné, aby byla zajištěna jejich kompatibilita se službami s přidanou hodnotou poskytovanými v rámci programu Galileo, jak je stanoveno v nařízení Evropského parlamentu a Rady (EU) č. 1285/2013 ([1]), s cílem zlepšit bezpečnost inteligentních tachografů.

(6) V souladu s čl. 8 odst. 1, čl. 9 odst. 1 a čl. 10 odst. 1 a 2 nařízení (EU) č. 165/2014 by se bezpečnostní mechanismy zavedené uvedeným nařízením měly použít 36 měsíců po vstupu potřebných prováděcích aktů v platnost, aby výrobci mohli vyvinout novou generaci inteligentních tachografů a získat od příslušných orgánů osvědčení o schválení typu.

(7) V souladu s nařízením (EU) č. 165/2014 by vozidla poprvé registrovaná v členském státě 36 měsíců po vstupu tohoto nařízení Komise v platnost měla být vybavena inteligentním tachografem, který splňuje požadavky tohoto nařízení Komise. V každém případě by všechna vozidla provozovaná v jiném členském státě, než je členský stát jejich registrace, měla být vybavena inteligentním tachografem, který splňuje požadavky, 15 let ode dne použitelnosti uvedených požadavků.

(8) Nařízení Komise (ES) č. 68/2009 ([2]) povolovalo během přechodného období, které skončilo dnem 31. prosince 2013, použití adaptéru, který umožňoval montáž tachografů do vozidel typu M1 a N1. Vzhledem k technickým problémům souvisejícím s nalezením alternativy k použití adaptéru došli odborníci z automobilového průmyslu a z řad výrobců tachografů spolu s Komisí k závěru, že k použití adaptéru neexistuje alternativní řešení, jež by se obešlo bez nepřiměřeně vysokých nákladů pro dotčené odvětví, což by nebylo úměrné velikosti trhu. Proto by používání adaptéru ve vozidlech typu M1 a N1 mělo být povoleno bez časového omezení.

(9) 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

Předmět a oblast působnosti

1. Toto nařízení obsahuje ustanovení nezbytná pro jednotné uplatňování následujících aspektů týkajících se tachografů:

a) zaznamenávání polohy vozidla v určitých místech během denní pracovní doby řidiče;

b) dálkového včasného odhalování případné manipulace s inteligentními tachografy nebo jejich zneužití;

c) rozhraní s inteligentními dopravními systémy;

d) administrativních a technických požadavků na postupy schválení typu tachografů, včetně bezpečnostních mechanismů.

2. Konstrukce, zkoušení, montáž, kontrola, provoz a opravy inteligentních tachografů a jejich součástí musí splňovat technické požadavky stanovené v příloze 1C tohoto nařízení.

3. Tachografy jiné než inteligentní musí nadále, pokud jde o jejich konstrukci, zkoušení, montáž, kontrolu, provoz a opravy, splňovat podle konkrétního případu buď požadavky stanovené v příloze 1, nebo v příloze 1B nařízení Rady (EHS) č. 3821/85 ([3]).

([1]) Nařízení Evropského parlamentu a Rady (EU) č. 1285/2013 ze dne 11. prosince 2013 o zřízení evropských systémů družicové navigace a jejich využití a o zrušení nařízení Rady (ES) č. 876/2002 a nařízení Evropského parlamentu a Rady (ES) č. 683/2008 (Úř. věst. L 347, 20.12.2013, s. 1).

([2]) Nařízení Komise (ES) č. 68/2009 ze dne 23. ledna 2009, kterým se podeváté přizpůsobuje technickému pokroku nařízení Rady (EHS) č. 3821/85 o záznamovém zařízení v silniční dopravě (Úř. věst. L 21, 24.1.2009, s. 3).

([3]) 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).

4. Podle článku 10d směrnice Evropského parlamentu a Rady 96/53/ES musí zařízení pro včasné dálkové odhalování rovněž předávat údaje o hmotnosti poskytované interním palubním systémem pro zjišťování hmotnosti za účelem včasného odhalování podvodů.

Článek 2

Definice

Pro účely tohoto nařízení se použijí definice stanovené v článku 2 nařízení (EU) č. 165/2014.

Kromě toho se rozumí:

1) „digitálním tachografem“ nebo „tachografem první generace“ digitální tachograf, který není inteligentním tachografem;

2) „vnějším zařízením GNSS“ zařízení, které obsahuje přijímač GNSS v případě, kdy celek ve vozidle není jediným celkem, jakož i další součásti nezbytné pro ochranu sdělování údajů o poloze zbytku celku ve vozidle;

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 1C tohoto nařízení, jakož i výkresy, fotografie a další příslušné doklady;

4) „schvalovací dokumentací“ dokumentace výrobce v elektronické nebo tištěné podobě společně s dalšími dokumenty přiloženými orgánem příslušným pro schvalování typu k dokumentaci výrobce v průběhu výkonu jeho funkcí, včetně osvědčení ES schválení typu tachografu nebo jeho konstrukční součásti na konci postupu schvalování typu;

5) „seznamem schvalovací dokumentace“ dokument uvádějící očíslovaný obsah schvalovací dokumentace identifikující všechny relevantní části této dokumentace. Formát tohoto dokumentu musí rozlišovat po sobě jdoucí kroky při postupu ES schvalování typu, včetně dat všech revizí a aktualizací uvedené dokumentace;

6) „zařízením pro včasné dálkové odhalování“ zařízení celku ve vozidle, které je používáno k provádění cílených silničních kontrol;

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 1C tohoto nařízení;

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

9) „orgánem příslušným pro schvalování typu“ orgán členského státu oprávněný k provádění schvalování typu tachografu nebo jeho součástí, provádění postupu schvalování, vydávání a v příslušných případech odebírání osvědčení o schválení typu, který působí jako kontaktní místo pro orgány příslušné pro schvalování typu ostatních členských států a zajišťuje, aby výrobci plnili své povinnosti týkající se souladu s požadavky tohoto nařízení.

Článek 3

Služby vycházející z určení polohy

1. Výrobci zajistí, aby inteligentní tachografy byly kompatibilní se službami určování polohy, které poskytují systémy Galileo a evropská služba pro pokrytí geostacionární navigací (EGNOS).

2. Výrobci se mohou také rozhodnout, že kromě systémů uvedených v odstavci 1 zajistí kompatibilitu s dalšími družicovými navigačními systémy.

Článek 4

Postup schvalování typu tachografu a součástí tachografu

1. Výrobce nebo jeho zmocněnec předloží žádost o schválení typu tachografu nebo jakékoli jeho součásti nebo skupiny součástí orgánům příslušným pro schvalování typu určeným každým členským státem. Žádost se skládá se z dokumentace výrobce obsahující informace o všech dotčených součástech, v příslušných případech včetně osvědčení o schválení typu ostatních součástí, jež jsou nezbytné ke zkompletování tachografu, jakož i všech dalších příslušných dokumentů.

2. Členský stát udělí schválení typu všem tachografům, součástem nebo skupinám součástí, které splňují administrativní a technické požadavky uvedené v příslušných případech v čl. 1 odst. 2 nebo 3. V takovém případě vydá orgán příslušný pro schvalování typu žadateli osvědčení o schválení typu, které musí být v souladu se vzorem uvedeným v příloze II tohoto nařízení.

3. Orgán příslušný pro schvalování typu může požádat výrobce nebo jeho zmocněnce o předložení jakýchkoli dalších informací.

4. Výrobce nebo jeho zmocněnec dá orgánům příslušným pro schvalování typu, jakož i subjektům odpovědným za vydávání osvědčení uvedených v čl. 12 odst. 3 nařízení (EU) č. 165/2014 k dispozici takový počet tachografů nebo součástí tachografů, který je nezbytný k tomu, aby mohl být uspokojivé proveden postup schválení typu.

5. Jestliže chce výrobce nebo jeho zmocněnec získat schválení typu určitých součástí nebo skupin součástí tachografu, musí orgánům příslušným pro schvalování typu poskytnout ostatní součásti, jejichž typ byl již schválen, jakož i ostatní součásti nezbytné pro konstrukci kompletního tachografu, aby tyto orgány mohly provést potřebné zkoušky.

Článek 5

Změny schválení typu

1. Výrobce nebo jeho zmocněnec neprodleně uvědomí orgány příslušné pro schvalování typu, které udělily původní schválení typu, o všech změnách softwarového nebo hardwarového vybavení tachografu nebo povahy materiálů použitých k jeho výrobě, které jsou zaznamenány ve schvalovací dokumentaci, a předloží žádost o změnu schválení typu.

2. Orgány příslušné pro schvalování typu mohou podle povahy a charakteru těchto změn revidovat či rozšířit stávající schválení typu nebo vydat nové schválení typu.

„Revize“ se provede, jestliže se orgán příslušný pro schvalování typu domnívá, že změny softwarového nebo hardwarového vybavení tachografu nebo povahy materiálů použitých k jeho výrobě jsou malé. V takových případech orgán příslušný pro schvalování typu vydá revidované dokumenty schvalovací dokumentace a uvede povahu provedených změn a datum jejich schválení. Pro splnění tohoto požadavku postačuje aktualizovaná verze schvalovací dokumentace v konsolidované podobě spolu s podrobným popisem provedených změn.

„Rozšíření“ se provede, jestliže se orgán příslušný pro schvalování typu domnívá, že změny softwarového nebo hardwarového vybavení tachografu nebo povahy materiálů použitých k jeho výrobě jsou významné. V takových případech může požadovat provedení nových zkoušek a v souladu s tím informovat výrobce nebo jeho zmocněnce. Pokud jsou tyto zkoušky uspokojivé, vydá orgán příslušný pro schvalování typu revidované osvědčení o schválení typu, s číslem odkazujícím na udělené rozšíření. V osvědčení o schválení typu se uvede důvod rozšíření a datum jeho vystavení.

3. V seznamu schvalovací dokumentace se uvede datum posledního rozšíření, nebo revize schválení typu, nebo datum poslední konsolidace aktualizované verze tohoto schválení typu.

4. Nové schválení typu je nezbytné, pokud by požadované změny tachografu, jehož typ byl již schválen, nebo jeho součástí vedly k vydání nového osvědčení o bezpečnosti nebo interoperabilitě.

Článek 6

Vstup v platnost

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

Použije se ode dne 2. března 2016.

Přílohy se však použijí ode dne 2. března 2019, s výjimkou dodatku 16, který se použije ode dne 2. března 2016.

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

V Bruselu dne 18. března 2016.

Za Komisi
předseda
Jean-Claude JUNCKER

PŘÍLOHA I C

Požadavky na konstrukci, zkoušení, montáž a kontrolu

ÚVOD

Systém digitálních tachografů první generace byl zaveden 1. května 2006. V oblasti vnitrostátní dopravy se může používat po celou dobu své životnosti. Naproti tomu v oblasti mezinárodní dopravy musí být všechna vozidla nejpozději 15 let po vstupu tohoto nařízení Komise v platnost vybavena vyhovujícím inteligentním tachografem druhé generace, který zavádí toto nařízení.

Tato příloha obsahuje požadavky na záznamové zařízení a karty tachografu druhé generace.

Od data zavedení je záznamové zařízení druhé generace montováno ve vozidlech registrovaných poprvé a jsou vydávány karty tachografu druhé generace. Pro usnadnění plynulého zavádění systému tachografů druhé generace

— jsou karty tachografu druhé generace navrženy tak, aby byly použitelné i v celcích ve vozidle první generace,

— není k datu zavedení požadována výměna platných karet tachografu první generace.

Řidičům to umožní ponechat si svou jedinečnou kartu řidiče a používat ji v obou systémech.

Záznamové zařízení druhé generace však musí být kalibrováno pouze pomocí karet dílny druhé generace.

Tato příloha obsahuje všechny požadavky týkající se interoperability mezi systémy tachografů první a druhé generace.

Dodatek 15 obsahuje dodatečné podrobnosti o správě obou souběžně existujících systémů.

Seznam dodatků

1 DEFINICE

Pro účely této přílohy se rozumí:

a) „aktivací“:

fáze, ve které se tachograf použitím karty dílny stává plně funkčním a ve které provádí veškeré funkce, včetně funkcí bezpečnostních;

b) „prokázáním pravosti“:

funkce určená ke stanovení a ověření uváděné identity;

c) „pravostí“:

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

d) „integrovanou zkouškou“:

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

e) „kalendářním dnem“:

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

f) „kalibrací“ inteligentních tachografů:

aktualizace nebo potvrzení parametrů vozidla, které je třeba uchovat v datové paměti. Parametry vozidla zahrnují identifikaci vozidla (identifikační číslo vozidla VIN, registrační značka vozidla VRN a členský stát registrace) a vlastnosti vozidla (charakteristický koeficient vozidla *w*, konstantu záznamového zařízení *k*, účinný obvod kol *l*, rozměr pneumatik, nastavení omezovače rychlosti (v příslušných případech), aktuální čas UTC, aktuální stav počitadla ujetých kilometrů); během kalibrace záznamového zařízení jsou v datové paměti rovněž uloženy typy a identifikátory všech příslušných plomb schválení typu.

Jakékoli obnovení nebo potvrzení pouze času UTC se považuje za úpravu času, a nikoli za kalibraci, pokud není v rozporu s požadavkem 409.

Kalibrace záznamového zařízení vyžaduje použití karty dílny;

g) „číslem karty“:

šestnáctimístné alfanumerické označení, které v členském státě jednoznačně identifikuje kartu tachografu. Číslo karty zahrnuje (v příslušných případech) pořadový index karty, index náhrady karty a index obnovy karty.

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

h) „pořadovým indexem karty“:

čtrnáctý alfanumerický znak v čísle karty, který je užit pro rozlišení různých karet vydaných určitému podniku, dílně nebo kontrolnímu orgánu, které mají právo na vydání více karet tachografu. Podnik, dílna nebo kontrolní orgán jsou jednoznačně identifikovány prvními třinácti znaky čísla karty;

i) „indexem obnovy karty“:

šestnáctý alfanumerický znak v čísle karty, který je zvyšován pokaždé, když je karta obnovována;

j) „indexem náhrady karty“:

patnáctý alfanumerický znak v čísle karty, který je zvyšován pokaždé, když je karta nahrazována;

k) „charakteristickým koeficientem vozidla“:

číselné označení, které udává hodnotu výstupního signálu vysílaného částí vozidla, která je propojuje se záznamovým zařízením (výstupní hřídel převodovky nebo náprava), když vozidlo ujede za standardních zkušebních podmínek vzdálenost 1 km, jak stanoví požadavek 414. Charakteristický koeficient se vyjadřuje v počtu impulsů na kilometr (w = … imp/km);

l) „kartou podniku“:

karta tachografu vydaná orgány členského státu dopravci, který potřebuje provozovat vozidla vybavená tachografem. Karta identifikuje dopravce a umožňuje zobrazování, stahování a tištění údajů uložených v tachografu, která byla tímto dopravcem uzamčena;

m) „konstantou záznamového zařízení“:

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

n) „nepřetržitá doba řízení“ se vypočítává v záznamovém zařízení jako ([1]):

nepřetržitá doba řízení, která se vypočítává jako běžná součtová doba řízení určitého řidiče od konce jeho poslední POHOTOVOSTI nebo PŘESTÁVKY/ODPOČINKU nebo NEZNÁMÉ DOBY ([2]) v délce 45 minut nebo doby delší (tato doba může být rozdělena v souladu s nařízením Evropského parlamentu a Rady (ES) č. 561/2006 ([3])). Příslušné výpočty berou podle potřeby v úvahu minulé činnosti uložené na kartě řidiče. Pokud řidič nevložil svou kartu, jsou příslušné výpočty podloženy údaji z paměťových záznamů, které se vztahují k běžné době, kdy nebyla vložena žádná karta, a které se vztahují k odpovídajícímu otvoru pro kartu;

o) „kontrolní kartou“:

karta tachografu vydaná orgány členského státu příslušnému národnímu kontrolnímu orgánu, která identifikuje kontrolní organizaci a případně i kontrolora a umožňuje přístup k údajům uloženým v datové paměti nebo na kartách řidiče a případně na kartách dílny pro čtení, tisk a/nebo stahování.

Umožňuje rovněž přístup k funkci silniční kalibrační kontroly a k údajům na snímači komunikace včasného dálkového odhalování;

p) „souhrnnou dobou přestávek“ vypočítávanou v rámci záznamového zařízení jako ([1]):

souhrnná doba přestávek v jízdě vypočtená z běžných kumulovaných dob POHOTOVOSTI nebo PŘESTÁVKY/ODPOČINKU nebo NEZNÁMÉ DOBY ([2]) daného řidiče, které jsou dlouhé 15 minut nebo delší, od konce jeho poslední doby POHOTOVOSTI nebo PŘESTÁVKY/ODPOČINKU nebo NEZNÁMÉ DOBY ([2]), které jsou dlouhé 45 minut nebo delší (tato doba může být rozdělena v souladu s nařízením (ES) č. 561/2006).

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

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

([1]) Tento způsob výpočtu nepřetržité doby řízení a kumulativní doby přestávek slouží v záznamovém zařízení pro výpočet varování o nepřetržité době řízení. To však nenahrazuje právní výklad, který je třeba použít na tyto doby. Alternativní způsoby výpočtu nepřetržité doby řízení a souhrnné doby přestávek lze použít k nahrazení těchto definic, pokud by se staly zastaralými v důsledku aktualizací v jiných příslušných právních předpisech.

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

([3]) Nařízení Evropského parlamentu a Rady (ES) č. 561/2006 ze dne 15. března 2006 o harmonizaci některých předpisů v sociální oblasti týkajících se silniční dopravy, o změně nařízení Rady (EHS) č. 3821/85 a (ES) č. 2135/98 a o zrušení nařízení Rady (EHS) č. 3820/85 (Úř. věst. L 102, 11.4.2006, s. 1).

q) „datovou pamětí“:

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

r) „digitálním podpisem“:

údaje, které jsou připojeny k bloku údajů nebo kryptografická transformace bloku údajů, které příjemci bloku údajů umožňují prokázání pravosti a integrity bloku údajů;

s) „stahováním“:

kopírování, spolu s digitálním podpisem, části nebo úplné sady datových souborů zaznamenaných v datové paměti celku ve vozidle nebo v paměti karty tachografu, pokud tento postup nezmění nebo nesmaže žádné uložené údaje.

Výrobci inteligentních tachografových celků ve vozidle a výrobci zařízení konstruovaných a určených ke stahování datových souborů musí podniknout veškeré přiměřené kroky k zajištění toho, aby stahování takových údajů dopravce nebo řidiče co nejméně zdržovalo.

Stahování podrobných údajů o rychlosti nemusí být nutné k prokázání shody s nařízením (ES) č. 561/2006, ale může být použito pro jiné účely, např. pro vyšetřování nehod.

t) „kartou řidiče“:

karta tachografu vystavená orgány členského státu určitému řidiči, která identifikuje řidiče a umožňuje ukládání údajů o jeho činnostech;

u) „účinným obvodem kol“:

průměrná vzdálenost ujetá každým z kol poháněných vozidlo (hnací kola) v průběhu jedné ukončené otáčky. Tyto vzdálenosti jsou měřeny za normálních zkušebních podmínek, jak stanoví požadavek 414, a vyjadřují se ve tvaru: „l = … mm“. Výrobci vozidla mohou měření těchto vzdáleností nahradit teoretickým výpočtem, který bere v úvahu rozložení hmotností na nápravy pro nenaložené vozidlo v běžném provozním stavu ([1]). Postupy pro tyto teoretické výpočty podléhají schválení příslušného orgánu členského státu a mohou být provedeny výhradně před aktivací tachografu;

v) „událostí“:

mimořádná činnost zjištěná inteligentním tachografem, která může pocházet z pokusu o podvod;

w) „vnějším zařízením GNSS“:

zařízení obsahující přijímač GNSS, není-li celek ve vozidle samostatnou jednotkou, a další součásti potřebné k ochraně komunikace údajů o poloze se zbytkem celku ve vozidle;

x) „závadou“:

mimořádná činnost zjištěná inteligentním tachografem, která může pocházet z chybné funkce nebo z poruchy zařízení;

y) „přijímačem GNSS“:

elektronické zařízení, které přijímá a digitálně zpracovává signály z jednoho nebo více globálních navigačních družicových systémů (GNSS v angličtině) pro poskytování informací o poloze, rychlosti a čase;

z) „montáží“:

montáž tachografu do vozidla;

([1]) Nařízení Komise (EU) č. 1230/2012 ze dne 12. prosince 2012, kterým se provádí nařízení Evropského parlamentu a Rady (ES) č. 661/2009, pokud jde o požadavky pro schvalování typu motorových vozidel a jejich přípojných vozidel týkající se jejich hmotností a rozměrů, a mění směrnice Evropského parlamentu a Rady 2007/46/ES (Úř. věst. L 353, 21.12.2012, s. 31) v platném znění.

aa) „interoperabilitou“:

schopnost systémů a příslušných podnikových procesů vyměňovat si údaje a sdílet informace;

bb) „rozhraním“:

zařízení mezi systémy, které poskytuje prostředí pro jejich spojení a součinnost;

cc) „polohou“:

zeměpisné souřadnice vozidla v daném čase;

dd) „snímačem pohybu“:

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

ee) „neplatnou kartou“:

karta, která byla zjištěna jako vadná nebo u které chybí úvodní prokázání pravosti nebo u které ještě nebylo dosaženo data platnosti nebo u které již uplynulo datum platnosti;

ff) „otevřeným standardem“:

standard stanovený v dokumentu standardních specifikací dostupném volně nebo za nominální poplatek, který může být kopírován, rozšiřován nebo používán bezplatně nebo za nominální poplatek;

gg) „mimo působnost“:

případ, kdy není podle nařízení (ES) č. 561/2006 užívání záznamového zařízení požadováno;

hh) „překročením rychlosti“:

překročení povolené rychlosti vozidla, které je definováno jako jakékoliv období delší než 60 s, v němž měřená rychlost vozidla překračuje mezní hodnotu pro nastavení omezovače rychlosti, která byla stanovena směrnicí Rady 92/6/EHS [1] v platném znění;

ii) „pravidelnou kontrolou“:

řada operací ke kontrole, že tachograf správně pracuje, že jeho seřízení odpovídá parametrům vozidla a že k tachografu nejsou připojena žádná manipulační zařízení;

jj) „tiskárnou“:

součást záznamového zařízení, které zajišťuje vytištění uložených údajů;

kk) „komunikací včasného dálkového odhalování“:

komunikace mezi zařízením komunikace včasného dálkového odhalování a snímačem komunikace včasného dálkového odhalování během cílených silničních kontrol s cílem dálkového odhalování možné manipulace nebo zneužití záznamového zařízení;

ll) „zařízením pro dálkovou komunikaci“:

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

[1] Směrnice Rady 92/6/EHS ze dne 10. února 1992 o montáži a použití omezovačů rychlosti u určitých kategorií motorových vozidel ve Společenství (Úř. věst. L 57, 2.3.1992, s. 27).

mm) „snímačem komunikace včasného dálkového odhalování“:

systém používaný kontrolory pro cílené silniční kontroly;

nn) „obnovením“:

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

oo) „opravou“:

oprava snímače pohybu nebo celku ve vozidle nebo kabelu, která vyžaduje jejich odpojení od napájení nebo odpojení od jiných součástí tachografu nebo otevření snímače pohybu nebo celku ve vozidle;

pp) „náhradou karty“:

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

qq) „osvědčením bezpečnosti“:

postup, kterým orgán pro certifikaci všeobecných kritérií osvědčuje, že zkoumané záznamové zařízení (nebo jeho součást) nebo karta tachografu splňuje bezpečnostní požadavky stanovené v příslušných ochranných profilech;

rr) „autotestem“:

zkouška, která probíhá v záznamovém zařízení cyklicky a automaticky za účelem zjištění závad;

ss) „měřením času“:

nepřetržitý digitální záznam koordinovaného světového data a času (UTC);

tt) „nastavením času“:

automatické nastavení aktuálního času v pravidelných intervalech s maximální tolerancí jedné minuty, nebo nastavení prováděné během kalibrace;

uu) „rozměrem pneumatiky“:

stanovení rozměrů pneumatik (vnějších hnacích kol) podle směrnice Rady 92/23/EHS ([1]) v platném znění;

vv) „identifikací vozidla“:

čísla, která vozidlo identifikují: registrační značka vozidla (VRN) s uvedením členského státu registrace a identifikační číslo vozidla (VIN) ([2]);

ww) „týdnem“ pro účely výpočtu v záznamovém zařízení:

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

([1]) Směrnice Rady 92/23/EHS ze dne 31. března 1992 o pneumatikách pro motorová vozidla a jejich přípojná vozidla a o jejich montáži (Úř. věst. L 129, 14.5.1992, s. 95).

([2]) Směrnice Rady 76/114/EHS ze dne 18. prosince 1975 o sbližování právních předpisů členských států týkajících se povinných štítků a nápisů pro motorová vozidla a pro jejich přípojná vozidla a pro jejich umístění a způsob upevnění (Úř. věst. L 24, 30.1.1976, s. 1).

xx) „kartou dílny“:

karta tachografu vydaná orgány členského státu určeným pracovníkům výrobce tachografu, montážního podniku, výrobce vozidla nebo dílně schváleným uvedeným členským státem, která identifikuje držitele karty a umožňuje zkoušení, kalibraci a aktivaci tachografů a/nebo stahování údajů z nich;

yy) „adaptérem“:

zařízení, které zajišťuje signál trvale odpovídající rychlosti vozidla a/nebo vzdálenosti ujeté vozidlem, jiné než zařízení používané pro nezávislé sledování pohybu, a které je:

— zabudováno a užíváno pouze ve vozidlech typu M1 a N1 (podle definice v příloze II směrnice Evropského parlamentu a Rady 2007/46/ES ([1]) v platném znění), uvedených do provozu po 1. květnu 2006 včetně,

— zabudováno tam, kde není mechanicky možné zabudovat jiný typ existujícího snímače pohybu, který je jinak v souladu s ustanoveními této přílohy a dodatků 1 až 15,

— zabudováno mezi celkem ve vozidle a místem, odkud integrované snímače nebo alternativní rozhraní vysílají impulsy rychlosti/vzdálenosti,

— co se týče celku ve vozidle, je chování adaptéru stejné, jako by byl k celku ve vozidle připojen snímač pohybu, který je v souladu s ustanoveními této přílohy a dodatků 1 až 16.

Použití takového adaptéru ve výše popsaných vozidlech umožní montáž a správné užívání celku ve vozidle vyhovujícího všem požadavkům v této příloze.

U těchto vozidel inteligentní tachograf zahrnuje kabely, adaptér a celek ve vozidle;

zz) „integritou údajů“:

přesnost a konzistentnost uložených údajů, jejichž dokladem je absence jakékoli změny údajů mezi dvěma aktualizacemi záznamů. Integrita znamená, že údaje jsou přesnou kopií původní verze, např. že nebyly porušeny při zápisu na kartu tachografu nebo vyhrazené zařízení a načítání z nich nebo během přenosu jakýmkoli komunikačním kanálem;

aaa) „důvěrností údajů“:

všeobecná technická opatření pro řádné provádění zásad podle směrnice Evropského parlamentu a Rady 95/46/ES ([2]) a podle směrnice Evropského parlamentu a Rady 2002/58/ES ([3]);

bbb) „systémem inteligentního tachografu“:

záznamové zařízení, karty tachografu a veškerá zařízení přímo nebo nepřímo spolupracující během konstrukce, montáže, používání, zkoušení a kontroly, např. karty, snímač dálkové komunikace a další zařízení pro stahování údajů, analýzu údajů, kalibraci, vytváření, správu nebo zavádění bezpečnostních prvků atd.;

ccc) „datem zavedení“:

36 měsíců od vstupu podrobných ustanovení podle článku 11 nařízení Evropského parlamentu a Rady (EU) č. 165/2014 ([4]) v platnost.

([1]) Směrnice Evropského parlamentu a Rady 2007/46/ES ze dne 5. září 2007, kterou se stanoví rámec pro schvalování motorových vozidel a jejich přípojných vozidel, jakož i systémů, konstrukčních částí a samostatných technických celků určených pro tato vozidla (rámcová směrnice) (Úř. věst. L 263, 9.10.2007, s. 1).

([2]) Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (Úř. věst. L 281, 23.11.1995, s. 31).

([3]) Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (Úř. věst. L 201, 31.7.2002, s. 37).

([4]) Nařízení Evropského parlamentu a Rady (EU) č. 165/2014 ze dne 4. února 2014 o tachografech v silniční dopravě, o zrušení nařízení Rady (EHS) č. 3821/85 o záznamovém zařízení v silniční dopravě a o změně nařízení Evropského parlamentu a Rady (ES) č. 561/2006 o harmonizaci některých předpisů v sociální oblasti týkajících se silniční dopravy (Úř. věst. L 60, 28.2.2014, s. 1).

Je to datum, od kterého vozidla registrovaná poprvé:

— *musí být vybavena tachografem připojeným ke službě určování polohy na základě družicového navigačního systému,*

— *musí být schopna předávat údaje pro cílené silniční kontroly příslušným kontrolním orgánům během jízdy vozidla,*

— *a mohou být vybavena standardními rozhraními umožňujícími, aby údaje zaznamenané nebo vytvořené tachografem byly používány v provozním režimu vnějším zařízením;*

ddd) „ochranným profilem“:

dokument používaný jako součást certifikačního postupu v souladu se všeobecnými kritérii, který obsahuje specifikaci bezpečnostních požadavků na zabezpečení informací, nezávislou na způsobu provedení;

eee) „přesností GNSS“:

v souvislosti se zaznamenáváním polohy z globálního navigačního družicového systému (GNSS) pomocí tachografů, hodnota horizontálního zředění přesnosti (HDOP) vypočítaná jako minimum z hodnot HDOP zjištěných na dostupných systémech GNSS.

2 OBECNÉ VLASTNOSTI A FUNKCE ZÁZNAMOVÉHO ZAŘÍZENÍ

2.1 **Obecné vlastnosti**

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

Jakékoliv vozidlo vybavené záznamovým zařízením, které vyhovuje podmínkám této přílohy, musí mít displej rychloměru a počitadlo ujetých kilometrů. Tyto funkce mohou být součástí záznamového zařízení.

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

02) Rozhraní mezi snímači pohybu a celky ve vozidle musí splňovat požadavky specifikované v dodatku 11.

03) Celek ve vozidle musí být připojen k jednomu nebo více globálním navigačním družicovým systémům podle specifikace v dodatku 12.

04) Celek ve vozidle musí komunikovat se snímači komunikace včasného dálkového odhalování podle specifikace v dodatku 14.

05) Celek ve vozidle může obsahovat rozhraní ITS, které je specifikováno v dodatku 13.

Záznamové zařízení může být připojeno k dalším zařízením přídavnými rozhraními a/nebo volitelným rozhraním ITS.

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

Uživatelé záznamového zařízení se identifikují v zařízení prostřednictvím karet tachografu.

07) Záznamové zařízení zajišťuje selektivní přístupová práva k údajům a funkcím v závislosti na typu a/nebo identitě uživatele.

Záznamové zařízení zaznamenává a ukládá údaje do své datové paměti, do zařízení pro dálkovou komunikaci a na karty tachografu.

Toto se děje v souladu se směrnicí 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů ([1]), se směrnicí 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací ([2]) a v souladu s článkem 7 nařízení (EU) č. 165/2014.

2.2 **Funkce**

08) Záznamové zařízení musí zajistit tyto funkce:

- monitorování vkládání a vyjímání karet,
- měření rychlosti, vzdálenosti a polohy,
- měření času,
- monitorování činnosti řidiče,
- monitorování provozního stavu řidiče
- údaje vkládané řidičem ručně:
  - vkládání údajů o místech počátku a/nebo ukončení denní pracovní doby,
  - ruční vkládání údajů o činnostech řidiče,
  - vkládání údajů o zvláštních podmínkách
- správa zámků podniků,
- monitorování kontrolních činností,
- zjišťování událostí a/nebo závad,
- integrované zkoušky a autotesty,
- načítání z datové paměti,
- zaznamenávání a ukládání údajů do datové paměti,
- čtení údajů z karet tachografu,
- zaznamenávání a ukládání údajů na karty tachografu,
- zobrazování,
- tisk,
- výstraha,
- stahování údajů do vnějších médií,
- dálková komunikace pro cílené silniční kontroly,
- výstup údajů na přídavná zařízení,
- kalibrace,
- silniční kalibrační kontrola,
- nastavení času.

([1]) Úř. věst. č. L 281, 23.11.1995, s. 31.
([2]) Úř. věst. č. L 201, 31.7.2002, s. 37.

2.3 **Provozní režimy**

09) Záznamové zařízení musí být schopno pracovat ve čtyřech režimech:

— v provozním režimu,

— v kontrolním režimu,

— v kalibračním režimu,

— v podnikovém režimu.

10) Záznamové zařízení se přepíná do následujících provozních režimů podle platné karty tachografu vložené do čtecích zařízení karet. Pro určení provozního režimu nemá generace karty tachografu význam, je-li vložená karta platná. Karta dílny první generace je vždy považována za neplatnou, je-li vložena do celku ve vozidle druhé generace.

Provozní režim		Otvor pro vložení karty řidiče				
		Bez karty	Karta řidiče	Kontrolní karta	Karta dílny	Karta podniku
Otvor pro vložení karty druhého řidiče	Bez karty	Provozní	Provozní	Kontrolní	Kalibrační	Podnikový
	Karta řidiče	Provozní	Provozní	Kontrolní	Kalibrační	Podnikový
	Kontrolní karta	Kontrolní	Kontrolní	Kontrolní (*)	Provozní	Provozní
	Karta dílny	Kalibrační	Kalibrační	Provozní	Kalibrační (*)	Provozní
	Karta podniku	Podnikový	Podnikový	Provozní	Provozní	Podnikový (*)

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

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

12) Všechny funkce uvedené v bodě 2.2 musí být aktivní v jakémkoli provozním režimu s těmito výjimkami:

— kalibrační funkce je přístupná pouze v kalibračním režimu,

— funkce silniční kalibrační kontroly je přístupná pouze v kontrolním režimu,

— funkce správy zámků podniků je přístupná pouze v podnikovém režimu,

— funkce monitorování kontrolních činností je funkční pouze v kontrolním režimu,

— funkce stahování není přístupná v provozním režimu (s výjimkou ustanovení požadavku 193) a kromě stahování karty řidiče, není-li do celku ve vozidle vložen jiný typ karty.

13) Záznamové zařízení může předat data na displej, do tiskárny nebo na vnější rozhraní s těmito výjimkami:

— v provozním režimu musí být jakékoliv osobní identifikační údaje (příjmení nebo jméno(a)), které neodpovídají vložené kartě tachografu, ignorovány a jakékoliv číslo karty neodpovídající vložené kartě tachografu musí být částečně ignorováno (každý lichý znak – odleva doprava – musí obsahovat prázdnou hodnotu),

— v podnikovém režimu lze výstup údajů vztahujících se k osobě řidiče (požadavky 102, 105 a 108) provádět pouze za časová období, která nejsou uzamčena nebo která nemá uzamčena žádný jiný podnik (jak je označeno prvními 13 místy číselného kódu karty podniku),

— pokud není v záznamovém zařízené vložena žádná karta, výstup údajů vztahujících se k osobě řidiče lze provádět pouze pro aktuální den a osm předcházejících kalendářních dnů,

— výstup osobních údajů pocházejících z celku ve vozidle se nesmí provádět pomocí rozhraní ITS celku ve vozidle, není-li ověřen souhlas řidiče, k němuž se údaje vztahují,

— celky ve vozidle mají normální dobu platnosti používání 15 let od data vydání osvědčení celku ve vozidle, ale celky ve vozidle lze používat další tři měsíce pouze pro stahování údajů.

2.4 **Bezpečnost**

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 záznamovým zařízením 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.

14) Aby se dosáhlo bezpečnosti systému, musí následující součásti splnit bezpečnostní požadavky uvedené v jejich ochranných profilech, jak stanoví dodatek 10:

— celek ve vozidle,

— karta tachografu,

— snímač pohybu,

— vnější zařízení GNSS (tento profil je potřebný a použitelný pouze pro variantu vnějšího GNSS).

3 KONSTRUKČNÍ A FUNKČNÍ POŽADAVKY NA ZÁZNAMOVÉ ZAŘÍZENÍ

3.1 **Monitorování vkládání a vyjímání karet**

15) Záznamové zařízení monitoruje vkládání karty do čtecích zařízení karet a její vyjímání.

16) Při vložení karty ověřuje záznamové zařízení, zda vložená karta je platná karta tachografu, a v takovém případě identifikuje typ a generaci karty.

Pokud karta, která má stejné číslo a vyšší index obnovy, již byla vložena do záznamového zařízení, je označena za neplatnou.

Pokud karta, která má stejné číslo a index obnovy, ale vyšší index náhrady, již byla vložena do záznamového zařízení, je označena za neplatnou.

17) Karty tachografu první generace považuje záznamové zařízení za neplatné, pokud dílna zablokuje možnost použití karet tachografu první generace v souladu s dodatkem 15 (pož. MIG003).

18) Karty dílny první generace, které jsou vloženy do záznamového zařízení druhé generace, jsou považovány za neplatné.

19) Záznamové zařízení se navrhuje tak, že karty tachografu jsou po správném vložení do čtecích zařízení karet zamčeny v této poloze.

20) K uvolnění karet tachografu může dojít pouze po zastavení vozidla a poté, co byly příslušné údaje uloženy na kartách. Uvolnění karty musí vyžadovat aktivní zásah uživatele.

3.2 **Měření rychlosti, polohy a vzdálenosti**

21) Hlavním zdrojem měření rychlosti a vzdálenosti je snímač pohybu (případně zabudovaný v adaptéru).

22) Tato funkce musí měřit nepřetržitě a musí být schopna dodávat stav počitadla ujetých kilometrů odpovídající celkové vzdálenosti ujeté vozidlem na základě impulsů vydávaných snímačem pohybu.

23) Tato funkce musí měřit nepřetržitě a musí být schopna udávat rychlost vozidla na základě impulsů vydávaných snímačem pohybu.

24) Funkce měření rychlosti musí být také schopna dodávat informace, zda je vozidlo v pohybu, nebo se zastavilo. Vozidlo je považováno za pohybující se, jakmile funkce registruje od snímače pohybu více než 1 imp/s po dobu nejméně pěti sekund. Jinak se vozidlo považuje za stojící.

25) Zařízení zobrazující rychlost (rychloměr) a měřidlo celkové ujeté vzdálenosti (počítadlo ujetých kilometrů), namontované v jakémkoli vozidle, které je vybaveno záznamovým zařízením, vyhovujícím ustanovením tohoto nařízení, musí vyhovovat požadavkům týkajícím se maximálních tolerancí (viz body 3.2.1 a 3.2.2), které jsou uvedeny v této příloze.

26) Aby bylo možno zjistit manipulaci údajů o pohybu, je nutno informace ze snímače pohybu podpořit dalšími údaji o pohybu vozidla odvozenými z přijímače GNSS a volitelně z jednoho nebo více dalších zdrojů nezávislých na snímači pohybu.

27) Tato funkce měří polohu vozidla, čímž umožňuje automatický záznam:

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

— poloh, kde nepřetržitá doba řízení řidiče dosáhne násobku tří hodin;

— poloh, kde řidič a/nebo druhý řidič končí svou denní pracovní dobu.

3.2.1 *Měření ujeté vzdálenosti*

28) Ujetá vzdálenost může být měřena buď:

— tak, že se načítá dopředný i zpětný pohyb, nebo

— tak, že je brán v úvahu pouze dopředný pohyb.

29) Záznamové zařízení měří vzdálenost od 0 do 9 999 999,9 km.

30) Měření vzdálenosti musí být v následujících tolerancích (vzdálenosti nejméně 1 000 m):

— ± 1 % před montáží,

— ± 2 % při montáži a pravidelné kontrole,

— ± 4 % v provozu.

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

3.2.2 *Měření rychlosti*

32) Záznamové zařízení musí měřit v rozsahu 0 až 220 km/h.

33) Aby byla zajištěna tolerance zobrazované rychlosti maximálně ± 6 km/h a byly vzaty v úvahu:

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

— tolerance ± 1 km/h při měřeních provedených při montáži nebo pravidelných kontrolách.

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

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

34) Rychlost se měří přesně s normální tolerancí během 2 sekund po ukončení změny rychlosti, jestliže změna proběhla při hodnotě 2 m/s^2.

35) Měření rychlosti se provádí s rozlišením 1 km/h nebo jemnějším.

3.2.3 *Měření polohy*

36) Záznamové zařízení měří absolutní polohu vozidla pomocí přijímače GNSS.

37) Absolutní poloha je měřena v zeměpisných souřadnicích šířky a délky ve stupních a minutách s rozlišením 1/10 minuty.

3.3 **Měření času**

38) Funkce měření času musí měřit nepřetržitě a udávat v digitální podobě údaje o koordinovaném světovém datu a času UTC.

39) K datování údajů v záznamovém zařízení (záznamy, výměna údajů) a pro všechny výtisky uvedené v dodatku 4 „Výtisky“ se musí používat datum a čas UTC.

40) Aby bylo možno zobrazit místní čas, musí se dát měnit posun zobrazovaného času s půlhodinovým krokem. Nejsou povoleny žádné jiné posuny než v záporných nebo kladných násobcích půl hodiny.

41) Nepoužívá-li se žádné nastavení času, nesmí zpožďování nebo zrychlování hodin překročit ± 2 sekundy za den v podmínkách schvalování typu.

42) Měření času musí mít rozlišovací schopnost vyšší nebo rovnou 1 sekundě.

43) Měření času nesmí být ovlivněno vypnutím vnějšího elektrického napájení na dobu kratší nežli 12 měsíců v podmínkách schvalování typu.

3.4 **Monitorování činností řidiče**

44) Tato funkce musí nepřetržitě a odděleně monitorovat činnosti jednoho řidiče a jednoho druhého řidiče.

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

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

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

48) Jestliže se vozidlo zastaví, musí se u řidiče automaticky nastavit režim PRÁCE.

49) První změna činnosti řidiče na režim 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).

50) Tato funkce předává informaci o změně činnosti s rozlišením jedné minuty.

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

52) Pokud jde o danou kalendářní minutu, která není podle požadavku 051 považována za JÍZDU, je celá minuta považována za stejný typ činnosti jako nejdéle nepřetržitě trvající činnost v této minutě (nebo poslední ze stejně dlouho trvajících činností).

53) Tato funkce musí také nepřetržitě monitorovat nepřetržitou dobu řízení a načítaný čas doby přestávek řidiče.

3.5 **Monitorování provozního stavu řidiče**

54) Tato funkce musí nepřetržitě a automaticky monitorovat provozní stav řidiče.

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

3.6 **Řidičem vkládané údaje**

3.6.1 *Vložení údajů o místě počátku a/nebo ukončení denní pracovní doby*

56) Tato funkce musí umožnit vložení údajů o místě, kde podle řidiče a/nebo druhého řidiče začíná a/nebo končí denní pracovní doba.

57) Místa jsou definována jako stát a případně region, které se zadávají nebo potvrzují ručně.

58) V době vyjmutí karty řidiče vyzve záznamové zařízení (druhého) řidiče, aby vložil údaj o místě ukončení denní pracovní doby.

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

60) Pomocí příkazů v nabídkách musí být možno zadávat místa, kde dochází k zahájení a/nebo ukončení denní pracovní doby řidiče. Pokud v průběhu jedné kalendářní minuty dojde k zadání více než jednoho takového údaje, zůstane zaznamenáno jen poslední místo zahájení práce a poslední místo ukončení práce provedené v dané době.

3.6.2 *Ruční vkládání údajů o činnostech řidiče a souhlas řidiče pro rozhraní ITS*

61) Při vložení karty řidiče (nebo karty dílny) a pouze v tomto okamžiku musí záznamové zařízení umožňovat ruční zadávání činností. Ruční zadávání činností se provádí za použití místního času a hodnot data podle daného časového pásma (posun oproti UTC) aktuálně nastaveného pro celek ve vozidle.

Při vložení karty řidiče nebo karty dílny přístroj držiteli karty připomene:

— datum a čas jeho posledního vyjmutí karty;

— volitelně: posun místního času oproti UTC momentálně nastavený pro celek ve vozidle.

Při prvním vložení karty řidiče nebo karty dílny, které celek ve vozidle aktuálně nezná, je držitel karty vyzván, aby vyjádřil souhlas s výstupem osobních údajů uložených v tachografu pomocí volitelného rozhraní ITS.

Souhlas řidiče (resp. dílny) lze kdykoli aktivovat nebo deaktivovat pomocí příkazů v menu, je-li vložena karta řidiče (resp. dílny).

Musí být možno zadávat činnosti s následujícími omezeními:

— typy činnosti jsou JÍZDA, POHOTOVOST nebo PŘESTÁVKA/ODPOČINEK;

— časy zahájení a ukončení každé činnosti musí spadat pouze do intervalu mezi posledním vyjmutím karty a jejím aktuálním vložením;

— není dovoleno, aby se jednotlivé činnosti navzájem časově překrývaly.

V případě potřeby musí být možno vkládat ruční záznamy při prvním vložení dříve nepoužívané karty řidiče (nebo dílny).

Postup ručního zadávání činností musí zahrnovat tolik po sobě jdoucích kroků, kolik je nezbytné k nastavení typu, času zahájení a času ukončení každé činnosti. U libovolné části doby mezi posledním vyjmutím karty a jejím aktuálním vložením musí mít držitel karty možnost neuvést žádnou činnost.

Při ručním zadávání údajů spojeném s vložením karty musí mít držitel karty v příslušných případech možnost zadat:

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

— místo zahájení aktuální denní pracovní doby spolu s příslušným časem.

Pokud držitel karty při ručním vkládání údajů spojeném s vložením karty nevloží žádné místo, kde zahájil nebo ukončil pracovní dobu, má se za to, že se jeho pracovní doba od posledního vyjmutí karty nezměnila. Další vložení údaje o místě, kde ukončil předchozí denní pracovní dobu, pak přepíše dočasné údaje vytvořené při posledním vyjmutí karty.

Pokud je zadáno nějaké místo, musí být zaznamenáno na příslušnou kartu tachografu.

Ruční zadávání se přeruší, jestliže:

— dojde k vyjmutí karty, nebo

— je vozidlo v pohybu a karta je v otvoru pro kartu řidiče.

Jsou povolena i další přerušení, například prodleva přístroje po určité době nečinnosti uživatele. V případě přerušení ručního zadávání údajů záznamové zařízení validuje veškeré již provedené úplné záznamy místa a činnosti (které mají zadáno buď jednoznačné místo a čas, nebo typ činnosti, čas zahájení a čas ukončení).

Pokud dojde k vložení karty druhého řidiče nebo karty dílny během ručního zadávání údajů pro dříve vloženou kartu, musí být možno ruční zadání údajů pro tuto předchozí kartu dokončit před zahájením ručního zadávání údajů pro druhou kartu.

Držitel karty musí mít možnost ručně zadávat údaje za použití následujícího minimálního postupu:

— ruční zadání činností v chronologickém pořadí za dobu mezi posledním vyjmutím karty a jejím aktuálním vložením,

— čas zahájení první činnosti se nastaví na čas vyjmutí karty. U každé následující zadané činnosti se čas zahájení předem nastaví na hodnotu, která bezprostředně následuje po času ukončení předchozí zadané činnosti. U každé činnosti se zvolí typ činnosti a čas ukončení.

Postup je ukončen v okamžiku, kdy se čas ukončení ručně vložené činnosti shoduje s časem vložení karty. Záznamové zařízení poté může případně povolit držiteli karty upravovat údaje kterékoli ručně zadané činnosti, a to až do okamžiku, kdy dojde k validaci zvolením zvláštního příkazu. Poté už budou jakékoli takové úpravy zakázány.

3.6.3 *Vkládání údajů o zvláštních podmínkách*

62) Záznamové zařízení musí řidiči umožnit vložit v reálném čase údaje o následujících dvou zvláštních podmínkách:

— „MIMO PŮSOBNOST“ (začátek, konec),

— „PŘEVOZ LODÍ / PŘEVOZ VLAKEM“ (začátek, konec).

K záznamu podmínky „PŘEVOZ LODÍ / PŘEVOZ VLAKEM“ nesmí dojít, pokud je otevřen záznam podmínky „MIMO PŮSOBNOST“.

Otevřený záznam podmínky „MIMO PŮSOBNOST“ musí být záznamovým zařízením automaticky uzavřen při vložení nebo vyjmutí karty řidiče.

Otevřený záznam podmínky „MIMO PŮSOBNOST“ musí deaktivovat následující události a varování:

— jízda bez příslušné karty,

— varování týkající se nepřetržité doby řízení.

Ukazatel začátku podmínky „PŘEVOZ LODÍ / PŘEVOZ VLAKEM“ musí být nastaven před tím, nežli se na lodi / ve vlaku vypne motor.

Otevřený záznam podmínky „PŘEVOZ LODÍ / PŘEVOZ VLAKEM“ musí skončit, nastane-li některá z následujících možností:

— řidič ručně ukončí „PŘEVOZ LODÍ / PŘEVOZ VLAKEM“,

— řidič vyjme svou kartu,

otevřený záznam podmínky „PŘEVOZ LODÍ / PŘEVOZ VLAKEM“ musí skončit, pokud již není platný na základě pravidel uvedených v nařízení (ES) č. 561/2006.

3.7 **Správa zámků podniků**

63) Tato funkce umožňuje správu zámků použitých podnikem k omezení přístupu k údajům v podnikovém režimu pouze na tento podnik.

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

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

66) Zámek může odemknout pouze podnik, jehož zámek je uzamčen (identifikováno prvními 13 znaky v čísle karty podniku), nebo

67) odemknutí se provede automaticky při uzamčení jiným podnikem.

68) V případě, že podnik provede uzamčení a předcházející uzamčení provedl týž podnik, předpokládá se, že předcházející uzamčení nebylo ukončeno a stále pokračuje.

3.8 **Monitorování kontrolních činností**

69) Tato funkce musí monitorovat činnosti ZOBRAZOVÁNÍ, TISKU, STAHOVÁNÍ ÚDAJŮ z celku ve vozidle nebo z karty a SILNIČNÍ KALIBRAČNÍ kontroly, které jsou prováděny v kontrolním režimu.

70) Tato funkce také monitoruje KONTROLU PŘEKROČENÍ POVOLENÉ RYCHLOSTI v kontrolním režimu. Činnost je považována za kontrolu překročení povolené rychlosti v případě, že v kontrolním režimu dojde k odeslání výtisku „překročení povolené rychlosti" do tiskárny nebo zobrazovací jednotky nebo jsou z datové paměti celku ve vozidle stahovány údaje „události a závady".

3.9 **Zjišťování událostí a/nebo závad**

71) Tato funkce identifikuje následující události a/nebo závady:

3.9.1 *„Vložení neplatné karty"*

72) Tato událost se vyvolá vložením neplatné karty, již nahrazené karty řidiče a/nebo karty s prošlým datem.

3.9.2 *„Rozpor karet"*

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

Rozpor karet		Otvor pro vložení karty řidiče				
		Bez karty	Karta řidiče	Kontrolní karta	Karta dílny	Karta podniku
Otvor pro vložení karty druhého řidiče	Bez karty					
	Karta řidiče				X	
	Kontrolní karta			X	X	X
	Karta dílny		X	X	X	X
	Karta podniku			X	X	X

3.9.3 *„Překrytí časových údajů"*

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

3.9.4 *„Jízda bez náležité karty“*

75) Tato událost nastane při jakékoliv z kombinací údajů platných karet tachografu označených v následující tabulce jako X, když se řidičova činnost mění na režim JÍZDA nebo nastane změna režimu provozu v době nastaveného režimu řidičovy činnosti JÍZDA:

Jízda bez příslušné karty,		Otvor pro vložení karty řidiče				
		Žádná (nebo neplatná) karta	Karta řidiče	Kontrolní karta	Karta dílny	Karta podniku
Otvor pro vložení karty druhého řidiče	Žádná (nebo neplatná) karta	X		X		X
	Karta řidiče	X		X	X	X
	Kontrolní karta	X	X	X	X	X
	Karta dílny	X	X	X		X
	Karta podniku	X	X	X	X	X

3.9.5 *„Vložení karty v průběhu jízdy“*

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

3.9.6 *„Nesprávné uzavření poslední relace karty“*

77) Tato událost nastane, jestliže při vložení karty záznamové zařízení zjistí, že přes opatření popsaná v bodě 3.1 předcházející vložení karty nebylo správným způsobem ukončeno (karta byla vyjmuta dříve, nežli na ni byly uloženy příslušné údaje). Tato událost nastane pouze při vložení karty řidiče nebo karty dílny.

3.9.7 *„Překročení povolené rychlosti“*

78) Tato událost nastane při každém překročení povolené rychlosti.

3.9.8 *„Přerušení elektrického napájení“*

79) Tato událost nastane při každém přerušení elektrického napájení snímače pohybu a/nebo celku ve vozidle delším nežli 200 milisekund, pokud zařízení není v kalibračním nebo kontrolním režimu. Prahovou hodnotu přerušení definuje výrobce. Pokles elektrického napájení v důsledku startování motoru vozidla nesmí vyvolat tuto událost.

3.9.9 *„Chyba komunikace se zařízením pro dálkovou komunikaci“*

80) Tato událost nastane, **není-li zařízení v kalibračním režimu** a nepotvrdí-li zařízení pro dálkovou komunikaci úspěšné přijetí údajů dálkové komunikace odeslaných z celku ve vozidle po více než třech pokusech.

3.9.10 *„Chybějící informace o poloze z přijímače GNSS“*

81) Tato událost nastane, **není-li zařízení v kalibračním režimu** a chybějí-li po dobu delší než 3 hodiny z celkové doby řízení informace o poloze pocházející z přijímače GNSS (vnitřního nebo vnějšího).

3.9.11 *„Chyba komunikace s vnějším zařízením GNSS“*

82) Tato událost nastane, **není-li zařízení v kalibračním režimu** a je-li po souvislou dobu delší než 20 minut přerušena komunikace mezi vnějším zařízením GNSS a celkem ve vozidle, je-li vozidlo v pohybu.

3.9.12 *„Chybné údaje o pohybu vozidla“*

83) Tato událost nastane, **není-li zařízení v kalibračním režimu**, v případě přerušení normálního toku dat mezi snímačem pohybu a celkem ve vozidle a/nebo v případě chyby v integritě nebo pravosti údajů přenášených mezi snímačem pohybu a celkem ve vozidle.

3.9.13 *„Nesoulad údajů o pohybu vozidla“*

84) Tato událost nastane, **není-li zařízení v kalibračním režimu**, v případě, že informace o pohybu vypočtené ze snímače pohybu jsou v rozporu s informacemi o pohybu vypočtenými z vnitřního přijímače GNSS nebo z vnějšího zařízení GNSS a volitelně z jiných nezávislých zdrojů údajů podle specifikace v dodatku 12. Tato událost nenastane během převozu lodí / převozu vlakem, za podmínky MIMO PŮSOBNOST, nebo nejsou-li k dispozici informace o poloze z přijímače GNSS.

3.9.14 *„Pokus o narušení bezpečnosti systému“*

85) Tato událost nastane v jakémkoliv jiném případě, který ohrožuje bezpečnost systému snímače pohybu a/nebo celku ve vozidle a/nebo vnějšího zařízení GNSS podle požadavků v dodatku 10, pokud není zařízení v kalibračním režimu.

3.9.15 *„Nesoulad času“*

86) Tato událost nastane, **není-li zařízení v kalibračním režimu**, pokud celek ve vozidle zjistí nesoulad větší než 1 minuta mezi časem funkce měření času celku ve vozidle a časem pocházejícím z přijímače GNSS. 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 během posledních 30 dnů nezjistil žádný platný signál GNSS. Jakmile jsou však informace o poloze z přijímače GNSS opět k dispozici, je provedeno automatické nastavení času.

3.9.16 *„Chyba karty“*

87) Tato závada nastane, když je v průběhu provozu zjištěna vada karty tachografu.

3.9.17 *„Chyba záznamového zařízení“*

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

— vnitřní závada celku ve vozidle

— závada tiskárny

— závada zobrazovací jednotky

— závada stahování

— závada snímače

— závada přijímače GNSS nebo vnějšího zařízení GNSS

— závada zařízení pro dálkovou komunikaci

3.10 **Integrované zkoušky a autotesty**

89) Záznamové zařízení musí samo zjistit vlastní závady v průběhu integrovaných zkoušek a autotestů v souladu s touto tabulkou:

Testovaný subsystém	Autotest	Integrovaná zkouška
Programové vybavení		Integrita
Datová paměť	Přístup	Přístup, integrita údajů
Čtecí zařízení karet	Přístup	Přístup
Klávesnice		Ruční kontrola
Tiskárna	(podle výrobce)	Výtisk
Zobrazování		Vizuální kontrola
Stahování údajů (prováděno pouze v průběhu stahování)	Správná funkce	
Snímač	Správná funkce	Správná funkce
Zařízení pro dálkovou komunikaci	Správná funkce	Správná funkce
Zařízení GNSS	Správná funkce	Správná funkce

3.11 **Načítání z datové paměti**

90) Záznamové zařízení musí být schopno načíst jakékoliv údaje uložené v jeho datové paměti.

3.12 **Zaznamenávání a ukládání do datové paměti**

Pro účely tohoto odstavce

— se „365 dny“ rozumí 365 kalendářních dnů průměrné činnosti řidiče ve vozidle. Průměrná činnost v průběhu dne ve vozidle se definuje jako nejméně 6 řidičů nebo druhých řidičů, 6 cyklů vložení a vyjmutí karty a 256 změn činnosti. „365 dnů“ tedy obsahuje minimálně 2 190 (druhých) řidičů, 2 190 cyklů vložení a vyjmutí karty a 93 440 změn činnosti,

— se průměrným počtem poloh za den rozumí nejméně 6 poloh, ve kterých začíná denní pracovní doba, 6 poloh, kdy nepřetržitá doba řízení řidiče dosáhne násobku tří hodin, a 6 poloh, ve kterých končí denní pracovní doba, takže „365 dnů“ obsahuje minimálně 6 570 poloh,

— časové údaje jsou zaznamenávány s rozlišovací schopností jedné minuty, pokud není stanoveno jinak,

— stav počitadla ujetých kilometrů se zaznamenává s rozlišovací schopností jednoho kilometru,

— údaje o rychlosti jsou zaznamenávány s rozlišovací schopností 1 km/h,

— polohy (zeměpisné šířky a délky) jsou zaznamenávány ve stupních a minutách, s rozlišením 1/10 minuty, s příslušnou přesností GNSS a dobou zjištění.

91) Údaje uložené do datové paměti nesmějí být ovlivněny přerušením elektrického napájení z vnějšího zdroje v rozsahu kratším nežli dvanáct měsíců v podmínkách schvalování typu. Údaje uložené ve vnějším zařízení pro dálkovou komunikaci podle dodatku 14 navíc nesmějí být ovlivněny přerušením elektrického napájení v rozsahu kratším nežli 28 dnů.

92) Záznamové zařízení musí být schopno zaznamenávat a implicitně nebo explicitně ukládat do své datové paměti následující údaje:

3.12.1 *Údaje identifikující zařízení*

3.12.1.1 Identifikační údaje o celku ve vozidle

93) Záznamové zařízení musí být schopno ukládat do své datové paměti tyto identifikační údaje o celku ve vozidle:

— jméno výrobce,

— adresa výrobce,

— číslo součásti,

— výrobní číslo,

— generace celku ve vozidle,

— schopnost používat karty tachografu první generace,

— číslo verze programového vybavení,

— datum instalace aktuální verze programového vybavení,

— rok výroby zařízení,

— číslo schválení.

94) Identifikační údaje o celku ve vozidle jsou zaznamenány a uloženy jednou provždy výrobcem celku ve vozidle, s výjimkou údajů vztahujících se k programovému vybavení a čísla schválení, které se může měnit v případě aktualizace programového vybavení, a schopnosti používat karty tachografu první generace.

3.12.1.2 Identifikační údaje snímače pohybu

95) Snímač pohybu musí být schopen uložit do své datové paměti tyto identifikační údaje:

— jméno výrobce,

— výrobní číslo,

— číslo schválení,

— identifikátor vloženého bezpečnostního komponentu (např. číslo součásti vnitřního čipu / číslo procesoru),

— identifikátor operačního systému (např. číslo verze programového vybavení).

96) Identifikační údaje snímače pohybu jsou zaznamenány a uloženy výrobcem tohoto snímače jednou provždy do snímače.

97) Celek ve vozidle musí být schopen zaznamenat a uložit do své datové paměti následující údaje vztahující se k 20 posledním párování snímačů pohybu (dojde-li k několika párováním během jednoho kalendářního dne, uloží se pouze první a poslední z nich):

Pro každé z těchto párování se uloží tyto údaje:

— identifikační údaje snímače pohybu,

— výrobní číslo,

— číslo schválení,

— párovací údaje snímače pohybu:

— datum párování.

3.12.1.3 Identifikační údaje globálních navigačních družicových systémů

98) Vnější zařízení GNSS musí být schopno uložit do své datové paměti tyto identifikační údaje:

— jméno výrobce,

— výrobní číslo,

— číslo schválení,

— identifikátor vloženého bezpečnostního komponentu (např. číslo součásti vnitřního čipu / číslo procesoru),

— identifikátor operačního systému (např. číslo verze programového vybavení).

99) Identifikační údaje jsou zaznamenány a uloženy výrobcem vnějšího zařízení GNSS jednou provždy do tohoto zařízení.

100) Celek ve vozidle musí být schopen zaznamenat a uložit do své datové paměti následující údaje vztahující se k posledním 20 párování s vnějšími zařízeními GNSS (pokud během jednoho kalendářního dne dojde k několika párováním, uloží se jenom první a poslední z nich).

Pro každé z těchto párování se uloží tyto údaje:

— identifikační údaje vnějšího zařízení GNSS:

— výrobní číslo,

— číslo schválení,

— párovací údaje vnějšího zařízení GNSS:

— datum spárování.

3.12.2 *Klíče a certifikáty*

101) Záznamové zařízení musí být schopno uložit řadu kryptografických klíčů a certifikátů podle specifikace v dodatku 11 části A a části B.

3.12.3 *Data související s vložením a vyjmutím karty řidiče nebo dílny*

102) Při každém cyklu vložení a vyjmutí karty řidiče nebo karty dílny musí záznamové zařízení zaznamenat a uložit do své datové paměti tyto informace:

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

— číslo karty, členský stát vydávající kartu a datum platnosti v podobě uložené na kartě,

— generaci karty,

— datum a čas vložení karty,

— stav počitadla ujetých kilometrů při vložení karty,

— otvor pro vkládání karet, do kterého byla tato karta vložena,

— datum a čas vyjmutí karty,

— stav počitadla ujetých kilometrů při vyjmutí karty,

— následující informace o posledním řidičem použitém vozidle tak, jak jsou uloženy na kartě:

— registrační značku vozidla a členský stát registrace,

— generaci celku ve vozidle (je-li k dispozici),

— datum a čas vyjmutí karty,

— značku informující, zda držitel karty při vložení karty vložil ručně údaje o činnosti, nebo ne.

103) Datová paměť musí být schopna uchovat tato data nejméně po dobu 365 dnů.

104) Jestliže je kapacita datové paměti vyčerpána, musí nové údaje nahradit nejstarší údaje.

3.12.4 *Údaje o činnostech řidiče*

105) Záznamové zařízení musí provést záznam a uložení do své datové paměti, kdykoliv dojde ke změně činnosti u řidiče a/nebo druhého řidiče a/nebo dojde ke změně provozního stavu řidiče a/nebo je vsunuta nebo vyjmuta karta řidiče nebo karta dílny:

— provozní stav řidiče (POSÁDKA, SAMOTNÝ ŘIDIČ),

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

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

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

— datum a čas změny.

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

Údaje o činnosti vložené ručně řidičem nejsou zaznamenávány do datové paměti.

106) Datová paměť musí být schopna uchovat údaje o činnostech řidiče nejméně po dobu 365 dnů.

107) Jestliže je kapacita datové paměti vyčerpána, musí nové údaje nahradit nejstarší údaje.

3.12.5 *Místa a polohy, kde začíná nebo končí denní pracovní doba a/nebo kde je dosaženo tří hodin nepřetržité 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,

— poloh, kde nepřetržitá doba řízení řidiče dosáhne násobku tří hodin;

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

109) Není-li v těchto časech z přijímače GNSS k dispozici poloha vozidla, záznamové zařízení použije poslední dostupnou polohu a příslušné datum a čas.

110) Společně s příslušným místem nebo polohou musí záznamové zařízení zaznamenat a uložit do své datové paměti:

— číslo karty (druhého) řidiče a členský stát, který vydal kartu,

— generaci karty,

— datum a čas vložení údajů,

— typ vložených údajů (začátek a konec nebo tři hodiny nepřetržité doby řízení),

— příslušnou přesnost GNSS, v příslušných případech datum a čas,

— stav počitadla ujetých kilometrů.

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 nepřetržité doby řízení, minimálně po dobu 365 dnů.

112) Jestliže je kapacita datové paměti vyčerpána, musí nové údaje nahradit nejstarší údaje.

3.12.6 *Údaje počitadla ujetých kilometrů*

113) Záznamové zařízení musí zaznamenávat do své datové paměti stav počitadla ujetých kilometrů vozidla a odpovídající datum o půlnoci každého kalendářního dne.

114) Datová paměť musí být schopna ukládat stav počitadla ujetých kilometrů o půlnoci nejméně po dobu 365 kalendářních dnů.

115) Jestliže je kapacita datové paměti vyčerpána, musí nové údaje nahradit nejstarší údaje.

3.12.7 *Podrobné údaje o rychlosti*

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.

3.12.8 *Údaje o událostech*

Pro účely tohoto bodu musí být čas zaznamenáván s přesností jedné sekundy.

117) Záznamové zařízení musí zaznamenávat a uchovávat ve své datové paměti tyto údaje o každé zjištěné události podle následujících pravidel ukládání:

Událost	Pravidla ukládání	Údaje, které se ukládají pro každou událost
Vložení neplatné karty	— deset posledních událostí	— datum a čas události — typ, číslo, vydávající členský stát a generace karty (karet) vytvářející(ch) událost — počet podobných událostí v tentýž den
Rozpor karet	— deset posledních událostí	— datum a čas začátku události — datum a čas konce události — typ, číslo, vydávající členský stát a generace dvou karet vytvářejících konflikt
Jízda bez příslušné karty,	— 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

Událost	Pravidla ukládání	Údaje, které se ukládají pro každou událost
Vložení karty během řízení	— poslední událost v každém z posledních deseti dnů výskytu	— datum a čas události — typ, číslo, vydávající členský stát a generace karty (karet) — počet podobných událostí v tentýž den
Nesprávné uzavření poslední relace karty	— deset posledních událostí	— datum a čas vložení karty — typ, číslo, vydávající členský stát a generace karty (karet) — poslední data relace přečtená z karty: — datum a čas vložení karty — VRN, členský stát registrace a generace VU
Překročení povolené rychlosti (1)	— nejzávažnější událost v každém z deseti posledních dnů výskytu (tj. případ s nejvyšší průměrnou rychlostí) — pět nejzávažnějších událostí za posledních 365 dnů — první událost, která nastala po poslední kalibraci	— datum a čas začátku události — datum a čas konce události — maximální rychlost změřená v průběhu události — aritmetický průměr rychlostí změřených v průběhu události — typ, číslo, vydávající členský stát a generace karty řidiče (v příslušných případech) — počet podobných událostí v tentýž den
Přerušení napájení (2)	— 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
Chyba komunikace se zařízením pro dálkovou komunikaci	— 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
Chybí informace o poloze z přijímače 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

Událost	Pravidla ukládání	Údaje, které se ukládají pro každou událost
Chyba údajů o pohybu vozidla	— 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
Nesoulad údajů o pohybu vozidla	— 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
Pokus o narušení zabezpečení	— posledních deset událostí pro každý typ události	— datum a čas začátku události — datum a čas konce události (je-li relevantní) — typ, číslo, vydávající členský stát a generace všech karet vložených na začátku a/nebo na konci události — typ události
Časový konflikt	— nejdelší událost v každém z posledních deseti dnů výskytu — pět nejdelších 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

(1) Záznamové zařízení musí také zaznamenat a uchovat ve své datové paměti:

— datum a čas poslední KONTROLY PŘEKROČENÍ POVOLENÉ RYCHLOSTI,

— datum a čas prvního překročení povolené rychlosti následujícího po této KONTROLE PŘEKROČENÍ POVOLENÉ RYCHLOSTI,

— počet událostí, při kterých došlo k překročení povolené rychlosti od poslední KONTROLY PŘEKROČENÍ POVOLENÉ RYCHLOSTI.

(2) Tyto údaje mohou být zaznamenávány pouze při opětovném připojení elektrického napájení, časové údaje mohou být udávány s přesností jedné minuty.

3.12.9 *Údaje o závadách*

Pro účely tohoto bodu musí být čas zaznamenáván s přesností jedné sekundy.

118) Záznamové zařízení se musí pokusit zaznamenat a uložit tato data pro každou zjištěnou závadu do své datové paměti podle následujících pravidel o ukládání dat:

Závada	Pravidla ukládání	Údaje, které se ukládají při závadě
Chyba karty	— deset posledních závad karty řidiče	— datum a čas začátku závady — datum a čas konce závady — typ, číslo, vydávající členský stát a generace karty (karet)
Závady záznamového zařízení	— deset posledních závad pro každý typ závady — první závada po poslední kalibraci	— datum a čas začátku závady — datum a čas konce závady — typ závady — typ, číslo, vydávající členský stát a generace všech karet vložených na začátku a/nebo konci závady

3.12.10 *Kalibrační údaje*

119) Záznamové zařízení musí zaznamenávat a ukládat do své datové paměti údaje týkající se:

— známých kalibračních parametrů v okamžiku aktivace,

— jeho první kalibrace po aktivaci,

— jeho první kalibrace v současném vozidle (identifikovaném jeho identifikačním číslem vozidla),

— posledních dvaceti kalibrací (jestliže proběhne několik kalibrací v průběhu jednoho kalendářního dne, je zaznamenána pouze první a poslední kalibrace).

120) Následující údaje se zaznamenávají pro každou z těchto kalibrací:

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

— název a adresa dílny,

— číslo karty dílny, členský stát vydávající kartu a datum ukončení použitelnosti karty,

— identifikace vozidla,

— aktualizované nebo potvrzené parametry: w, k, l, rozměr pneumatik, nastavení zařízení omezujícího rychlost vozidla, počitadlo ujetých kilometrů (stará a nová hodnota), datum a čas (stará a nová hodnota),

— typy a identifikátory všech použitých plomb.

121) Záznamové zařízení musí navíc zaznamenávat a uchovávat ve své datové paměti schopnost používat karty tachografu první generace (dosud aktivované, či nikoli).

122) Snímač pohybu musí zaznamenávat a uchovávat ve své datové paměti tyto montážní údaje snímače pohybu:

— první spárování s celkem ve vozidle (datum, čas, číslo schválení celku ve vozidle, výrobní číslo celku ve vozidle),

— poslední spárování s celkem ve vozidle (datum, čas, číslo schválení celku ve vozidle, výrobní číslo celku ve vozidle).

123) Vnější zařízení GNSS musí zaznamenávat a uchovávat ve své datové paměti tyto montážní údaje vnějšího zařízení GNSS:

— první spárování s celkem ve vozidle (datum, čas, číslo schválení celku ve vozidle, výrobní číslo celku ve vozidle),

— poslední spárování s celkem ve vozidle (datum, čas, číslo schválení celku ve vozidle, výrobní číslo celku ve vozidle).

3.12.11 *Údaje o nastavení času*

124) Záznamové zařízení musí zaznamenávat a uchovávat ve své datové paměti údaje vztahující se k nastavením času provedeným v kalibračním režimu mimo rámec pravidelné kalibrace (def. f)):

— času posledního nastavení času,

— pěti největším nastavením času.

125) Tyto údaje musí být zaznamenávány pro každé z těchto nastavení času:

— datum a čas, stará hodnota,

— datu a čas, nová hodnota,

— název a adresa dílny,

— číslo karty dílny, členský stát vydávající kartu, generace karty a datum ukončení použitelnosti karty.

3.12.12 *Údaje o kontrolních činnostech*

126) Záznamové zařízení musí zaznamenávat a uchovávat ve své datové paměti tyto údaje týkající se posledních dvaceti případů kontrolní činnosti:

— datum a čas kontroly,

— číslo kontrolní karty, členský stát vydávající kartu a generaci karty,

— druh kontroly (zobrazení a/nebo tisk a/nebo stahování z celku ve vozidle a/nebo stahování z karty a/nebo silniční kalibrační kontrola),

127) V případě stahování údajů jsou také zaznamenávány údaje o nejstarším a o posledním dni stahování údajů.

3.12.13 *Údaje o zámcích podniků*

128) Záznamové zařízení musí zaznamenávat a uchovávat ve své datové paměti tyto údaje týkající se 255 posledních případů použití zámků podniků:

— datum a čas uzamčení,

— datum a čas odemknutí,

— číslo karty podniku, členský stát, který kartu vydal, a generaci karty,

— název a adresu podniku.

Údaje, které byly dříve uzamčeny zámkem odstraněným z paměti v důsledku výše uvedeného limitu, se považují za neuzamčené.

3.12.14 *Údaje o stahování*

129) Záznamové zařízení musí zaznamenávat a uchovávat ve své datové paměti tyto údaje týkající se posledního stahování dat z datové paměti do vnějšího média v podnikovém nebo kalibračním režimu:

— datum a čas stahování dat,

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

— název podniku nebo dílny.

3.12.15 *Údaje o zvláštních podmínkách*

130) Záznamové zařízení musí zaznamenávat ve své datové paměti tyto údaje týkající se zvláštních podmínek:

— datum a čas záznamu,

— druh zvláštní podmínky.

131) Datová paměť musí být schopna uchovat zvláštní podmínky po dobu nejméně 365 dnů (za předpokladu, že průměrně jedna podmínka je otevřena a uzavřena během jednoho dne). Jestliže je kapacita paměti vyčerpána, musí nové údaje nahradit nejstarší údaje.

3.12.16 *Údaje o kartě tachografu*

132) Záznamové zařízení musí být schopno uchovávat tyto údaje týkající se různých karet tachografu, které byly použity v celku ve vozidle:

— číslo karty tachografu a její výrobní číslo,

— výrobce karty tachografu,

— typ karty tachografu,

— verzi karty tachografu.

133) Záznamové zařízení musí být schopno uchovávat minimálně 88 takových záznamů.

3.13 **Čtení z karet tachografu**

134) Záznamové zařízení musí být schopno, pokud je třeba, přečíst z karet tachografu první a druhé generace údaje nezbytné k(e):

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

— kontrole správného uzavření poslední relace karty,

— výpočtu nepřetržité doby řízení řidiče, souhrnné doby přestávek a souhrnné doby řízení v předchozím a probíhajícím týdnu,

— vytištění požadovaných dat zaznamenaných na kartě řidiče,

— stažení dat z karty řidiče na externí média.

Tento požadavek platí pouze pro karty tachografu první generace, pokud dílna nezablokuje jejich používání.

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

3.14 **Zaznamenávání a ukládání údajů na kartách tachografu**

3.14.1 *Zaznamenávání a ukládání údajů na kartách tachografu první generace*

136) Pokud dílna nezablokovala použití karet tachografu první generace, musí záznamové zařízení zaznamenávat a uchovávat údaje naprosto stejným způsobem jako záznamové zařízení první generace.

137) Záznamové zařízení musí v kartě řidiče nebo kartě dílny nastavit režim „údaje o použití karty“ okamžitě po vložení karty.

138) Záznamové zařízení musí aktualizovat údaje uložené na platných kartách řidiče, kartách dílny, kartách podniku a/nebo kontrolních kartách se všemi nezbytnými údaji vztahujícími se k době, kdy byla karta vložena, a k držiteli karty. Údaje uložené na kartách jsou specifikovány v kapitole 4.

139) Záznamové zařízení musí aktualizovat údaje o činnostech řidiče a místech (podle specifikace v bodech 4.5.3.1.9 a 4.5.3.1.11), které jsou uloženy na platných kartách řidiče a/nebo kartách dílny, s údaji týkajícími se činností řidiče a míst, které byly vloženy ručně držitelem karty.

140) Všechny události, které nejsou definovány pro záznamové zařízení první generace, se na karty řidiče a karty dílny neukládají.

141) Údaje uložené na kartách tachografu jsou aktualizovány takovým způsobem a v takovou dobu, jak je třeba s ohledem na momentální kapacitu datové paměti a nahrazení nejstarších uložených údajů posledními údaji.

142) V případě chybného zápisu se záznamové zařízení maximálně třikrát pokusí vyplnit daný příkaz k zápisu a potom v případě neúspěchu vyznačí chybu karty a její neplatnost.

143) Před uvolněním karty řidiče a po uložení všech příslušných údajů, které se měly na kartu uložit, nastaví záznamové zařízení znovu „údaje o použití karty (*card session data*)“.

3.14.2 *Zaznamenávání a ukládání údajů na kartách tachografu druhé generace*

144) Karty tachografu druhé generace musí obsahovat dvě různé aplikace karet, z nichž první je přesně stejná jako aplikace TACHO karet tachografu první generace a druhá je aplikace „TACHO_G2“ podle specifikace v kapitole 4 a dodatku 2.

145) Záznamové zařízení musí v kartě řidiče nebo kartě dílny nastavit režim „údaje o použití karty“ okamžitě po vložení karty.

146) Záznamové zařízení musí aktualizovat údaje uložené na dvou aplikacích platných karet řidiče, karet dílny, karet podniku a/nebo kontrolních karet se všemi nezbytnými údaji vztahujícími se k době, kdy byla karta vložena, a k držiteli karty. Údaje uložené na těchto kartách jsou specifikovány v kapitole 4.

147) Záznamové zařízení musí aktualizovat údaje o činnostech řidiče, místech a polohách (podle specifikace v bodech 4.5.3.1.9, 4.5.3.1.11, 4.5.3.2.9 a 4.5.3.2.11), které jsou uloženy na platných kartách řidiče a/nebo kartách dílny, s údaji týkajícími se činností řidiče a míst, které byly ručně vloženy držitelem karty.

148) Údaje uložené na kartách tachografu jsou aktualizovány takovým způsobem a v takovou dobu, jak je třeba s ohledem na momentální kapacitu datové paměti a nahrazení nejstarších uložených údajů posledními údaji.

149) V případě chybného zápisu se záznamové zařízení maximálně třikrát pokusí vyplnit daný příkaz k zápisu a potom v případě neúspěchu vyznačí chybu karty a její neplatnost.

150) Před uvolněním karty řidiče a po uložení všech příslušných údajů na dvou aplikacích karty nastaví záznamové zařízení znovu „údaje o použití karty“.

3.15 **Zobrazení**

151) Displej musí mít minimálně 20 znaků.

152) Minimální velikost znaků musí být 5 mm na výšku a 3,5 mm na šířku.

153) Zobrazovací jednotka musí podporovat znaky uvedené v dodatku 1 kapitole 4 „Znakové sady". Zobrazovací jednotka může používat zjednodušené znaky (např. znaky s diakritikou mohou být zobrazeny bez diakritiky nebo malá písmena mohou být zobrazena jako velká).

154) Zobrazovací jednotka musí vydávat přiměřené, neoslňující světlo.

155) Údaje záznamového zařízení musí být dobře viditelné.

156) Záznamové zařízení musí být schopno zobrazit:

— implicitní údaje,

— údaje vztahující se k výstražným sdělením,

— údaje vztahující se k přístupovému menu,

— ostatní údaje požadované uživatelem.

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

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

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

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

Formát zobrazení je uveden v dodatku 5.

3.15.1 *Výchozí zobrazení*

160) Pokud není třeba zobrazit žádnou jinou informaci, musí záznamové zařízení standardně zobrazovat tyto údaje:

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

— provozní režim,

— aktuální činnost řidiče a aktuální činnost druhého řidiče,

— informace vztahující se k řidiči:

— jeho současná nepřetržitá doba řízení a jeho současná souhrnná doba přestávek, pokud je jeho aktuální činností JÍZDA,

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

161) Zobrazení údajů vztahujících se ke každému řidiči musí být jasné, jednoduché a jednoznačné. V případě, že informace o řidiči i druhém řidiči nemohou být zobrazeny současně, musí záznamové zařízení implicitně ukazovat informaci týkající se řidiče a musí umožnit uživateli zobrazit informaci týkající se druhého řidiče.

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

163) Záznamové zařízení musí při vložení karty krátce zobrazit jméno držitele karty.

164) Jestliže je otevřena podmínka „MIMO PŮSOBNOST“ nebo „PŘEVOZ LODÍ/PŘEVOZ VLAKEM“, potom musí displej ukázat odpovídající piktogram, že příslušná podmínka je otevřena (je povoleno, aby zároveň nebyla zobrazena informace o současné činnosti řidiče).

3.15.2 *Varovné zobrazení*

165) Záznamové zařízení musí zobrazit výstražné sdělení primárně použitím piktogramů podle dodatku 3, doplněné v případě potřeby dodatečnými numericky kódovanými informacemi. Přesné popisy výstražných sdělení mohou být také zobrazeny v preferovaném jazyce řidiče.

3.15.3 *Přístupové menu*

166) Záznamové zařízení musí nabídnout nezbytné příkazy prostřednictvím odpovídající struktury menu.

3.15.4 *Další zobrazení*

167) Musí být možné na vyžádání selektivně zobrazit:

— datum a čas UTC a posun místního času,

— obsah kteréhokoli ze šesti výtisků v témže formátu, jaký mají samotné výtisky,

— nepřetržitou dobu řízení a souhrnnou dobu přestávek řidiče,

— nepřetržitou dobu řízení a souhrnnou dobu přestávek druhého řidiče,

— souhrnnou dobu řízení řidiče v předchozím a probíhajícím týdnu,

— souhrnnou dobu jízdy druhého řidiče v předchozím a probíhajícím týdnu,

volitelně:

— současné trvání činnosti druhého řidiče (od doby, kdy byla navolena),

— souhrnnou dobu řízení řidiče v probíhajícím týdnu,

— souhrnnou dobu řízení druhého řidiče v probíhající denní pracovní době,

— souhrnnou dobu řízení řidiče v probíhající denní pracovní době.

168) Zobrazování obsahu výtisku musí probíhat sekvenčně, řádek po řádce. Jestliže je šířka displeje menší nežli 24 znaků, musí být uživateli nabídnuta úplná informace vhodným způsobem (několik řádek, rolování…).

Řádky výtisku věnované ručně napsaným informacím mohou být ze zobrazení vypuštěny.

3.16 **Tisk**

169) Záznamové zařízení musí být schopno vytisknout údaje z vlastní datové paměti a/nebo karet tachografu v podobě následujících sedmi výtisků:

— denní výtisk činnosti řidiče z karty,

— denní výtisk činnosti řidiče z celku ve vozidle,

— výtisk událostí a závad z karty,

— výtisk událostí a závad z celku ve vozidle,

— výtisk technických údajů,

— výtisk překročení povolené rychlosti.

— historie údajů karty tachografu pro daný celek ve vozidle (viz kapitola 3.12.16).

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

Dodatečné údaje mohou být přidány na konci těchto výtisků.

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

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

171) Aby se vytiskl záznam „denní výtisk činnosti řidiče z karty“ nebo „výtisk událostí a závad z karty“, musí záznamové zařízení:

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

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

172) Tiskárna musí být schopna vytisknout 24 znaků na řádku.

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

174) Tiskárna musí podporovat znaky uvedené v dodatku 1 kapitole 4 „Znakové sady“.

175) Tiskárny musí být navrženy tak, aby se při tisku výtisků s dostatečnou pravděpodobností vyhnuly jakékoliv nejednoznačnosti při čtení.

176) Výtisky si musí podržet své rozměry a záznamy za normálních podmínek vlhkosti (10 až 90 %) a teploty.

177) Typově schválený papír používaný v záznamovém zařízení musí nést příslušnou značku schválení typu a označení typu(ů) záznamových zařízení, ve kterých jej lze používat.

178) Za normálních podmínek skladování, co se týče intenzity osvětlení, vlhkosti a teploty, musí výtisky zůstat dobře čitelné nejméně po dobu dvou let.

179) Výtisky musí splňovat alespoň požadavky na zkoušky definované v dodatku 9.

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

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

3.17 **Výstražná sdělení**

182) Záznamové zařízení musí upozornit řidiče při zjištění jakékoliv události a/nebo závady.

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

184) Záznamové zařízení musí řidiče upozornit 15 minut před uplynutím maximální povolené nepřetržité doby řízení a při jejím překročení.

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

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

187) Vizuální výstrahy mohou být zabudovány v záznamovém zařízení a/nebo umístěny mimo záznamové zařízení.

188) Ve druhém případě musí nést symbol „T“.

189) Výstražná sdělení musí trvat nejméně 30 sekund, pokud není uživatelem potvrzeno, že je bere na vědomí stiskem jednoho nebo více speciálních ovládacích prvků záznamového zařízení. První potvrzení nesmí smazat zobrazení příčiny výstražného sdělení v souladu s následujícím odstavcem.

190) Příčina výstrahy musí být zobrazena na záznamovém zařízení a zůstat viditelná, dokud není uživatelem potvrzeno, že ji bere na vědomí, použitím specifického ovladače nebo vložením příkazu záznamového zařízení.

191) Další výstražná sdělení mohou být také použita, pokud nebudou mást řidiče ve vztahu ke sdělením výše popsaným.

3.18 Stahování údajů do externích médií

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

193) Kromě toho jako přídavná funkce mohou být údaje stahovány v jakémkoli provozním režimu jiným způsobem pro podnik, který se ověří tímto kanálem. V tomto případě se při stahování využijí přístupová práva podniku pro stahování údajů.

194) Stahování údajů nesmí změnit nebo odstranit žádné uložené údaje.

195) Elektrické rozhraní spojovacího konektoru pro kalibraci nebo stahování údajů je popsáno v dodatku 6.

196) Protokoly pro stahování údajů jsou uvedeny v dodatku 7.

3.19 Dálková komunikace pro cílené silniční kontroly

197) Při zapnutém zapalování musí celek ve vozidle ukládat každých 60 sekund do zařízení pro dálkovou komunikaci nejnovější údaje potřebné pro účely cílených silničních kontrol. Tyto údaje musí být šifrovány a podepsány podle specifikace v dodatcích 11 a 14.

198) Dálkově kontrolované údaje musí být dostupné snímačům dálkové komunikace prostřednictvím bezdrátové komunikace podle specifikace v dodatku 14.

199) Údaje potřebné pro účely cílených silničních kontrol zahrnují:

— poslední pokus o narušení zabezpečení,

— nejdelší přerušení dodávky energie,

— poruchu snímače,

— chybu v údajích o pohybu vozidla,

— nesoulad údajů o pohybu vozidla,

— jízdu bez platné karty,

— vložení karty během řízení,

— údaje o úpravě času,

— kalibrační údaje, včetně údajů dvou posledních uložených kalibračních záznamů,

— registrační značku vozidla,

— rychlost zaznamenanou tachografem.

3.20 **Výstupní údaje pro přídavná externí zařízení**

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, pokud zcela odpovídají požadavkům dodatku 13 z hlediska minimálního výčtu údajů, zabezpečení a souhlasu řidiče.

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 ostatní externí zařízení informovat o souhlasu řidiče.

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

201) Sériové rozhraní podle specifikace v příloze 1B nařízení (EHS) č. 3821/85 v platném znění může být nadále používáno pro zpětnou slučitelnost tachografů. V případě přenášení osobních údajů je však stále nezbytný souhlas řidiče.

3.21 **Kalibrace**

202) Kalibrační funkce musí umožnit:

— automatické spárování snímače pohybu a celku ve vozidle,

— v příslušných případech automatickou vazbu vnějšího zařízení GNSS a celku ve vozidle,

— digitální přizpůsobení konstanty záznamového zařízení (k) charakteristickému koeficientu vozidla (w),

— nastavení aktuálního času v době platnosti vložené karty dílny,

— nastavit současnou hodnotu počitadla ujetých kilometrů,

— aktualizovat identifikační data snímače pohybu uložená v datové paměti,

— v příslušných případech aktualizaci identifikačních údajů vnějšího zařízení GNSS uložených v datové paměti,

— aktualizaci typů a identifikátorů všech použitých plomb,

— aktualizaci nebo potvrzení dalších parametrů známých záznamovému zařízení: identifikaci vozidla, w, l, rozměr pneumatik a v příslušných případech nastavení omezovače rychlosti.

203) Kalibrační funkce musí navíc umožňovat zablokovat používání karet tachografu první generace v záznamovém zařízení, jsou-li splněny podmínky uvedené v dodatku 15.

204) Párování snímače pohybu s celkem ve vozidle spočívá minimálně v:

— aktualizaci montážních údajů snímače pohybu ukládaných do snímače pohybu (podle potřeby),

— kopírování potřebných identifikačních údajů snímače pohybu ze snímače do datové paměti celku ve vozidle.

205) Párování vnějšího zařízení GNSS s celkem ve vozidle spočívá minimálně v:

— aktualizaci montážních údajů vnějšího zařízení GNSS ukládaných do vnějšího zařízení GNSS (podle potřeby,

— kopírování potřebných identifikačních údajů vnějšího zařízení GNSS z vnějšího zařízení GNSS do datové paměti celku ve vozidle, včetně výrobního čísla vnějšího zařízení GNSS.

Po párování následuje ověření polohových informací GNSS.

206) Kalibrační funkce musí být schopna vložit nezbytné údaje prostřednictvím kalibračního/stahovacího konektoru v souladu s kalibračním protokolem definovaným v dodatku 8. Kalibrační funkce musí být schopna vložit nezbytné údaje i pomocí jiných prostředků.

3.22 **Silniční kalibrační kontrola**

207) Funkce silniční kalibrační kontroly musí umožnit čtení výrobního čísla snímače pohybu (případně zabudovaného v adaptéru) a výrobního čísla vnějšího zařízení GNSS (v příslušných případech), připojeného k celku ve vozidle v čase vyslání žádosti.

208) Toto čtení musí být možné minimálně na displeji celku ve vozidle prostřednictvím příkazů v menu.

209) Funkce silniční kalibrační kontroly musí rovněž umožnit kontrolu volby režimu I/O kalibračního signálního spojení I/O podle dodatku 6 pomocí rozhraní vodiče K. Tento postup je realizován pomocí parametru ECUAdjustmentSession podle specifikace v dodatku 8, části 7 Řízení zkušebních impulsů – Řídicí funkční celek vstup/výstup.

3.23 **Nastavení času**

210) Funkce nastavení času musí umožnit automatické nastavení aktuálního času. V záznamovém zařízení se pro nastavení času používají dva zdroje času: 1) vnitřní hodiny celku ve vozidle, 2) přijímač GNSS.

211) Nastavení času vnitřních hodin celku ve vozidle se provádí automaticky v intervalech maximálně 12 hodin. Pokud tato lhůta uplyne a 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. Nesoulad času nastane v případě, že se aktuální čas odchýlí od časové informace poskytované přijímačem GNSS o více než jednu (1) minutu.

212) Funkce nastavení času musí rovněž umožnit aktivované nastavení aktuálního času v kalibračním režimu.

3.24 **Provozní charakteristiky**

213) Celek ve vozidle musí být plně provozuschopný v rozsahu teplot od – 20 °C do 70 °C, vnější zařízení GNSS v rozsahu teplot od – 20 °C do 70 °C a snímač pohybu v rozmezí od – 40 °C do 135 °C. Obsah datové paměti musí být zachován při teplotách do – 40 °C.

214) Tachograf musí být plně funkční v rozsahu vlhkosti 10 % až 90 %.

215) Plomby používané v inteligentním tachografu musí odolávat stejným podmínkám, které platí pro součásti tachografu, k nimž jsou připojeny.

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

217) Snímače pohybu musí buď:

— reagovat na magnetické pole, které ruší detekci pohybu vozidla; za takových okolností celek ve vozidle zaznamená a uloží chybu snímače (požadavek 88); nebo

— mít snímací prvek, který je chráněn proti magnetickým polím, nebo je vůči jejich působení imunní.

218) Záznamové zařízení a vnější zařízení GNSS musí vyhovovat mezinárodnímu předpisu EHK OSN R10 a musí být chráněno proti elektrostatickým výbojům a přechodovým jevům.

3.25 **Materiály**

219) Všechny komponenty, ze kterých se záznamové zařízení skládá, musí být vyrobeny z materiálů s dostatečnou stabilitou, mechanickou pevností a stabilními elektrickými i magnetickými charakteristikami.

220) Při normálním použití musí být všechny vnitřní části zařízení chráněny proti vlhkosti a prachu.

221) Celek ve vozidle a vnější zařízení GNSS musí vyhovovat stupni ochrany IP 40 a snímač pohybu stupni ochrany IP 64 podle normy IEC 60529:1989, včetně A1:1999 a A2:2013.

222) Zařízení musí vyhovovat odpovídajícím technickým specifikacím vztahujícím se k ergonomii konstrukce.

223) Zařízení musí být chráněno proti náhodnému poškození.

3.26 **Značení**

224) Pokud záznamové zařízení zobrazuje údaje počitadla ujetých kilometrů a rychlost, musí se na zobrazovací jednotce objevit i následující údaje:

— v blízkosti údaje ujeté vzdálenosti jsou uvedeny jednotky vzdálenosti vyznačené zkratkou „km“,

— v blízkosti údaje zobrazujícího rychlost je jednotka „km/h“.

Záznamové zařízení může být také přepnuto, aby zobrazovalo rychlost v mílích za hodinu, a v tom případě je jednotka měřené rychlosti vyznačena zkratkou „mph“. Záznamové zařízení může být také přepnuto, aby zobrazovalo vzdálenost v mílích, a v tom případě je jednotka měřené vzdálenosti vyznačena zkratkou „mi“.

225) Popisný štítek musí být připevněn na každou samostatnou komponentu záznamového zařízení a nese tyto údaje:

— název a adresu výrobce zařízení,

— katalogové číslo součásti podle výrobce a rok výroby zařízení,

— výrobní číslo zařízení,

— značku schválení typu zařízení.

226) Pokud není k dispozici dostatečný prostor pro zobrazení všech výše uvedených podrobností, musí popisný štítek obsahovat alespoň: název nebo logo výrobce a katalogové číslo komponentu.

4 KONSTRUKČNÍ A FUNKČNÍ POŽADAVKY NA KARTY TACHOGRAFU

4.1 **Viditelné údaje**

Přední strana musí obsahovat:

227) slova „Karta řidiče“ nebo „Kontrolní karta“ nebo „Karta dílny“ nebo „Karta podniku“ vytištěná velkými písmeny v úředním jazyce nebo jazycích členského státu vydávajícího kartu, podle typu karty;

228) jméno členského státu vydávajícího kartu (volitelné);

229) rozlišovací značku členského státu vydávajícího kartu, která je tištěna inverzně v modrém obdélníku a je obklopena 12 žlutými hvězdami. Rozlišovací značky jsou tyto:

B	Belgie	LV	Lotyšsko
BG	Bulharsko	L	Lucembursko
CZ	Česká republika	LT	Litva
CY	Kypr	M	Malta
DK	Dánsko	NL	Nizozemsko

D EST	Německo Estonsko	A PL	Rakousko Polsko
GR	Řecko	P RO SK SLO	Portugalsko Rumunsko Slovensko Slovinsko
E	Španělsko	FIN	Finsko
F HR H	Francie Chorvatsko Maďarsko	S	Švédsko
IRL	Irsko	UK	Spojené království
I	Itálie		

230) zvláštní údaje k vydaným kartám číslované takto:

	Karta řidiče	Kontrolní karta	Karta podniku nebo dílny
1.	příjmení řidiče	název kontrolního orgánu	název podniku nebo dílny
2.	jméno(a) řidiče	příjmení kontrolora (v příslušných případech)	příjmení držitele karty (v příslušných případech)
3.	datum narození řidiče	jméno(a) kontrolora (v příslušných případech)	jméno (jména) držitele karty (v příslušných případech)
4.a	datum počátku platnosti karty		
4.b	datum konce platnosti karty		
4.c	orgán, který kartu vydal (může být vytištěno na druhé straně)		
4.d	číslo odlišné od čísla uvedeného v záhlaví 5, pro administrativní účely (volitelné)		
5. a	číslo řidičského průkazu (k datu vydání karty řidiče)	—	—
5. b	číslo karty		
6.	fotografie řidiče	fotografie kontrolora (volitelné)	fotografie montéra (volitelné)

	Karta řidiče	Kontrolní karta	Karta podniku nebo dílny
7.	podpis držitele (volitelné)		
8.	obvyklé místo pobytu nebo poštovní adresa držitele (volitelné).	poštovní adresa kontrolního orgánu	poštovní adresa podniku nebo dílny

231) datum musí být uváděno ve formátu „dd/mm/rrrr“ nebo „dd.mm.rrrr“ (den, měsíc, rok).

Rubová strana musí obsahovat:

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

233) na základě zvláštní psané dohody s držitelem mohou být uvedeny další informace, které se nevztahují ke správě karty, pokud nikterak nemění způsob použití daného modelu karty tachografu.

234) Karty tachografu musí být vydávány s těmito převládajícími barvami pozadí:

— karta řidiče: bílá barva,

— kontrolní karta: modrá barva,

— karta dílny: červená barva,

— karta podniku: žlutá barva.

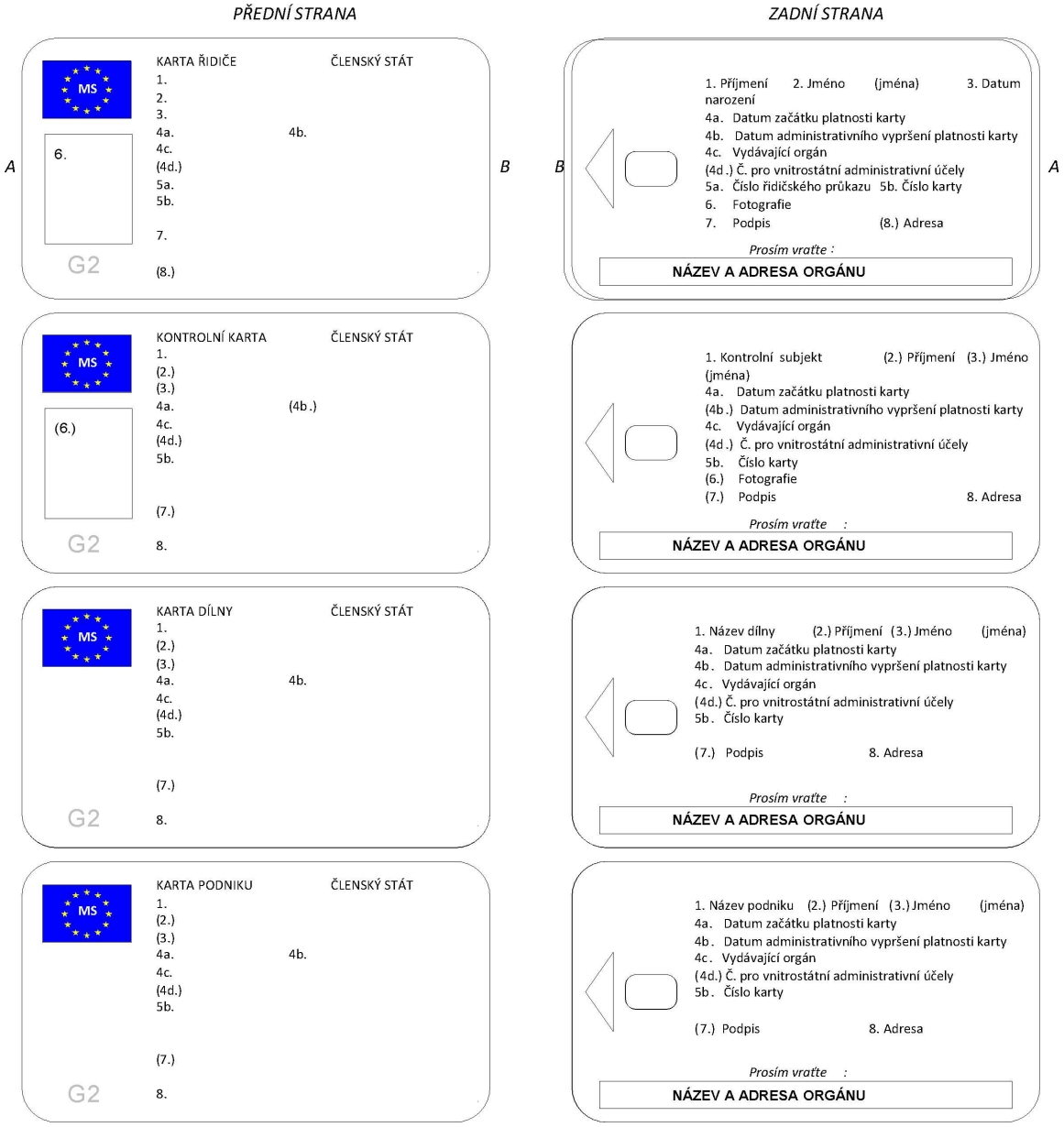
235) Karty tachografu musí nést minimálně následující ochranné prvky, chránící karty proti padělání a pozměňování:

— bezpečnostní provedení pozadí ve formě proplétané textury a duhového tisku,

— v oblasti fotografie se musí překrývat bezpečnostní provedení pozadí a fotografie,

— nejméně jednu dvoubarevnou mikrotiskovou linku.

MODEL SPOLEČENSTVÍ KARET TACHOGRAFU



236) Po konzultaci s Komisí mohou členské státy přidat barvy nebo označení, jako vnitrostátní symboly a bezpečnostní prvky, aniž by byla dotčena ostatní opatření této přílohy.

237) Dočasné karty podle článku 26.4 nařízení (EU) č. 165/2014 musí odpovídat ustanovením této přílohy.

4.2 Zabezpečení

Zabezpečení systému se zaměřuje na ochranu integrity a pravosti údajů přenášených mezi kartou a záznamovým zařízením, ochranu integrity a pravosti údajů stahovaných z karet, umožňuje zapsání jistých údajů na kartu pouze záznamovým zařízením, zaměřuje se na dešifrování některých údajů, vyloučení možnosti falzifikace údajů uložených na kartách, zabránění neoprávněné manipulaci a zjištění pokusu o podobné jednání.

238) Aby se dosáhlo systémové bezpečnosti, musí karty tachografu splňovat bezpečnostní požadavky definované v dodatcích 10 a 11.

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

4.3 **Normy**

240) Karty tachografu musí vyhovovat následujícím normám:

— ISO/IEC 7810 Identification cards – Physical characteristics, (Identifikační karty – Fyzikální charakteristiky),

— ISO/IEC 7816 Identification cards – Integrated circuit cards (Identifikační karty – Karty s integrovanými obvody s kontakty):

— Část 1: Fyzikální charakteristiky,

— Část 2: Rozměry a umístění kontaktů (ISO/IEC 7816-2:2007),

— Část 3: Elektronické rozhraní a protokoly přenosu (ISO/IEC 7816-3:2006),

— Část 4: Organizace, bezpečnost a příkazy pro výměnu (ISO/IEC 7816-4:2013 + opr. 1:2014),

— Část 6: Mezioborové datové prvky pro výměnu (ISO/IEC 7816-6:2004 + opr. 1:2006),

— Část 8: Příkazy pro bezpečnostní operace (ISO/IEC 7816-8:2004).

— Karty tachografu musí být testovány v souladu s normou ISO/IEC 10373-3:2010 Identification cards – Test methods (Identifikační karty – Zkušební metody) – Část 3: Karty s integrovanými obvody s kontakty a příslušná čtecí zařízení karet.

4.4 **Environmentální a elektrické specifikace**

241) Karty tachografu musí být schopny správné funkce za všech klimatických podmínek běžně se vyskytujících na území Společenství a nejméně v rozsahu teplot od – 25 °C do + 70 °C s příležitostnými špičkami do + 85 °C; „příležitostnými“ se myslí doba nepřesahující 4 hodiny a ne více než sto opakování v průběhu životnosti karty.

242) Karty tachografu musí být schopny správné funkce při vlhkosti v rozsahu 10 % až 90 %.

243) Karty tachografu musí být schopny správné funkce po dobu pěti let, pokud jsou používány ve shodě s předepsanými environmentálními a elektrickými specifikacemi.

244) V průběhu používání musí karty tachografu vyhovovat požadavkům nařízení EHK R10, vztahujícím se k elektromagnetické kompatibilitě, a musí být ochráněny proti elektrostatickým výbojům.

4.5 **Ukládání údajů**

Pro účely tohoto odstavce

— časové údaje jsou zaznamenávány s rozlišením jedné minuty, pokud není stanoveno jinak,

— stav počitadla ujetých kilometrů se zaznamenává s rozlišením jednoho kilometru,

— údaje o rychlosti jsou zaznamenávány s rozlišením 1 km/h,

— polohy (zeměpisné šířky a délky) jsou zaznamenávány ve stupních a minutách s rozlišením 1/10 minuty.

Funkce karty tachografu, příkazy a logické struktury, splnění požadavků na ukládání údajů jsou popsány v dodatku 2.

Není-li stanoveno jinak, je ukládání údajů na kartách tachografu organizováno tak, aby nové údaje nahrazovaly nejstarší uložené údaje, je-li vyčerpána velikost paměti vyhrazené pro příslušné záznamy.

245) Tento odstavec stanovuje minimální kapacitu pro ukládání dat v různých aplikačních souborech. Karty tachografu musí být schopny informovat záznamové zařízení o skutečné kapacitě těchto datových souborů.

246) Jakékoliv další údaje vztahující se k jiným aplikacím, případně přítomným na kartě, které smějí být ukládány na karty tachografu, musí být ukládány v souladu se směrnicí 95/46/ES a se směrnicí 2002/58/ES a v souladu s článkem 7 nařízení (EU) č. 165/2014.

247) Každý hlavní soubor (MF) každé karty tachografu musí obsahovat až pět elementárních souborů (EF) pro správu karty, identifikaci aplikace a čipu a dva vyhrazené soubory (DF):

— DF Tachograph, který obsahuje aplikaci přístupnou pro celky ve vozidle první generace, který je rovněž přítomen na kartách tachografu první generace,

— DF Tachograph_G2, který obsahuje aplikaci přístupnou pouze pro celky ve vozidle druhé generace, který je přítomen pouze na kartách tachografu druhé generace.

Úplné informace o struktuře karet tachografu jsou uvedeny v dodatku 2.

4.5.1 *Elementární soubory pro identifikaci a správu karty*

4.5.2 *Identifikace čipové karty*

248) Karty tachografu musí být schopny uchovávat následující identifikační údaje čipové karty:

— zastavení hodin,

— výrobní číslo karty (včetně výrobních referencí),

— číslo schválení typu karty,

— personifikovanou identifikaci (ID) karty,

— identifikátor integrátoru,

— identifikátor integrovaného obvodu.

4.5.2.1 Identifikace čipu

249) Karty tachografu musí být schopny uchovávat následující identifikační údaje integrovaného obvodu:

— výrobní číslo integrovaného obvodu,

— výrobní reference integrovaného obvodu.

4.5.2.2 DIR (pouze v kartách tachografu druhé generace)

250) Karty tachografu musí být schopny uchovávat datové objekty s identifikací aplikace specifikované v dodatku 2.

4.5.2.3 Informace ATR (podmínečné, pouze v kartách tachografu druhé generace)

251) Karty tachografu musí být schopny uchovávat následující datový objekt s s informací o rozšířené délce:

— pokud karta tachografu podporuje pole s rozšířenou délkou, datový objekt s informací o rozšířené délce specifikovaný v dodatku 2.

4.5.2.4 Informace o rozšířené délce (podmínečná, pouze v kartách tachografu druhé generace)

252) Karty tachografu musí být schopny uchovávat následující datové objekty s informací o rozšířené délce:

— pokud karta tachografu podporuje pole s rozšířenou délkou, datové objekty s informací o rozšířené délce specifikované v dodatku 2.

4.5.3 *Karta řidiče*

4.5.3.1 Aplikace tachografu (přístupná pro celky ve vozidle první a druhé generace)

4.5.3.1.1 Identifikace aplikace

253) Karta řidiče musí být schopna uchovat následující identifikační údaje aplikace:

— identifikaci aplikace tachografu,

— identifikaci typu karty tachografu.

4.5.3.1.2 Klíče a certifikáty

254) Karta řidiče musí být schopna uchovat řadu kryptografických klíčů a certifikátů podle specifikace v dodatku 11 části A.

4.5.3.1.3 Identifikace karty

255) Karta řidiče musí být schopna uchovat následující identifikační údaje karty:

— číslo karty,

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

— datum počátku platnosti karty, datum konce platnosti.

4.5.3.1.4 Identifikace držitele karty

256) Karta řidiče musí být schopna uchovat následující identifikační údaje držitele karty:

— příjmení držitele,

— jméno(a) držitele,

— datum narození,

— preferovaný jazyk.

4.5.3.1.5 Stahování z karty

257) Karta řidiče musí být schopna uchovat následující údaje týkající se stahování z karty:

— datum a čas posledního stahování z karty (pro jiné než kontrolní účely).

258) Karta řidiče musí být schopna uchovat jeden takový záznam.

4.5.3.1.6 Informace o řidičském průkazu

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

— vydávající členský stát, název vydávajícího orgánu,

— číslo řidičského průkazu (ke dni vydání karty).

4.5.3.1.7 Údaje o událostech

Pro účely tohoto pododstavce je čas ukládán s rozlišením jedné sekundy.

260) Karta řidiče musí být schopna uchovat údaje týkající se následujících událostí zjištěných záznamovým zařízením v době, kdy byla karta vložena:

— časové překrytí (v případě, že je tato karta příčinou události),

— vložení karty v průběhu jízdy, (v případě, že je tato karta předmětem události),

— nesprávné uzavření poslední relace karty (v případě, že je tato karta předmětem události),

— přerušení elektrického napájení,

— chyba údajů o pohybu vozidla

— pokusy o narušení zabezpečení.

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

— kód události,

— datum a čas počátku události (nebo vložení karty, pokud událost v této době probíhala),

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

— registrační značku vozidla a členský stát registrace, ve kterém k události došlo.

Poznámka: V případě události časového překrytí:

— datum a čas počátku události musí odpovídat datu a času vyjmutí karty z předcházejícího vozidla,

— datum a čas ukončení události musí odpovídat datu a času vložení karty v současně používaném vozidle,

— údaje o vozidle musí odpovídat současně používanému vozidlu, které vyvolalo událost.

Poznámka: V případě „nesprávného uzavření poslední relace karty“:

— datum a čas počátku události by měly odpovídat datu a času vložení karty, u níž došlo k nesprávnému uzavření poslední relace,

— datum a čas konce události by měl odpovídat datu a času vložení karty při relaci, v jejímž průběhu došlo k detekci události (aktuální relace),

— údaje o vozidlu musí odpovídat vozidlu, ve kterém došlo k nesprávnému uzavření poslední relace.

262) Karta řidiče musí být schopna uchovat údaje vztahující se k posledním šesti událostem každého typu (tzn. 36 událostem).

4.5.3.1.8 Údaje o závadách

Pro účely tohoto bodu musí být čas zaznamenáván s přesností jedné sekundy.

263) Karta řidiče musí být schopna uchovat údaje vztahující se k následujícím závadám zjištěným záznamovým zařízením době, kdy byla karta vložena:

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

— chyba záznamového zařízení.

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

— chybový kód,

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

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

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

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

4.5.3.1.9 Údaje o činnostech řidiče

266) Karta řidiče musí být schopna uchovat pro každý kalendářní den, kdy byla karta použita nebo pro který řidič vložil činnosti ručně, následující údaje:

— datum,

— stav počitadla denní přítomnosti (vzroste o jednotku každý kalendářní den),

— celkovou vzdálenost ujetou řidičem v průběhu tohoto dne,

— provozní stav řidiče v 00.00,

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

— provozní stav řidiče (POSÁDKA, SAMOTNÝ ŘIDIČ),

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

— stav karty (VLOŽENA, NEVLOŽENA),

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

— čas změny.

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

268) Údaje uvedené v požadavcích 261, 264 a 266 musí být uchovány způsobem umožňujícím vyhledání činností v chronologickém pořadí i v případě překrývajících se časových údajů.

4.5.3.1.10 Údaje o použitých vozidlech

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

— datum a čas prvního použití vozidla (tzn. první vložení karty v tomto časovém úseku použití vozidla, nebo 00h00, jestliže použití vozidla pokračuje v této době),

— údaj počitadla ujetých kilometrů v této době,

— datum a čas posledního použití vozidla (tzn. poslední vyjmutí karty v tomto časovém úseku použití vozidla, nebo 23h59, jestliže použití vozidla pokračuje v této době),

— údaj počitadla ujetých kilometrů v této době,

— registrační značku vozidla a členský stát registrace.

270) Karta řidiče musí být schopna uchovat 84 takových záznamů.

4.5.3.1.11 Místa, kde začíná a/nebo končí denní pracovní doba

271) Karta řidiče musí být schopna uchovat následující údaje vložené řidičem a vztahující se k místům, kde začíná a/nebo končí denní pracovní doba:

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

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

— zadanou zemi a region,

— stav počitadla ujetých kilometrů.

272) Paměť karty řidiče musí být schopna uchovat nejméně 42 párů takových záznamů.

4.5.3.1.12 Údaje o relaci karty

273) Karta řidiče musí být schopna uchovat údaje vztahující se k vozidlu, které otevřelo aktuální relaci:

— datum a čas otevření relace (tzn. vložení karty) s rozlišovací schopností jedné vteřiny,

— registrační značku vozidla a členský stát registrace.

4.5.3.1.13 Údaje o kontrolních činnostech

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

— datum a čas kontroly,

— číslo kontrolní karty a členský stát vydávající kartu,

— typ kontrolní činnosti (zobrazení a/nebo vytištění a/nebo stahování z celku ve vozidle a/nebo stahování z karty (viz poznámka)),

— dobu stahování dat, pokud k němu došlo,

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

Poznámka: Stahování z karty je zaznamenáno pouze v případě, že proběhne přes záznamové zařízení.

275) Karta řidiče musí být schopna uchovat jeden takový záznam.

4.5.3.1.14 Údaje o zvláštních podmínkách

276) Karta řidiče musí být schopna uchovat následující údaje vztahující se ke zvláštním podmínkám, které byly zadány v době, kdy byla karta vložena (v jakémkoliv otvoru pro vkládání karet):

— datum a čas záznamu,

— druh zvláštní podmínky.

277) Karta řidiče musí být schopna uchovat 56 takových záznamů.

4.5.3.2 Aplikace tachografu druhé generace (nepřístupná pro celek ve vozidle první generace)

4.5.3.2.1 Identifikace aplikace

278) Karta řidiče musí být schopna uchovat následující identifikační údaje aplikace:

— identifikaci aplikace tachografu,

— identifikaci typu karty tachografu.

4.5.3.2.2 Klíče a certifikáty

279) Karta řidiče musí být schopna uchovat řadu kryptografických klíčů a certifikátů podle specifikace v dodatku 11 části B.

4.5.3.2.3 Identifikace karty

280) Karta řidiče musí být schopna uchovat následující identifikační údaje karty:

— číslo karty,

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

— datum počátku platnosti karty, datum konce platnosti.

4.5.3.2.4 Identifikace držitele karty

281) Karta řidiče musí být schopna uchovat následující identifikační údaje držitele karty:

— příjmení držitele,

— jméno(a) držitele,

— datum narození,

— preferovaný jazyk.

4.5.3.2.5 Stahování z karty

282) Karta řidiče musí být schopna uchovat následující údaje týkající se stahování z karty:

— datum a čas posledního stahování z karty (pro jiné než kontrolní účely).

283) Karta řidiče musí být schopna uchovat jeden takový záznam.

4.5.3.2.6 Informace o řidičském průkazu

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

— vydávající členský stát, název vydávajícího orgánu,

— číslo řidičského průkazu (ke dni vydání karty).

4.5.3.2.7 Údaje o událostech

Pro účely tohoto pododstavce je čas ukládán s rozlišením jedné sekundy.

285) Karta řidiče musí být schopna uchovat údaje týkající se následujících událostí zjištěných záznamovým zařízením v době, kdy byla karta vložena:

— časové překrytí (v případě, že je tato karta příčinou události),

— vložení karty v průběhu jízdy, (v případě, že je tato karta předmětem události),

— nesprávné uzavření poslední relace karty (v případě, že je tato karta předmětem události),

— přerušení elektrického napájení,

— chyba komunikace se zařízením pro dálkovou komunikaci,

— chybějící informace o poloze z přijímače GNSS,

— komunikační chyba s vnějším zařízením GNSS,

— chyba údajů o pohybu vozidla,

— nesoulad údajů o pohybu vozidla,

— pokusy o narušení zabezpečení,

— časový konflikt.

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

— kód události,

— datum a čas počátku události (nebo vložení karty, pokud událost v té době probíhala),

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

— registrační značka vozidla a členský stát registrace, ve kterém k události došlo.

Poznámka: V případě události časového překrytí:

— datum a čas počátku události musí odpovídat datu a času vyjmutí karty z předcházejícího vozidla,

— datum a čas ukončení události musí odpovídat datu a času vložení karty v současně používaném vozidle,

— údaje o vozidle musí odpovídat současně používanému vozidlu, které vyvolalo událost.

Poznámka: V případě „nesprávného uzavření poslední relace karty“:

— datum a čas počátku události by měly odpovídat datu a času vložení karty, u níž došlo k nesprávnému uzavření poslední relace,

— datum a čas konce události by měly odpovídat datu a času vložení karty při relaci, v jejímž průběhu došlo k detekci události (aktuální relace),

— údaje o vozidlu musí odpovídat vozidlu, ve kterém došlo k nesprávnému uzavření poslední relace.

287) Karta řidiče musí být schopna uchovat údaje vztahující se k posledním šesti událostem každého typu (tzn. 66 událostem).

4.5.3.2.8 Údaje o závadách

Pro účely tohoto bodu musí být čas zaznamenáván s přesností jedné sekundy.

288) Karta řidiče musí být schopna uchovat údaje vztahující se k následujícím závadám zjištěným záznamovým zařízením době, kdy byla karta vložena:

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

— chyba záznamového zařízení.

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

— chybový kód,

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

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

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

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

4.5.3.2.9 Údaje o činnostech řidiče

291) Karta řidiče musí být schopna uchovat pro každý kalendářní den, kdy byla karta použita nebo pro který řidič vložil činnosti ručně, následující údaje:

— datum,

— stav počitadla denní přítomnosti (vzroste o jednotku každý kalendářní den),

— celkovou vzdálenost ujetou řidičem v průběhu tohoto dne,

— provozní stav řidiče v 00.00,

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

— provozní stav řidiče (POSÁDKA, SAMOTNÝ ŘIDIČ),

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

— stav karty (VLOŽENA, NEVLOŽENA),

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

— čas změny.

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

293) Údaje uvedené v požadavcích 286, 289 a 291 musí být uchovány způsobem umožňujícím vyhledání v chronologickém pořadí i v případě překrývajících se časových údajů.

4.5.3.2.10 Údaje o použitých vozidlech

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

— datum a čas prvního použití vozidla (tzn. první vložení karty v tomto časovém úseku použití vozidla, nebo 00h00, jestliže použití vozidla pokračuje v této době),

— údaj počitadla ujetých kilometrů v této době prvního použití,

— datum a čas posledního použití vozidla (tzn. poslední vyjmutí karty v tomto časovém úseku použití vozidla, nebo 23h59, jestliže použití vozidla pokračuje v této době),

— údaj počitadla ujetých kilometrů v této době posledního použití,

— registrační značku vozidla a členský stát registrace.

— číslo VIN.

295) Karta řidiče musí být schopna uchovat 84 takových záznamů.

4.5.3.2.11 Místa a polohy, kde začíná a/nebo končí denní pracovní doba

296) Karta řidiče musí být schopna uchovat následující údaje vložené řidičem a vztahující se k místům, kde začíná a/nebo končí denní pracovní doba:

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

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

— zadanou zemi a region,

— stav počitadla ujetých kilometrů,

— polohu vozidla,

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

297) Paměť karty řidiče musí být schopna uchovat nejméně 84 párů takových záznamů.

4.5.3.2.12 Údaje o relaci karty

298) Karta řidiče musí být schopna uchovat údaje vztahující se k vozidlu, které otevřelo aktuální relaci:

— datum a čas otevření relace (tzn. vložení karty) s rozlišovací schopností jedné vteřiny,

— registrační značku vozidla a členský stát registrace.

4.5.3.2.13 Údaje o kontrolních činnostech

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

— datum a čas kontroly,

— číslo kontrolní karty a členský stát vydávající kartu,

— typ kontrolní činnosti (zobrazení a/nebo vytištění a/nebo stahování z celku ve vozidle a/nebo stahování z karty (viz poznámka)),

— dobu stahování dat, pokud k němu došlo,

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

Poznámka: Bezpečnostní požadavky předpokládají, že stahování z karty je zaznamenáno pouze v případě, že proběhne přes záznamové zařízení.

300) Karta řidiče musí být schopna uchovat jeden takový záznam.

4.5.3.2.14 Údaje o zvláštních podmínkách

301) Karta řidiče musí být schopna uchovat následující údaje vztahující se ke zvláštním podmínkám, které byly zadány v době, kdy byla karta vložena (v jakémkoliv otvoru pro vkládání karet):

— datum a čas záznamu,

— druh zvláštní podmínky.

302) Karta řidiče musí být schopna uchovat 56 takových záznamů.

4.5.3.2.15 Údaje o použitých celcích ve vozidle

303) Karta řidiče musí být schopna uchovat následující údaje vztahující se k různým celkům ve vozidle, ve kterých byla karta použita:

— datum a čas zahájení doby používání celku ve vozidle (tj. první vložení karty do celku ve vozidle pro příslušnou dobu),

— výrobce celku ve vozidle,

— typ celku ve vozidle,

— číslo verze softwaru celku ve vozidle.

304) Karta řidiče musí být schopna uchovat 84 takových záznamů.

4.5.3.2.16 Údaje o místech nepřetržité tříhodinové doby řízení

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

— datum a čas, kdy nepřetržitá doba řízení držitele karty dosáhne násobku tří hodin,

— polohu vozidla,

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

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

4.5.4 *Karta dílny*

4.5.4.1 Aplikace tachografu (přístupná pro celky ve vozidle první a druhé generace)

4.5.4.1.1 Identifikace aplikace

307) Karta dílny musí být schopna uchovat následující identifikační údaje aplikace:

— identifikaci aplikace tachografu,

— identifikaci typu karty tachografu.

4.5.4.1.2 Klíče a certifikáty

308) Karta dílny musí být schopna uchovat řadu kryptografických klíčů a certifikátů podle specifikace v dodatku 11 části A.

309) Karta dílny musí být schopna uchovat osobní identifikační číslo (kód PIN).

4.5.4.1.3 Identifikace karty

310) Karta dílny musí být schopna uchovat následující identifikační údaje karty:

— číslo karty,

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

— datum počátku platnosti karty, datum konce platnosti.

4.5.4.1.4 Identifikace držitele karty

311) Karta dílny musí být schopna uchovat následující identifikační údaje držitele karty:

— název dílny,

— adresu dílny,

— příjmení držitele,

— jméno(a) držitele,

— preferovaný jazyk.

4.5.4.1.5 Stahování z karty

312) Karta dílny musí být schopna uchovat údaje o stahování z karty stejným způsobem jako karta řidiče.

4.5.4.1.6 Údaje o kalibraci a nastavování času

313) Karta dílny musí být schopna uchovat záznamy o kalibracích a/nebo nastavování času provedených v době, kdy byla karta vložena v záznamovém zařízení.

314) Každý kalibrační záznam musí být schopen uchovat následující údaje:

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

— identifikaci vozidel

— aktualizované nebo potvrzené parametry (w, k, l, rozměr pneumatik, nastavení zařízení omezujícího rychlost vozidla, údaje počitadla ujetých kilometrů (nová a stará hodnota), datum a čas (nová a stará hodnota)),

— identifikaci záznamového zařízení (katalogové číslo celku ve vozidle, výrobní číslo celku ve vozidle, výrobní číslo snímače rychlosti).

315) Karta dílny musí být schopna uchovat nejméně 88 takových záznamů.

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

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

4.5.4.1.7 Údaje o událostech a závadách

318) Karta dílny musí být schopna uchovat údaje o událostech a závadách stejným způsobem jako karta řidiče.

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

4.5.4.1.8 Údaje o činnostech řidiče

320) Karta dílny musí být schopna uchovat údaje o činnostech řidiče stejným způsobem jako karta řidiče.

321) Karta dílny musí být schopna uchovat údaje o činnostech řidiče pro nejméně jeden den průměrné činnosti řidiče.

4.5.4.1.9 Údaje o použitých vozidlech

322) Karta dílny musí být schopna uchovat údaje o použitých vozidlech stejným způsobem jako karta řidiče.

323) Karta dílny musí být schopna uchovat nejméně čtyři takové záznamy.

4.5.4.1.10 Údaje o začátku a/nebo konci denní pracovní doby

324) Karta dílny musí být schopna uchovat údaje o začátku a/nebo konci denní pracovní doby stejným způsobem jako karta řidiče.

325) Karta dílny musí být schopna uchovat nejméně tři páry takových záznamů.

4.5.4.1.11 Údaje o relaci karty

326) Karta dílny musí být schopna uchovat údaje o relaci karty stejným způsobem jako karta řidiče.

4.5.4.1.12 Údaje o kontrolních činnostech

327) Karta dílny musí být schopna uchovat údaje o kontrolní činnosti stejným způsobem jako karta řidiče.

4.5.4.1.13 Údaje o zvláštních podmínkách

328) Karta dílny musí být schopna uchovat údaje o zvláštních podmínkách stejným způsobem jako karta řidiče.

329) Karta dílny musí být schopna uchovat nejméně dva takové záznamy.

4.5.4.2 Aplikace tachografu druhé generace (nepřístupná pro celek ve vozidle první generace)

4.5.4.2.1 Identifikace aplikace

330) Karta dílny musí být schopna uchovat následující identifikační údaje aplikace:

— identifikaci aplikace tachografu,

— identifikaci typu karty tachografu.

4.5.4.2.2 Klíče a certifikáty

331) Karta dílny musí být schopna uchovat řadu kryptografických klíčů a certifikátů podle specifikace v dodatku 11 části B.

332) Karta dílny musí být schopna uchovat osobní identifikační číslo (kód PIN).

4.5.4.2.3 Identifikace karty

333) Karta dílny musí být schopna uchovat následující identifikační údaje karty:

— číslo karty,

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

— datum počátku platnosti karty, datum konce platnosti.

4.5.4.2.4 Identifikace držitele karty

334) Karta dílny musí být schopna uchovat následující identifikační údaje držitele karty:

— název dílny,

— adresu dílny,

— příjmení držitele,

— jméno(a) držitele,

— preferovaný jazyk.

4.5.4.2.5 Stahování z karty

335) Karta dílny musí být schopna uchovat údaje o stahování z karty stejným způsobem jako karta řidiče.

4.5.4.2.6 Údaje o kalibraci a nastavování času

336) Karta dílny musí být schopna uchovat záznamy o kalibracích a/nebo nastavování času provedených v době, kdy byla karta vložena v záznamovém zařízení.

337) Každý kalibrační záznam musí být schopen uchovat následující údaje:

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

— identifikaci vozidla,

— aktualizované nebo potvrzené parametry (w, k, l, rozměr pneumatik, nastavení zařízení omezujícího rychlost vozidla, údaje počitadla ujetých kilometrů (nová a stará hodnota), datum a čas (nová a stará hodnota),

— identifikaci záznamového zařízení (katalogové číslo celku ve vozidle, výrobní číslo celku ve vozidle, výrobní číslo snímače rychlosti, výrobní číslo zařízení dálkové komunikace a v příslušných případech výrobní číslo vnějšího zařízení GNSS),

— typ plomby a identifikátor všech použitých plomb,

— schopnost celku ve vozidle používat karty tachografu první generace (aktivována nebo nikoli).

338) Karta dílny musí být schopna uchovat nejméně 88 takových záznamů.

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

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

4.5.4.2.7 Údaje o událostech a závadách

341) Karta dílny musí být schopna uchovat údaje o událostech a závadách stejným způsobem jako karta řidiče.

342) Karta dílny musí být schopna uchovat údaje o třech posledních událostech každého typu (tzn. 33 událostí) a šest posledních záznamů o závadách každého typu (tzn. 12 závad).

4.5.4.2.8 Údaje o činnostech řidiče

343) Karta dílny musí být schopna uchovat údaje o činnostech řidiče stejným způsobem jako karta řidiče.

344) Karta dílny musí být schopna uchovat údaje o činnostech řidiče pro nejméně jeden den průměrné činnosti řidiče.

4.5.4.2.9 Údaje o použitých vozidlech

345) Karta dílny musí být schopna uchovat údaje o použitých vozidlech stejným způsobem jako karta řidiče.

346) Karta dílny musí být schopna uchovat nejméně čtyři takové záznamy.

4.5.4.2.10 Údaje o začátku a/nebo konci denní pracovní doby

347) Karta dílny musí být schopna uchovat údaje o začátku a/nebo konci denní pracovní doby stejným způsobem jako karta řidiče.

348) Karta dílny musí být schopna uchovat nejméně tři páry takových záznamů.

4.5.4.2.11 Údaje o relaci karty

349) Karta dílny musí být schopna uchovat údaje o relaci karty stejným způsobem jako karta řidiče.

4.5.4.2.12 Údaje o kontrolních činnostech

350) Karta dílny musí být schopna uchovat údaje o kontrolní činnosti stejným způsobem jako karta řidiče.

4.5.4.2.13 Údaje o použitých celcích ve vozidle

351) Karta dílny musí být schopna uchovat následující údaje vztahující se k různým celkům ve vozidle, ve kterých byla karta použita:

— datum a čas zahájení doby používání celku ve vozidle (tj. první vložení karty do celku ve vozidle pro příslušnou dobu),

— výrobce celku ve vozidle,

— typ celku ve vozidle,

— číslo verze softwaru celku ve vozidle.

352) Karta dílny musí být schopna uchovat nejméně čtyři takové záznamy.

4.5.4.2.14 Údaje o místech nepřetržité tříhodinové doby řízení

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

— datum a čas, kdy nepřetržitá doba řízení držitele karty dosáhne násobku tří hodin,

— polohu vozidla,

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

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

4.5.4.2.15 Údaje o zvláštních podmínkách

355) Karta dílny musí být schopna uchovat údaje o zvláštních podmínkách stejným způsobem jako karta řidiče.

356) Karta dílny musí být schopna uchovat nejméně dva takové záznamy.

4.5.5 *Kontrolní karta*

4.5.5.1 Aplikace tachografu (přístupná pro celky ve vozidle první a druhé generace)

4.5.5.1.1 Identifikace aplikace

357) Kontrolní karta musí být schopna uchovat následující identifikační údaje aplikace:

— identifikaci aplikace tachografu,

— identifikaci typu karty tachografu.

4.5.5.1.2 Klíče a certifikáty

358) Karta dílny musí být schopna uchovat řadu kryptografických klíčů a certifikátů podle specifikace v dodatku 11 části A.

4.5.5.1.3 Identifikace karty

359) Kontrolní karta musí být schopna uchovat následující identifikační údaje karty:

— číslo karty,

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

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

4.5.5.1.4 Identifikace držitele karty

360) Kontrolní karta musí být schopna uchovat následující identifikační údaje držitele karty:

— název kontrolního orgánu,

— adresu kontrolního orgánu,

— příjmení držitele,

— jméno(a) držitele,

— preferovaný jazyk.

4.5.5.1.5 Údaje o kontrolních činnostech

361) Kontrolní karta musí být schopna uchovat následující údaje o kontrolní činnosti:

— datum a čas kontroly,

— druh kontroly (zobrazení a/nebo tisk a/nebo stahování z celku ve vozidle a/nebo stahování z karty a/nebo silniční kalibrační kontrola),

— dobu stahování dat (pokud proběhlo),

— registrační značku vozidla a registrační orgán členského státu kontrolovaného vozidla,

— číslo karty a členský stát vydávající kontrolovanou kartu řidiče.

362) Kontrolní karta musí být schopna uchovat nejméně 230 takových záznamů.

4.5.5.2 Aplikace tachografu druhé generace (nepřístupná pro celek ve vozidle první generace)

4.5.5.2.1 Identifikace aplikace

363) Kontrolní karta musí být schopna uchovat následující identifikační údaje aplikace:

— identifikaci aplikace tachografu,

— identifikaci typu karty tachografu.

4.5.5.2.2 Klíče a certifikáty

364) Kontrolní karta musí být schopna uchovat řadu kryptografických klíčů a certifikátů podle specifikace v dodatku 11 části B.

4.5.5.2.3 Identifikace karty

365) Kontrolní karta musí být schopna uchovat následující identifikační údaje karty:

— číslo karty,

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

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

4.5.5.2.4 Identifikace držitele karty

366) Kontrolní karta musí být schopna uchovat následující identifikační údaje držitele karty:

— název kontrolního orgánu,

— adresu kontrolního orgánu,

— příjmení držitele,

— jméno(a) držitele,

— preferovaný jazyk.

4.5.5.2.5 Údaje o kontrolních činnostech

367) Kontrolní karta musí být schopna uchovat následující údaje o kontrolní činnosti:

— datum a čas kontroly,

— druh kontroly (zobrazení a/nebo tisk a/nebo stahování z celku ve vozidle a/nebo stahování z karty a/nebo silniční kalibrační kontrola),

— dobu stahování dat (pokud proběhlo),

— registrační značku vozidla a registrační orgán členského státu kontrolovaného vozidla,

— číslo karty a členský stát vydávající kontrolovanou kartu řidiče.

368) Kontrolní karta musí být schopna uchovat nejméně 230 takových záznamů.

4.5.6 *Karta podniku*

4.5.6.1 Aplikace tachografu (přístupná pro celky ve vozidle první a druhé generace)

4.5.6.1.1 Identifikace aplikace

369) Karta podniku musí být schopna uchovat následující identifikační údaje aplikace:

— identifikaci aplikace tachografu,

— identifikaci typu karty tachografu.

4.5.6.1.2 Klíče a certifikáty

370) Karta podniku musí být schopna uchovat řadu kryptografických klíčů a certifikátů podle specifikace v dodatku 11 části A.

4.5.6.1.3 Identifikace karty

371) Karta podniku musí být schopna uchovat následující identifikační údaje karty:

— číslo karty,

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

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

4.5.6.1.4 Identifikace držitele karty

372) Karta podniku musí být schopna uchovat následující identifikační údaje držitele karty:

— název podniku,

— adresu podniku.

4.5.6.1.5 Údaje o činnosti podniku

373) Karta podniku musí být schopna uchovat následující údaje o činnosti podniku:

— datum a čas činnosti,

— druh činnosti (odemčení a/nebo uzamčení celku ve vozidle a/nebo stahování z celku ve vozidle a/nebo stahování z karty)

— dobu stahování dat (pokud proběhlo),

— registrační značku vozidla a registrační orgán vozidla členského státu,

— číslo karty a kartu vydávající členský stát (v případě stahování dat z karty).

374) Karta podniku musí být schopna uchovat nejméně 230 takových záznamů.

4.5.6.2 Aplikace tachografu druhé generace (nepřístupná pro celek ve vozidle první generace)

4.5.6.2.1 Identifikace aplikace

375) Karta podniku musí být schopna uchovat následující identifikační údaje aplikace:

— identifikaci aplikace tachografu,

— identifikaci typu karty tachografu.

4.5.6.2.2 Klíče a certifikáty

376) Karta dílny musí být schopna uchovat řadu kryptografických klíčů a certifikátů dle specifikace v dodatku 11 části B.

4.5.6.2.3 Identifikace karty

377) Karta podniku musí být schopna uchovat následující identifikační údaje karty:

— číslo karty,

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

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

4.5.6.2.4 Identifikace držitele karty

378) Karta podniku musí být schopna uchovat následující identifikační údaje držitele karty:

— název podniku,

— adresu podniku.

4.5.6.2.5 Údaje o činnosti podniku

379) Karta podniku musí být schopna uchovat následující údaje o činnosti podniku:

— datum a čas činnosti,

— druh činnosti (odemčení a/nebo uzamčení celku ve vozidle a/nebo stahování z celku ve vozidle a/nebo stahování z karty)

— dobu stahování dat (pokud proběhlo),

— registrační značku vozidla a registrační orgán vozidla členského státu,

— číslo karty a kartu vydávající členský stát (v případě stahování dat z karty).

380) Karta podniku musí být schopna uchovat nejméně 230 takových záznamů.

5 MONTÁŽ ZÁZNAMOVÉHO ZAŘÍZENÍ

5.1 **Montáž**

381) Nové záznamové zařízení musí být dodáno servisní dílně nebo výrobci vozidla neaktivované, se všemi kalibračními parametry, jak je uvedeno v kapitole 3.21, a s nastavenými příslušnými platnými implicitními hodnotami. V případě, že žádná konkrétní hodnota není považována za „příslušnou", musí se písmenné parametry nastavit na řetězce „?" a numerické parametry na „0". Dodávky součástí záznamového zařízení důležitých pro zabezpečení mohou být omezeny, pokud o to bude během certifikace zabezpečení požádáno.

382) Záznamové zařízení musí před aktivací umožnit přístup ke kalibrační funkci dokonce, i když není v kalibračním režimu.

383) Záznamové zařízení nesmí před aktivací zaznamenávat ani ukládat údaje uvedené v bodech 3.12.3, 3.12.9 a 3.12.12 až 3.12.15 včetně.

384) V průběhu montáže musí výrobci vozidel přednastavit všechny známé parametry.

385) Výrobci vozidel nebo montážní pracovníci musí namontované záznamové zařízení aktivovat nejpozději do té doby, než je vozidlo použito v rámci působnosti nařízení (ES) č. 561/2006.

386) Aktivace záznamového zařízení se musí spustit automaticky prvním vložením platné karty dílny do jednoho ze zařízení rozhraní karty.

387) Specifické úkony párování potřebné mezi snímačem pohybu a celkem ve vozidle, pokud je namontován, musí proběhnout automaticky před nebo v průběhu aktivace.

388) Podobně musí případné specifické úkony vytvoření vazby mezi vnějším zařízením GNSS a celkem ve vozidle proběhnout automaticky před aktivací nebo v jejím průběhu.

389) Po aktivaci záznamového zařízení musí být plně aktivní funkce zařízení a přístupová práva.

390) Po aktivaci musí záznamové zařízení předávat zařízení pro dálkovou komunikaci zabezpečené údaje potřebné za účelem cílených silničních kontrol.

391) Záznamové a ukládací funkce záznamového zařízení musí být po aktivaci plně funkční.

392) Po instalaci musí následovat kalibrace. První kalibrace nemusí nutně zahrnovat zadání registrační značky vozidla VRN, pokud ji schválená dílna, která má tuto kalibraci provést, nezná. Za těchto okolností musí mít vlastník vozidla možnost, a to pouze v tomto případě, zadat VRN pomocí karty dílny před použitím vozidla v rámci působnosti nařízení (ES) č. 561/2006 (např. pomocí příkazů v příslušné struktuře nabídky rozhraní člověk-stroj celku ve vozidle). [1] Případné pozměnění nebo potvrzení této položky musí být možné jen za použití karty dílny.

393) Montáž vnějšího zařízení GNSS vyžaduje spárování s celkem ve vozidle a následné ověření informací o poloze z GNSS.

394) Záznamové zařízení se musí ve vozidle umístit takovým způsobem, aby umožňovalo řidiči přístup k potřebným funkcím z jeho sedadla.

[1] Úř. věst. č. L 102, 11.4.2006, s. 1.

5.2 **Montážní štítek**

395) Po provedení kontroly záznamového zařízení, která následuje po montáži, se na záznamové zařízení upevní dobře viditelný a snadno přístupný, rytý nebo trvanlivě tištěný montážní štítek. V případech, kdy toto není možné, musí být štítek upevněn na sloupek „B“ vozidla tak, aby byl dobře viditelný. U vozidel, která sloupek „B“ nemají, musí být montážní štítek upevněn na rám dveří vozidla na straně řidiče a v každém případě musí být dobře viditelný.

Po každé prohlídce provedené schváleným montérem nebo dílnou musí být původní štítek nahrazen novým.

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,

— výrobní číslo vnějšího zařízení GNSS,

— výrobní číslo zařízení dálkové komunikace,

— 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.

397) Pouze u vozidel kategorií M1 a N1, která jsou vybavena adaptérem v souladu s nařízením Komise (ES) č. 68/2009 ([1]) v platném znění a u kterých není možné zahrnout všechny potřebné informace podle požadavku 396, může být použit druhý doplňkový štítek. V takových případech musí tento doplňkový štítek obsahovat alespoň informace uvedené v posledních čtyřech odrážkách požadavku 396.

Pokud je tento druhý, doplňkový štítek použit, musí být upevněn vedle prvního, hlavního štítku popsaného v požadavku 396 a musí mít stejnou úroveň ochrany. Kromě toho musí být na doplňkovém štítku uvedeno jméno a adresa nebo obchodní název schváleného montéra nebo dílny, která montáž provedla, a datum montáže.

([1]) Úř. věst. č. L 21, 24.1.2009, s. 3

5.3 **Plomby**

398) Následující díly musí být zaplombovány:

— jakékoliv spojení, jehož rozpojení by umožnilo provedení neidentifikovatelných změn nebo neidentifikovatelnou ztrátu dat (toto opatření může např. platit pro upevnění snímače pohybu na převodovce, adaptér pro vozidla M1/N1, vnější připojení GNSS nebo celek ve vozidle);

— montážní štítek, pokud není připevněn tak, aby jej nebylo možno sejmout bez zničení jeho údajů.

399) Výše uvedené plomby mohou být odstraněny:

— v nouzových situacích,

— při montáži, seřizování nebo opravě omezovače rychlosti vozidla nebo jiného zařízení přispívajícího k bezpečnosti silničního provozu za předpokladu, že záznamové zařízení nadále spolehlivě a správně funguje a bude opětovně zaplombováno schváleným montérem nebo dílnou (v souladu s kapitolou 6) okamžitě po namontování omezovače rychlosti nebo jiného zařízení přispívajícího k bezpečnosti silničního provozu nebo v průběhu sedmi dnů v ostatních případech.

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

401) Plomby jsou opatřeny identifikačním číslem přiděleným jejich výrobcem. Toto číslo musí být jedinečné a odlišné od všech ostatních čísel plomb přidělených jakýmkoli jiným výrobcem plomb.

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

402) Plomby musí mít volné místo, kam mohou schválení montéři, dílny nebo výrobci vozidel přidat zvláštní značku podle čl. 22 odst. 3 nařízení (EU) č. 165/2014.

Tato značka nesmí zakrývat identifikační číslo plomby.

403) Výrobci plomb musí být registrováni v příslušné databázi a musí zveřejnit identifikační čísla svých plomb postupem stanoveným Evropskou komisí.

404) Schválené dílny a výrobci vozidel musí v rámci nařízení (EU) č. 165/2014 používat pouze plomby od výrobců uvedených ve výše uvedené databázi.

405) Výrobci plomb a jejich prodejci musí zachovat plnou sledovatelnost záznamů prodaných plomb pro použití v rámci nařízení (EU) č. 165/2014 a musí být připraveni je podle potřeby předložit příslušným vnitrostátním orgánům.

406) Jedinečná identifikační čísla plomb musí být viditelná na montážním štítku.

6 KONTROLY, INSPEKCE A OPRAVY

Požadavky týkající se okolností, za kterých mohou být odstraněny plomby uváděné v čl. 22 odst. 5 nařízení (EU) č. 165/2014, jsou definovány v kapitole 5.3 této přílohy.

6.1 **Schválení montérů, dílen a výrobců vozidel**

Členské státy schvalují a pravidelně kontrolují subjekty a vydávají jim osvědčení k provádění:

— montáží,

— kontrol,

— prohlídek,

— oprav.

Karty dílny se vydávají pouze montérům a/nebo dílnám oprávněným k aktivaci a/nebo kalibraci záznamových zařízení v souladu s touto přílohou, a kromě řádně odůvodněných případů:

— které nejsou oprávněny k použití karty podniku

— a jejichž další profesní činnosti nepředstavují potenciální střet zájmů z hlediska celkového zabezpečení systému podle požadavků v dodatku 10.

6.2 **Kontrola nových nebo opravených přístrojů**

407) Každé jednotlivé zařízení, ať již nové nebo opravené, musí být kontrolováno s ohledem na jeho správnou funkci a přesnost odečtů a záznamů, která musí odpovídat limitům stanoveným v bodech 3.2.1, 3.2.2, 3.2.3 a 3.3, zaplombováním v souladu s kapitolou 5.3 a kalibrací.

6.3 **Montážní kontrola**

408) Po namontování záznamového zařízení do vozidla musí celá montáž (včetně záznamového zařízení) vyhovovat ustanovením vztahujícím se k přípustným tolerancím stanoveným v bodech 3.2.1, 3.2.2, 3.2.3 a 3.3.

6.4 **Periodické prohlídky**

409) Pravidelná kontrola zařízení namontovaného do vozidla musí proběhnout po každé opravě zařízení, po jakékoliv změně charakteristického koeficientu vozidla, účinného obvodu pneumatik kol, odchylce referenčního času UTC o více než 20 minut, při změně VRN, ale minimálně jednou v průběhu dvou let (24 měsíců) od poslední prohlídky.

410) Tyto prohlídky musí obsahovat následující kontroly zajišťující, že:

— je zajištěna správná funkce záznamového zařízení včetně ukládání údajů na kartách tachografu a komunikace se snímači dálkové komunikace,

— je zajištěn soulad s ustanoveními bodů 3.2.1 a 3.2.2, které se týkají povolených tolerancí při montáži,

— je zajištěn soulad s ustanoveními bodů 3.2.3 a 3.3,

— záznamové zařízení nese značku schválení typu,

— je upevněn montážní štítek definovaný v požadavku 396 a popisný štítek definovaný v požadavku 225,

— odpovídá velikost pneumatik a skutečný obvod pneumatik,

— k zařízení nejsou připojeny žádné manipulační pomůcky,

— plomby jsou správně umístěné, v dobrém stavu, že jsou jejich identifikační čísla platná (příslušný výrobce plomb v databázi EK) a že jejich identifikační čísla odpovídají značkám na montážním štítku (viz požadavek 401).

411) Pokud se zjistí, že od poslední kontroly došlo k výskytu některé z událostí uvedených v kapitole 3.9 (Zjišťování událostí a/nebo závad), pokud je taková událost výrobci tachografů a/nebo vnitrostátními orgány považována za možné ohrožení zabezpečení zařízení, potom je dílna povinna:

a. porovnat identifikační údaje snímače pohybu připojeného k převodovce s identifikačními údaji párového snímače pohybu zaregistrovaného v celku ve vozidle;

b. zkontrolovat, zda informace uvedené na montážním štítku odpovídají informacím obsaženým v záznamu celku ve vozidle;

c. zkontrolovat, zda výrobní číslo a číslo schválení snímače pohybu, pokud je vytištěno na těle snímače pohybu, odpovídá informacím obsaženým v datové paměti záznamového zařízení;

d. porovnat případné identifikační údaje uvedené na popisném štítku vnějšího zařízení GNSS s údaji uloženými v datové paměti celku ve vozidle.

412) Dílny jsou povinny ve svých kontrolních zprávách evidovat veškerá zjištění týkající se porušených plomb nebo manipulačních pomůcek. Tyto zprávy musí dílny uchovávat po dobu nejméně dvou let a zpřístupnit je příslušnému orgánu, kdykoli jsou o to požádány.

413) Tyto prohlídky musí obsahovat kalibraci a preventivní výměnu plomb, za jejichž upevnění jsou odpovědné dílny.

6.5 **Měření odchylek**

414) Měření odchylek při montáži a při užívání se provádí za následujících podmínek, jež jsou považovány za obvyklé zkušební podmínky:

— prázdné vozidlo v obvyklých provozních podmínkách,

— tlak v pneumatikách podle údajů výrobce,

— opotřebení pneumatik je v mezích povolených vnitrostátními právními předpisy,

— pohyb vozidla:

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

— za předpokladu, že je zajištěna srovnatelná přesnost, může být pro provedení zkoušky použito alternativních metod, jako je vhodné zkušební zařízení.

6.6 **Opravy**

415) Dílny musí být schopny stahovat data ze záznamového zařízení, aby údaje mohly být předloženy zpět dotyčnému dopravnímu podniku.

416) Schválení montéři a servisní dílny musí dopravnímu podniku vydat potvrzení o nemožnosti stáhnout data, pokud špatná funkce záznamového zařízení brání stažení dříve zaznamenaných dat i v případě, že oprava byla prováděna v téže dílně. Dílny musí archivovat kopie vydaných potvrzení nejméně po dobu dvou let.

7 VYDÁVÁNÍ KARET

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

417) Číslo karty při prvním vydání karty tachografu žadateli musí obsahovat pořadový index (v příslušných případech), index náhrady a index obnovy, které jsou nastaveny na hodnotu „0“.

418) Čísla karet všech neosobních karet tachografu, které byly vydány témuž kontrolnímu orgánu, téže dílně nebo témuž dopravnímu podniku, musí mít shodných prvních 13 číslic, ale všechna musí mít odlišné pořadové indexy.

419) Karta tachografu, která se vydává jako náhrada již existující karty, musí mít stejné číslo karty jako nahrazovaný exemplář s výjimkou indexu náhrady, který se zvedne o jednotku (v pořadí 0, …, 9, A, …, Z).

420) Karta tachografu, která se vydává jako náhrada již existující karty, musí mít shodné datum ukončení použitelnosti jako nahrazovaný exemplář.

421) Karta tachografu vydávaná při obnovení již existující karty musí mít stejné číslo karty jako obnovovaný exemplář s výjimkou indexu náhrady, který je nastaven na hodnotu „0“, a indexu obnovy, který je zvýšen o jednotku (v pořadí 0, …, 9, A, …, Z).

422) Výměna existující karty tachografu při úpravách administrativních údajů, musí proběhnout podle pravidel platných pro obnovu karty, pokud proces probíhá ve stejném členském státě, nebo podle pravidel pro první vydání karty, pokud probíhá v jiném členském státě.

423) „Příjmení držitele karty“ u neosobních karet dílny nebo kontrolních karet musí být vyplněno názvem dílny nebo kontrolního orgánu nebo jménem montéra nebo kontrolora, pokud se tak členské státy rozhodnou.

424) Členské státy si musí elektronicky vyměňovat údaje, aby byla zajištěna jedinečnost karet řidiče, které vydávají v souladu s článkem 31 nařízení (EU) č. 165/2014.

8 SCHVÁLENÍ TYPU ZÁZNAMOVÉHO ZAŘÍZENÍ A KARET TACHOGRAFU

8.1 **Všeobecně**

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 zařízení dálkové komunikace s celkem ve vozidle. Papír používaný záznamovým zařízením je považován za součást záznamového zařízení.

Kterýkoli výrobce může požádat o schválení typu pro svou součást s libovolným snímačem pohybu, vnějším zařízením GNSS a naopak, pokud každá součást splňuje požadavky této přílohy. Alternativně mohou výrobci rovněž požádat o schválení typu záznamového zařízení.

425) Záznamové zařízení musí být předloženo ke schválení typu úplné se všemi integrovanými přídavnými zařízeními.

426) Postup schvalování typu záznamového zařízení a karet tachografu musí zahrnovat zkoušky bezpečnostních opatření, funkční zkoušky a zkoušky vzájemné interoperability. Pozitivní výsledky každé z těchto zkoušek se potvrdí příslušnými osvědčeními.

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

— osvědčení o bezpečnosti,

— osvědčení o funkčnosti,

— a osvědčení o interoperabilitě

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

428) Jakákoli úprava programového nebo technického vybavení zařízení nebo povahy materiálu použitého pro jeho výrobu musí být před zavedením oznámena orgánu, který vydal schválení typu zařízení. Tento orgán potvrdí výrobci rozšíření schválení typu, nebo může požadovat aktualizaci nebo potvrzení příslušného osvědčení o funkčnosti, o bezpečnosti a/nebo o interoperabilitě.

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

430) Schválení typu úprav programového vybavení zaměřených na aktualizaci záznamového zařízení s dřívějším schválením typu nesmí být zamítnuto, pokud takové úpravy platí pouze pro funkce, které nejsou uvedeny v této příloze. Aktualizace programového vybavení záznamového zařízení může vylučovat zavedení nových sad písma, není-li to technicky proveditelné.

8.2 **Osvědčení o bezpečnosti**

431) Vydání osvědčení o bezpečnosti se provede v souladu s ustanoveními dodatku 10 této přílohy. Součásti záznamového zařízení, pro které se vydává osvědčení, jsou celek ve vozidle, snímač pohybu, vnější zařízení GNSS a karty tachografu.

432) Za výjimečných okolností, kdy orgány provádějící certifikaci zabezpečení odmítnou vystavit osvědčení pro nové zařízení z důvodu zastaralosti zabezpečovacích mechanismů, musí být schválení typu nadále vydáváno pouze za těchto konkrétních a výjimečných okolností a když neexistuje žádné alternativní řešení, které by bylo v souladu s nařízením.

433) Za těchto okolností je dotyčný členský stát povinen neprodleně informovat Evropskou komisi, která do dvanácti měsíců od udělení schválení typu zahájí postup, který zajistí obnovení původní úrovně zabezpečení.

8.3 **Osvědčení o funkčnosti**

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

435) Výrobci musí poskytovat příslušné vzorky výrobků ucházejících se o schválení typu a související dokumentaci požadovanou zkušebnami pověřenými prováděním funkčních zkoušek, a to do jednoho měsíce od data vyžádání. Veškeré náklady související s touto žádostí nese žádající subjekt. Zkušebny jsou povinny uchovávat veškeré obchodně citlivé informace v tajnosti.

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

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

438) V osvědčení o funkčnosti kterékoli součásti záznamového zařízení musí být také uvedena čísla schválení typu ostatních kompatibilních součástí záznamového zařízení se schválením typu, testovaných pro vydání osvědčení.

439) V osvědčení o funkčnosti kterékoli součásti záznamového zařízení musí být také uvedena norma ISO nebo CEN, na jejímž základě bylo vydáno osvědčení pro funkční rozhraní.

8.4 **Osvědčení o interoperabilitě**

440) Zkoušky interoperability se provádějí v jediné zkušebně schválené a podléhající Evropské komisi.

441) Zkušebna registruje požadavky výrobců na zkoušky interoperability v pořadí, v jakém byly doručeny.

442) Požadavky budou úředně registrovány pouze tehdy, jestliže zkušebně již byly dodány:

— úplná sada materiálů a dokumentů nezbytných pro takové zkoušky interoperability,

— související osvědčení o bezpečnosti,

— související osvědčení o funkčnosti.

Datum registrace žádosti musí být oznámeno výrobci.

443) U záznamového zařízení nebo karty tachografu, ke kterým nebyla poskytnuta osvědčení o zabezpečení a funkčnosti, zkušebna neprovádí žádné zkoušky interoperability, kromě případů výskytu výjimečných okolností popsaných v požadavku 432.

444) Každý výrobce požadující zkoušky interoperability se zaváže ponechat zkušebně, která odpovídá za provedení zkoušek, úplnou sadu materiálů a dokumentace, které byly ke zkouškám dodány.

445) Zkoušky interoperability musí být provedeny v souladu s dodatkem 9 této přílohy postupně se všemi typy záznamových zařízení a karet tachografu:

— jejichž schválení typu je dosud platné, nebo

— jejichž schválení typu není dosud vyřízeno, ale mají platné osvědčení o interoperabilitě.

446) Zkoušky interoperability se musí vztahovat na všechny generace záznamového zařízení nebo karet tachografu, které se dosud používají.

447) Osvědčení o interoperabilitě musí zkušebna doručit výrobci teprve tehdy, až jsou úspěšně absolvovány všechny požadované zkoušky interoperability.

448) Jestliže zkoušky interoperability nejsou úspěšné s jedním nebo několika záznamovými zařízeními nebo kartou/kartami tachografu, osvědčení o interoperabilitě nesmí být vydáno, dokud výrobce žádající o schválení neprovede nezbytné úpravy a neabsolvuje úspěšně zkoušky interoperability. Zkušebna identifikuje příčinu problému týkajícího se interoperability s pomocí příslušného výrobce a pokusí se mu pomoci nalézt technické řešení. V případě, že výrobce již upravil svůj výrobek, musí zajistit od příslušných orgánů potvrzení o pokračující platnosti osvědčení o bezpečnosti a funkčnosti.

449) Osvědčení o interoperabilitě je platné šest měsíců. Na konci tohoto období je odebráno, pokud výrobce neobdržel odpovídající osvědčení o schválení typu. Osvědčení doručí výrobce orgánu příslušnému pro schvalování typu členského státu, který vydal osvědčení o funkčnosti.

450) Jakýkoli prvek, který by mohl způsobit závadu interoperability, nesmí být použit pro vytvoření zisku a nesmí vést k získání dominantního postavení.

8.5 **Osvědčení o schválení typu**

451) Orgán členského státu příslušný pro schvalování typu může vydat osvědčení o schválení typu, jakmile obdrží tři požadovaná osvědčení.

452) Osvědčení o schválení typu jakékoli součásti záznamového zařízení musí rovněž obsahovat čísla schválení typu ostatních interoperabilních záznamových zařízení se schválením typu.

453) Orgán příslušný pro schvalování typu předá kopii osvědčení o schválení typu zkušebně pověřené prováděním zkoušek interoperability v době vydání osvědčení výrobci.

454) Zkušebna pověřená prováděním zkoušek interoperability musí udržovat internetové stránky, na kterých je aktualizovaný seznam modelů záznamových zařízení a karet tachografu:

— pro které byla zaregistrována žádost o zkoušky interoperability,

— které obdržely osvědčení o interoperabilitě (i dočasné),

— které získaly osvědčení o schválení typu.

8.6 **Výjimečný postup: první osvědčení o interoperabilitě pro záznamové zařízení a karty tachografu druhé generace**

455) V průběhu čtyř měsíců po osvědčení první vazby mezi záznamovým zařízením a kartami tachografu (kartami řidiče, dílny, kontrolní a podniku) druhé generace z hlediska interoperability je jakékoliv vydané osvědčení o interoperabilitě (včetně těch prvních) týkající se žádostí registrovaných v tomto období považováno za dočasné.

456) Jestliže na konci tohoto období budou všechny dotčené výrobky vzájemně interoperabilní, stanou se všechna příslušná osvědčení o interoperabilitě definitivními.

457) Jestliže budou v tomto období zjištěny závady z hlediska interoperability, musí zkušebna pověřená prováděním zkoušek interoperability za pomoci všech zúčastněných výrobců identifikovat zdroje obtíží a vyzvat výrobce k provedení nezbytných úprav.

458) Jestliže na konci tohoto období budou problémy s interoperabilitou přetrvávat, musí odpovědná zkušebna ve spolupráci s dotčenými výrobci a orgány příslušnými pro schvalování typu, které vydaly související osvědčení o funkčnosti, zjistit důvody závad v interoperabilitě a stanovit, které úpravy by měl každý dotčený výrobce provést. Hledání technických řešení smí trvat maximálně dva měsíce, po kterých v případě nenalezení společného řešení rozhodne Komise po konzultaci se zkušebnou pověřenou prováděním zkoušek interoperability, která zařízení a karty obdrží definitivní osvědčení o interoperabilitě, a zdůvodní proč.

459) Všechny žádosti o zkoušky interoperability registrované mezi koncem čtyřměsíčního období po vydání prvního dočasného osvědčení o interoperabilitě a datem rozhodnutí Komise podle požadavku 455 musí být odloženy, dokud nebudou počáteční obtíže s interoperabilitou vyřešeny. Tyto žádosti budou potom vyřízeny v pořadí, v jakém byly registrovány.

Dodatek 1

DATOVÝ SLOVNÍK

OBSAH

1. ÚVOD

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

1.1 **Přístup k definování datových typů**

Tento dodatek používá k definování datových typů notaci ASN.1 (*Abstract Syntax Notation One*). Díky tomu lze jednoduchá a strukturovaná data definovat, aniž by se předpokládala nějaká konkrétní přenosová syntaxe (pravidla kódování), která bude závislá na aplikaci a systémovém prostředí.

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

— tam, kde je to možné, je význam datového typu naznačen zvolenými názvy,

— tam, kde je datový typ složen z jiných datových typů, je názvem datového typu nadále jednoduchá posloupnost abecedních znaků začínající velkým písmenem, nicméně velká písmena jsou použita uvnitř názvu ke sdělení příslušného významu,

— názvy datových typů obvykle souvisejí s názvy datových typů, od kterých jsou odvozeny, zařízením, ve kterém jsou data uložena, a funkcí vztahující se k datům.

Jestliže je typ ASN.1 již definován v rámci jiného standardu a jestliže má význam pro použití v záznamovém zařízení, je tento typ ASN.1 definován v tomto dodatku.

K umožnění několika typů kódovacích pravidel jsou některé typy ASN.1 v tomto dodatku omezeny pomocí identifikátorů rozsahu hodnot. Identifikátory rozsahu hodnot jsou definovány v bodě 3 a dodatku 2.

1.2 **Odkazy**

V tomto dodatku jsou použity tyto normy:

ISO 639	Code for the representation of names of languages. First Edition: 1988.
ISO 3166	Codes for the representation of names of countries and their subdivisions – Part 1: Country codes, 2013
ISO 3779	*Road vehicles – Vehicle identification number (VIN) – Content and structure.* 2009
ISO/IEC 7816-5	Identification cards – Integrated circuit cards – Part 5: Registration of application providers. Second edition: 2004.
ISO/IEC 7816-6	Identification cards – Integrated circuit cards – Part 6: Interindustry data elements for interchange, 2004 + Technical Corrigendum 1: 2006
ISO/IEC 8824-1	Information technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation. 2008 + Technical Corrigendum 1: 2012 and Technical Corrigendum 2: 2014.
ISO/IEC 8825-2	Information technology – ASN.1 encoding rules: Specification of Packed Encoding Rules (PER). 2008.
ISO/IEC 8859-1	Information technology – 8 bit single-byte coded graphic character sets – Part 1: Latin alphabet No.1. First edition: 1998.
ISO/IEC 8859-7	Information technology – 8 bit single-byte coded graphic character sets – Part 7: Latin/Greek alphabet. 2003.

ISO 16844-3 Road vehicles – Tachograph systems – Motion Sensor Interface. 2004 + Technical Corrigendum 1: 2006.

TR-03110-3 BSI / ANSSI Technical Guideline TR-03110-3, Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token – Part 3 Common Specifications, version 2.20, 3. February 2015

2. DEFINICE DATOVÝCH TYPŮ

U všech následujících datových typů spočívá standardní hodnota pro „neznámý“ nebo „bezpředmětný“ obsah v naplnění daného datového prvku bajty „FF“.

Není-li stanoveno jinak, všechny datové typy se použijí pro aplikace 1. a 2. generace.

2.1 **ActivityChangeInfo**

Tento datový typ umožňuje kódovat uvnitř dvoubajtového slova status otvoru pro kartu v 00:00 a/nebo status řidiče v 00:00 a/nebo změny činnosti a/nebo změny statusu řízení a/nebo změny statusu karty, a to pro řidiče nebo druhého řidiče. Tento datový typ se vztahuje k požadavkům 105, 266, 291, 320, 321, 343 a 344 přílohy 1C.

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

Přiřazení hodnoty – oktetové uspořádání: ‘scpaatttttttttt’B (16 bitů)

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

‘s’B otvor pro kartu:

‘0’B: ŘIDIČ,

‘1’B: DRUHÝ ŘIDIČ,

‘c’B status řízení vozidla:

‘0’B: SAMOTNÝ ŘIDIČ,

‘1’B: POSÁDKA,

‘p’B status karty řidiče (nebo karty dílny) v příslušném otvoru pro kartu:

‘0’B: VLOŽENA, karta je vložena,

‘1’B: NEVLOŽENA, není vložena žádná karta (nebo je karta vyjmuta),

‘aa’B činnost:

‘00’B: PŘESTÁVKA/ODPOČINEK,

‘01’B: POHOTOVOST,

‘10’B: PRÁCE,

‘11’B: ŘÍZENÍ,

‘ttttttttttt’B čas změny: počet minut od 00h00 daného dne.

Pro záznamy na kartě řidiče (nebo kartě dílny) (a status řidiče):

‘s’B	otvor pro kartu (není relevantní, jestliže ‘p’=1, kromě dále uvedené poznámky):
	‘0’B: ŘIDIČ,
	‘1’B: DRUHÝ ŘIDIČ,
‘c’B	status řízení (při ‘p’=0) nebo
	následující status činnosti (při ‘p’=1):
	‘0’B: SAMOTNÝ ŘIDIČ,
	‘0’B: NEZNÁMÁ
	‘1’B: POSÁDKA,
	‘1’B: ZNÁMÁ (= ručně zadaná)
‘p’B	status karty:
	‘0’B: VLOŽENA, karta je vložena do záznamového zařízení,
	‘1’B: NEVLOŽENA, karta není vložena (nebo je karta vyjmuta),
‘aa’B	činnost (nepoužije se, jestliže ‘p’=1 a ‘c’=0, kromě poznámky níže):
	‘00’B: PŘESTÁVKA/ODPOČINEK,
	‘01’B: POHOTOVOST,
	‘10’B: PRÁCE,
	‘11’B: ŘÍZENÍ,
‘ttttttttttt’B	čas změny: počet minut od 00h00 daného dne.

Poznámka pro případ „vyjmutí karty“:

Je-li karta vyjmuta:

— ‘s’ je relevantní a označuje otvor pro kartu, ze kterého je karta vyjmuta,

— ‘c’ musí být nastaveno na 0,

— ‘p’ musí být nastaveno na 1,

— ‘aa’ musí kódovat aktuální činnost, která je v tu dobu navolena.

Jako výsledek ručního zadání mohou být bity ‘c’ a ‘aa’ slova (uloženého na kartě) později přepsány s ohledem na toto zadání.

2.2 Address

Adresa.

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

codePage určuje znakovou sadu definovanou v kapitole 4.

address je adresa kódovaná za použití určené znakové sady.

2.3 **AESKey**

2. generace:

Klíč AES s délkou 128, 192 nebo 256 bitů.

```
AESKey ::= CHOICE {
   aes128Key                          AES128Key,
   aes192Key                          AES192Key,
   aes256Key                          AES256Key
}
```

Přiřazení hodnoty: není blíže specifikováno.

2.4 **AES128Key**

2. generace:

Klíč AES128.

```
AES128Key ::= SEQUENCE {
   length                             INTEGER(0..255),
   aes128Key                          OCTET STRING (SIZE(16))
}
```

length udává délku klíče AES128 v oktetech.

aes128Key je klíč AES s délkou 128 bitů.

Přiřazení hodnoty:

Délka musí mít hodnotu 16.

2.5 **AES192Key**

2. generace:

Klíč AES192.

```
AES192Key ::= SEQUENCE {
   length                             INTEGER(0..255),
   aes192Key                          OCTET STRING (SIZE(24))
}
```

length udává délku klíče AES192 v oktetech.

aes192Key je klíč AES s délkou 192 bitů.

Přiřazení hodnoty:

Délka musí mít hodnotu 24.

2.6 **AES256Key**

2. generace:

Klíč AES256.

```
AES256Key ::= SEQUENCE {
   length                                  INTEGER(0..255),
   aes256Key                               OCTET STRING (SIZE(32))
}
```

length udává délku klíče AES256 v oktetech.

aes256Key je klíč AES s délkou 256 bitů.

Přiřazení hodnoty:

Délka musí mít hodnotu 32.

2.7 **BCDString**

BCDString se použije pro vyjádření dekadických čísel binárním kódem (BCD). Tento datový typ se použije k vyjádření jedné dekadické číslice skupinou 4 bitů (poloviční oktet). BCDString je založen na typu „Character-StringType“ dle ISO/IEC 8824-1.

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

BCDString používá notaci „hstring“. Vnější levá hexadecimální číslice představuje nejvýznamnější 4 bity prvního oktetu. K získání více oktetů se musí podle potřeby vložit od pozice levé vnější 4bitové skupiny v prvním oktetu nulové 4bitové skupiny.

Přípustné číslice jsou: 0, 1, .. 9.

2.8 **CalibrationPurpose**

Kód k objasnění, proč byla zaznamenána sada kalibračních parametrů. Tento datový typ se vztahuje k požadavkům 097 a 098 přílohy 1B a k požadavku 119 přílohy 1C.

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

Přiřazení hodnoty:

1. generace:

‘00’H	vyhrazená hodnota,
‘01’H	aktivace: záznam známých kalibračních parametrů v okamžiku aktivace celku ve vozidle,
‘02’H	první montáž: první kalibrace celku ve vozidle po jeho aktivaci,
‘03’H	montáž: první kalibrace celku ve vozidle v aktuálním vozidle,
‘04’H	pravidelná kontrola.

2. generace:

Kromě hodnot 1. generace se používají tyto hodnoty:

'05'H zadání registrační značky vozidla (VRN) podnikem,

'06'H nastavení času bez kalibrace,

'07'H až '7F'H vyhrazeno pro budoucí použití,

'80'H až 'FF'H specifické pro výrobce.

2.9 **CardActivityDailyRecord**

Informace uložené na kartě a vztahující se k činnostem řidiče po určitý kalendářní den. Tento datový typ se vztahuje k požadavkům 266, 291, 320 a 343 přílohy 1C.

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

activityPreviousRecordLength je celková délka předchozího denního záznamu v bajtech. Maximální hodnota je dána délkou řetězce OCTET STRING obsahujícího tyto záznamy (viz CardActivityLengthRange, dodatek 2 bod 4). Jestliže tento záznam je nejstarším denním záznamem, musí být hodnota activityPreviousRecordLength nastavena na 0.

activityRecordLength je celková délka tohoto záznamu v bajtech. Maximální hodnota je dána délkou řetězce OCTET STRING obsahujícího tyto záznamy.

activityRecordDate je datum záznamu.

activityDailyPresenceCounter je stav počitadla dnů přítomnosti karty v tento den.

activityDayDistance je celková vzdálenost ujetá toho dne.

activityChangeInfo je sada dat ActivityChangeInfo toho dne pro řidiče. Může obsahovat maximálně 1 440 hodnot (jedna změna činnosti za minutu). Tato sada vždy obsahuje údaj activityChangeInfo udávající status řidiče v 00:00.

2.10 **CardActivityLengthRange**

Počet bajtů na kartě řidiče nebo kartě dílny, které jsou dostupné k ukládání záznamů o činnosti řidiče.

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

Přiřazení hodnoty: viz dodatek 2.

2.11 **CardApprovalNumber**

Číslo schválení typu karty.

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

Přiřazení hodnoty:

Číslo schválení musí být uvedeno tak, jak bylo zveřejněno na příslušných webových stránkách Evropské komise, tj. např. včetně případných spojovníků. Číslo schválení musí být zarovnáno doleva.

2.12 **CardCertificate**

1. generace:

Certifikát veřejného klíče karty.

```
CardCertificate ::= Certificate
```

2.13 **CardChipIdentification**

Informace uložené na kartě související s identifikací integrovaného obvodu karty (IC) (požadavek 249 přílohy 1C). Číslo icSerialNumber společně s číslem icManufacturingReferences jednoznačně identifikují čip karty. Samotné číslo icSerialNumber není jednoznačnou identifikací čipu karty.

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

icSerialNumber je výrobní číslo integrovaného obvodu.

icManufacturingReferences je identifikátor specifický pro výrobce integrovaného obvodu.

2.14 **CardConsecutiveIndex**

Pořadový index karty (definice h)).

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

Přiřazení hodnoty: (viz příloha 1C kapitola 7)

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

2.15 **CardControlActivityDataRecord**

Informace uložené na kartě řidiče nebo kartě dílny týkající se poslední kontroly, které byl řidič podroben (požadavky 274, 299, 327 a 350 přílohy 1C).

```
CardControlActivityDataRecord ::= SEQUENCE {
   controlType                       ControlType,
   controlTime                       TimeReal,
   controlCardNumber                 FullCardNumber,
   controlVehicleRegistration        VehicleRegistrationIdentification,
   controlDownloadPeriodBegin        TimeReal,
   controlDownloadPeriodEnd          TimeReal
}
```

controlType je typ kontroly.

controlTime je datum a čas kontroly.

controlCardNumber je FullCardNumber kontrolora, který provedl kontrolu.

controlVehicleRegistration je registrační značka (VRN) a členský stát registrace vozidla, ve kterém byla kontrola provedena.

controlDownloadPeriodBegin a **controlDownloadPeriodEnd** je stažené období v případě stahování dat.

2.16 CardCurrentUse

Informace o aktuálním použití karty (požadavky 273, 298, 326 a 349 přílohy 1C).

```
CardCurrentUse ::= SEQUENCE {
   sessionOpenTime                    TimeReal,
   sessionOpenVehicle                 VehicleRegistrationIdentification
}
```

sessionOpenTime je čas, kdy je karta vložena pro aktuální použití. Tento prvek se nastavuje na nulu při vyjmutí karty.

sessionOpenVehicle je identifikace aktuálně používaného vozidla, nastavuje se při vložení karty. Tento prvek se nastavuje na nulu při vyjmutí karty.

2.17 CardDriverActivity

Informace uložené na kartě řidiče nebo kartě dílny týkající se činností řidiče (požadavky 267, 268, 292, 293, 321 a 344 přílohy 1C).

```
CardDriverActivity ::= SEQUENCE {
   activityPointerOldestDayRecord     INTEGER(0.. CardActivityLengthRange-1),
   activityPointerNewestRecord        INTEGER(0.. CardActivityLengthRange-1),
   activityDailyRecords               OCTET STRING
                                      (SIZE(CardActivityLengthRange))
}
```

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

activityPointerNewestRecord je specifikace začátku paměťového místa (počet bajtů od začátku řetězce) nejnovějšího denního záznamu v řetězci activityDailyRecords. Maximální hodnota je dána délkou řetězce.

activityDailyRecords je prostor určený k ukládání dat o činnosti řidiče (datová struktura: CardActivityDaily-Record) pro každý kalendářní den, kdy byla karta použita.

Přiřazení hodnoty: tento oktetový řetězec je cyklicky plněn záznamy CardActivityDailyRecord. Při prvním použití se začíná ukládat od prvního bajtu řetězce. Každý nový záznam se připojuje za konec předchozího. Když je řetězec plný, ukládání pokračuje prvním bajtem řetězce nehledě na přerušení, které vznikne uvnitř datového prvku. Předtím, než jsou do řetězce uložena nová data o činnosti (zvětšení aktuálního záznamu activityDaily-Record nebo uložení nového záznamu activityDailyRecord), která nahrazují starší data o činnosti, musí být aktualizován ukazatel activityPointerOldestDayRecord, aby odrážel nové umístění nejstaršího úplného denního záznamu, a délka activityPreviousRecordLength tohoto (nového) nejstaršího úplného denního záznamu musí být nastavena na 0.

2.18 CardDrivingLicenceInformation

Informace uložené na kartě řidiče týkající se údajů o řidičském průkazu držitele karty (požadavky 259 a 284 přílohy 1C).

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

drivingLicenceIssuingAuthority je orgán odpovědný za vydání řidičského průkazu.

drivingLicenceIssuingNation je stát orgánu, který vydal řidičský průkaz.

drivingLicenceNumber je číslo řidičského průkazu.

2.19 CardEventData

Informace uložené na kartě řidiče nebo kartě dílny týkající se událostí souvisejících s držitelem karty (požadavky 260, 285, 318 a 341 přílohy 1C).

```
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).

2.20 CardEventRecord

Informace uložené na kartě řidiče nebo kartě dílny týkající se události související s držitelem karty (požadavky 261, 286, 318 a 341 přílohy 1C).

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

eventType je typ události.

eventBeginTime je datum a čas začátku události.

eventEndTime je datum a čas konce události.

eventVehicleRegistration je registrační značka (VRN) a členský stát registrace vozidla, ve kterém událost nastala.

2.21 CardFaultData

Informace uložené na kartě řidiče nebo kartě dílny týkající se závad souvisejících s držitelem karty (požadavky 263, 288, 318 a 341 přílohy 1C).

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

CardFaultData je posloupnost sad záznamů o závadách záznamového zařízení následovaná sadou záznamů o závadách karty.

cardFaultRecords je sada záznamů o závadách patřících do určité kategorie závad (záznamové zařízení nebo karta).

2.22 CardFaultRecord

Informace uložené na kartě řidiče nebo kartě dílny týkající se závady související s držitelem karty (požadavky 264, 289, 318 a 341 přílohy 1C).

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

faultType je typ závady.

faultBeginTime je datum a čas začátku závady.

faultEndTime je datum a čas konce závady.

faultVehicleRegistration je registrační značka (VRN) a členský stát registrace vozidla, ve kterém závada nastala.

2.23 CardIccIdentification

Informace uložené na kartě týkající se identifikace karty s integrovaným obvodem (požadavek 248 přílohy 1C).

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

clockStop je režim Clockstop dle dodatku 2.

cardExtendedSerialNumber je jedinečné výrobní číslo karty s integrovaným obvodem, dále specifikované datovým typem ExtendedSerialNumber.

cardApprovalNumber je číslo schválení typu karty.

cardPersonaliserID je identifikátor personalizace karty kódovaný jako ManufacturerCode.

embedderIcAssemblerId uvádí informace o subjektu, který vkládá/sestavuje integrovaný obvod.

icIdentifier je identifikátor integrovaného obvodu karty a jeho výrobce dle ISO/IEC 7816-6.

2.24 CardIdentification

Informace uložené na kartě týkající se identifikace karty (požadavky 255, 280, 310, 333, 359, 365, 371 a 377 přílohy 1C).

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

cardIssuingMemberState je kód členského státu vydávajícího kartu.

cardNumber je číslo karty.

cardIssuingAuthorityName je název orgánu vydávajícího kartu.

cardIssueDate je datum vydání karty současnému držiteli.

cardValidityBegin je datum prvního dne platnosti karty.

cardExpiryDate je datum konce platnosti karty.

2.25 CardMACertificate

2. generace:

Certifikát veřejného klíče karty pro vzájemné ověření pravosti s celkem ve vozidle. Struktura tohoto certifikátu je specifikována v dodatku 11.

```
CardMACertificate ::= Certificate
```

2.26 CardNumber

Číslo karty dle definice g).

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

driverIdentification je jednoznačná identifikace řidiče v členském státě.

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

cardConsecutiveIndex je pořadový index karty.

cardReplacementIndex je index náhrady karty.

cardRenewalIndex je index obnovy karty.

První posloupnost ve výběru je vhodná ke kódování čísla karty řidiče, druhá posloupnost ve výběru je vhodná ke kódování čísla karty dílny, kontrolní karty a karty podniku.

2.27 **CardPlaceDailyWorkPeriod**

Informace uložené na kartě řidiče nebo kartě dílny týkající se míst, kde začíná nebo končí denní pracovní doba (požadavky 272, 297, 325 a 348 přílohy 1C).

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

placePointerNewestRecord je index naposledy aktualizovaného záznamu o místě.

Přiřazení hodnoty: Číslo odpovídající čítači záznamů míst, začínající „0“ pro první výskyt záznamu místa ve struktuře.

placeRecords je sada záznamů obsahující informace týkající se zadaných míst.

2.28 **CardPrivateKey**

1. generace:

Soukromý klíč karty.

```
CardPrivateKey ::= RSAKeyPrivateExponent
```

2.29 **CardPublicKey**

Veřejný klíč karty.

```
CardPublicKey ::= PublicKey
```

2.30 **CardRenewalIndex**

Index obnovy karty (definice i)).

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

Přiřazení hodnoty: (viz kapitolu VII této přílohy).

‘0’ První vydání.

Posloupnost: ‘0, …, 9, A, …, Z’

2.31 **CardReplacementIndex**

Index náhrady karty (definice j)).

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

Přiřazení hodnoty: (viz kapitolu VII této přílohy).

‘0’ Původní karta.

Posloupnost: ‘0, …, 9, A, …, Z’

2.32 **CardSignCertificate**

2. generace:

Certifikát veřejného klíče karty pro podpis. Struktura tohoto certifikátu je specifikována v dodatku 11.

```
CardSignCertificate ::= Certificate
```

2.33 **CardSlotNumber**

Kód pro rozlišení mezi dvěma otvory pro kartu v celku ve vozidle.

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

Přiřazení hodnoty: není blíže specifikováno.

2.34 **CardSlotsStatus**

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

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

Přiřazení hodnoty – oktetové uspořádání: 'ccccdddd'B

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

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

s těmito identifikačními kódy:

'0000'B není vložena žádná karta,

'0001'B je vložena karta řidiče,

'0010'B je vložena karta dílny,

'0011'B je vložena kontrolní karta,

'0100'B je vložena karta podniku.

2.35 **CardSlotsStatusRecordArray**

2. generace:

CardSlotsStatus a metadata použitá v protokolu pro stahování.

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

recordType označuje typ záznamu (CardSlotsStatus). **Přiřazení hodnoty**: viz RecordType

recordSize je velikost záznamu CardSlotsStatus v bajtech.

noOfRecords je počet záznamů v sadě záznamů.

records je sada záznamů CardSlotsStatus.

2.36 **CardStructureVersion**

Kód udávající verzi implementované struktury v kartě tachografu.

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

Přiřazení hodnoty: 'aabb'H:

'aa'H Index pro změny struktury.

'00'H pro aplikace 1. generace

'01'H pro aplikace 2. generace

'bb'H Index pro změny týkající se používání datových prvků definovaných pro strukturu určenou vyšším bajtem.

'00'H pro tuto verzi aplikací 1. generace

'00'H pro tuto verzi aplikací 2. generace

2.37 **CardVehicleRecord**

Informace uložené na kartě řidiče nebo kartě dílny týkající se doby používání vozidla během kalendářního dne (požadavky 269, 294, 322 a 345 přílohy 1C).

1. generace:

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

vehicleOdometerBegin je hodnota počitadla ujetých kilometrů na začátku doby používání vozidla.

vehicleOdometerEnd je hodnota počitadla ujetých kilometrů na konci doby používání vozidla.

vehicleFirstUse je datum a čas začátku doby používání vozidla.

vehicleLastUse je datum a čas konce doby používání vozidla.

vehicleRegistration je registrační značka (VRN) a členský stát registrace vozidla.

vuDataBlockCounter je hodnota VuDataBlockCounter při poslední extrakci doby používání vozidla.

2. generace:

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

Kromě prvků 1. generace se použije tento datový prvek:

VehicleIdentificationNumber je identifikační číslo vozidla týkající se vozidla jako celku.

2.38 CardVehiclesUsed

Informace uložené na kartě řidiče nebo kartě dílny týkající vozidel použitých držitelem karty (požadavky 270, 295, 323 a 346 přílohy 1C).

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

vehiclePointerNewestRecord je index naposledy aktualizovaného záznamu o vozidle.

Přiřazení hodnoty: Číslo odpovídající čítači záznamů o vozidlech začínající hodnotou „0“ pro první výskyt záznamu o vozidle ve struktuře.

cardVehicleRecords je sada záznamů obsahující informace o použitých vozidlech.

2.39 CardVehicleUnitRecord

2. generace:

Informace uložené na kartě řidiče nebo kartě dílny týkající se celku ve vozidle, který byl použit (požadavky 303 a 351 přílohy 1C).

```
CardVehicleUnitRecord ::= SEQUENCE {
   timeStamp                           TimeReal,
   manufacturerCode                    ManufacturerCode,
   deviceID                            INTEGER(0..255),
   vuSoftwareVersion                   VuSoftwareVersion
}
```

timeStamp je začátek doby používání celku ve vozidle (tj. první vložení karty do celku ve vozidle pro dané období).

manufacturerCode označuje výrobce celku ve vozidle.

deviceID označuje typ celku ve vozidle od daného výrobce. Jedná se o hodnotu specifickou pro výrobce.

vuSoftwareVersion je číslo verze softwaru v celku ve vozidle.

2.40 CardVehicleUnitsUsed

2. generace:

Informace uložené na kartě řidiče nebo kartě dílny týkající se celků ve vozidle, které byly použity držitelem karty (požadavky 306 a 352 přílohy 1C).

```
CardVehicleUnitsUsed := SEQUENCE {
   vehicleUnitPointerNewestRecord       INTEGER(0..NoOfCardVehicleUnitRecords-1),
   cardVehicleUnitRecords               SET SIZE(NoOfCardVehicleUnitRecords) OF
                                        CardVehicleUnitRecord
}
```

vehicleUnitPointerNewestRecord je index naposledy aktualizovaného záznamu o celku ve vozidle.

Přiřazení hodnoty: Číslo odpovídající čítači záznamů o celku ve vozidle, začínající hodnotou „0“ pro první výskyt záznamů o celku ve vozidle ve struktuře.

cardVehicleUnitRecords je sada záznamů obsahující informace o použitých celcích ve vozidle.

2.41 Certificate

Certifikát veřejného klíče vydaný certifikační autoritou.

1. generace:

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

Přiřazení hodnoty: digitální podpis s částečnou obnovou CertificateContent podle dodatku 11 „Společné bezpečnostní mechanismy“: podpis (128 bajtů) || zbytek veřejného klíče (58 bajtů) || odkaz na certifikační autoritu (8 bajtů).

2. generace:

```
Certificate ::= OCTET STRING (SIZE(204..341))
```

Přiřazení hodnoty: viz dodatek 11

2.42 CertificateContent

1. generace:

(Nešifrovaný) obsah certifikátu veřejného klíče podle dodatku 11 „Společné bezpečnostní mechanismy“.

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

certificateProfileIdentifier je verze odpovídajícího certifikátu.

Přiřazení hodnoty: ‘01h’ pro tuto verzi.

certificationAuthorityReference identifikuje certifikační autoritu vydávající certifikát. Současně odkazuje na veřejný klíč této certifikační autority.

certificateHolderAuthorisation identifikuje práva držitele certifikátu.

certificateEndOfValidity je datum, kdy končí administrativní platnost certifikátu.

certificateHolderReference identifikuje držitele certifikátu. Zároveň odkazuje na jeho veřejný klíč.

publicKey je veřejný klíč, který je certifikován tímto certifikátem.

2.43 CertificateHolderAuthorisation

Identifikace práv držitele certifikátu.

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

1. generace:

tachographApplicationID je identifikátor aplikace pro aplikaci tachografu.

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

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

Přiřazení hodnoty: ve shodě s datovým typem EquipmentType. **0**, jestliže se jedná o certifikát členského státu.

2. generace:

tachographApplicationID označuje 6 nejvýznamnějších bajtů identifikátoru aplikace (AID) karty tachografu 2. generace. AID pro aplikaci karty tachografu je uveden v kapitole 6.2.

Přiřazení hodnoty: 'FF 53 4D 52 44 54'.

equipmentType je identifikace typu zařízení, jak je specifikováno pro 2. generaci, pro něž je certifikát určen.

Přiřazení hodnoty: ve shodě s datovým typem EquipmentType.

2.44 CertificateRequestID

Jednoznačná identifikace žádosti o certifikát. Může být použita také jako identifikátor veřejného klíče celku ve vozidle, jestliže výrobní číslo celku ve vozidle, pro který je klíč určen, není známo v době vystavení certifikátu.

```
CertificateRequestID ::= SEQUENCE{
   requestSerialNumber                  INTEGER(0..2^32-1),
   requestMonthYear                     BCDString(SIZE(2)),
   crIdentifier                         OCTET STRING(SIZE(1)),
   manufacturerCode                     ManufacturerCode
}
```

requestSerialNumber je sériové číslo žádosti o certifikát, jednoznačné pro výrobce a níže uvedený měsíc.

requestMonthYear je identifikace měsíce a roku žádosti o certifikát.

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

crIdentifier: je identifikátor k odlišení žádosti o certifikát od rozšířeného výrobního čísla.

Přiřazení hodnoty: 'FFh'.

manufacturerCode: je číselný kód výrobce žádajícího o certifikát.

2.45 CertificationAuthorityKID

Identifikátor veřejného klíče certifikační autority (členského státu nebo Evropského certifikačního úřadu).

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

nationNumeric je číselný kód státu certifikační autority.

nationAlpha je alfanumerický kód státu certifikační autority.

keySerialNumber je sériové číslo k odlišení různých klíčů certifikační autority v případě, že se klíče změní.

additionalInfo je dvoubajtové pole pro dodatečné kódování (specifické pro certifikační autoritu).

caIdentifier je identifikátor k odlišení identifikátoru klíče certifikační autority od jiných identifikátorů klíčů.

Přiřazení hodnoty: '01h'.

2.46 CompanyActivityData

Informace uložené na kartě podniku týkající se činností vykonaných s kartou (požadavky 373 a 379 přílohy 1C).

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

companyPointerNewestRecord je index naposledy aktualizovaného záznamu companyActivityRecord.

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

companyActivityRecords je sada všech záznamů o činnosti podniku.

companyActivityRecord je posloupnost informací vztahujících se k jedné činnosti podniku.

companyActivityType je typ činnosti podniku.

companyActivityTime je datum a čas činnosti podniku.

cardNumberInformation je číslo karty a členský stát vydávající kartu, z které jsou stažena data (v příslušných případech).

vehicleRegistrationInformation je registrační značka (VRN) a členský stát registrace vozidla, jehož data jsou stažena, zablokována nebo odblokována.

downloadPeriodBegin a **downloadPeriodEnd** je případné období, za něž byla z celku ve vozidle stažena data.

2.47 **CompanyActivityType**

Kód udávající činnost vykonávanou podnikem s použitím jeho karty podniku.

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

2.48 **CompanyCardApplicationIdentification**

Informace uložené na kartě podniku týkající se identifikace aplikace karty (požadavky 369 a 375 přílohy 1C).

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

typeOfTachographCardId udává implementovaný typ karty.

cardStructureVersion udává verzi struktury implementované v kartě.

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

2.49 **CompanyCardHolderIdentification**

Informace uložené na kartě podniku týkající se identifikace držitele karty (požadavky 372 a 378 přílohy 1C).

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

companyName je jméno podniku – držitele.

companyAddress je adresa podniku – držitele.

cardHolderPreferredLanguage je upřednostňovaný jazyk držitele karty.

2.50 **ControlCardApplicationIdentification**

Informace uložené na kontrolní kartě týkající se identifikace aplikace karty (požadavky 357 a 363 přílohy 1C).

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

typeOfTachographCardId udává implementovaný typ karty.

cardStructureVersion udává verzi struktury implementované v kartě.

noOfControlActivityRecords je počet záznamů o kontrolní činnosti, které lze na kartu uložit.

2.51 **ControlCardControlActivityData**

Informace uložené na kontrolní kartě týkající se kontrolní činnosti vykonané s kartou (požadavky 361 a 367 přílohy 1C).

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

controlPointerNewestRecord je index naposledy aktualizovaného záznamu o kontrolní činnosti.

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

controlActivityRecords je sada všech záznamů o kontrolní činnosti.

controlActivityRecord je posloupnost informací vztahujících se k jedné kontrole.

controlType je typ kontroly.

controlTime je datum a čas kontroly.

controlledCardNumber je číslo kontrolované karty a členský stát, který ji vydal.

controlledVehicleRegistration je registrační značka (VRN) a členský stát registrace vozidla, v kterém byla kontrola provedena.

controlDownloadPeriodBegin a **controlDownloadPeriodEnd** je období, za které byla případně stažena data.

2.52 **ControlCardHolderIdentification**

Informace uložené na kontrolní kartě týkající se identifikace držitele karty (požadavky 360 a 366 přílohy 1C).

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

controlBodyName je název kontrolního orgánu držitele karty.

controlBodyAddress je adresa kontrolního orgánu držitele karty.

cardHolderName je příjmení a jméno (jména) držitele kontrolní karty.

cardHolderPreferredLanguage je upřednostňovaný jazyk držitele karty.

2.53 **ControlType**

Kód udávající činnosti provedené během kontroly. Tento datový typ se vztahuje k požadavkům 126, 274, 299, 327 a 350 přílohy 1C.

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

1. generace:

Přiřazení hodnoty – oktetové uspořádání: 'cvpdxxxx'B (8 bitů)

'c'B stahování dat z karty:

'0'B: při této kontrolní činnosti nebyla stažena data z karty,

'1'B: při této kontrolní činnosti byla stažena data z karty

'v'B stahování dat z celku ve vozidle:

'0'B: při této kontrolní činnosti nebyla stažena data z celku ve vozidle,

'1'B: při této kontrolní činnosti byla stažena data z celku ve vozidle

'p'B tisk:

'0'B: při této kontrolní činnosti se netisklo,

'1'B: při této kontrolní činnosti se tisklo

'd'B zobrazení:

'0'B: při této kontrolní činnosti nebylo použito zobrazení,

'1'B: při této kontrolní činnosti bylo použito zobrazení

'xxxx'B nepoužito.

2. generace:

Přiřazení hodnoty – oktetové uspořádání: 'cvpdexxx'B (8 bitů)

'c'B stahování dat z karty:

'0'B: při této kontrolní činnosti nebyla stažena data z karty,

'1'B: při této kontrolní činnosti byla stažena data z karty

'v'B stahování dat z celku ve vozidle:

'0'B: při této kontrolní činnosti nebyla stažena data z celku ve vozidle,

'1'B: při této kontrolní činnosti byla stažena data z celku ve vozidle

'p'B tisk:

'0'B: při této kontrolní činnosti se netisklo,

'1'B: při této kontrolní činnosti se tisklo

'd'B zobrazení:

'0'B: při této kontrolní činnosti nebylo použito zobrazení,

'1'B: při této kontrolní činnosti bylo použito zobrazení

‘e’B	silniční kontrola kalibrace:
	‘0’B: při této kontrolní činnosti nebyly kontrolovány kalibrační parametry,
	‘1’B: při této kontrolní činnosti byly kontrolovány kalibrační parametry
‘xxx’B	vyhrazeno pro budoucí použití.

2.54 CurrentDateTime

Aktuální datum a čas záznamového zařízení.

```
CurrentDateTime ::= TimeReal
```

Přiřazení hodnoty: není blíže specifikováno.

2.55 CurrentDateTimeRecordArray

2. generace:

Aktuální datum a čas a metadata použitá v protokolu pro stahování.

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

recordType označuje typ záznamu (CurrentDateTime). **Přiřazení hodnoty**: viz RecordType

recordSize je velikost záznamu CurrentDateTime v bajtech.

noOfRecords je počet záznamů v sadě záznamů.

records je sada záznamů aktuálního data a času.

2.56 DailyPresenceCounter

Čítač uložený v kartě řidiče nebo kartě dílny, který se zvýší o jedničku za každý kalendářní den, kdy byla karta vložena v celku ve vozidle. Tento datový typ se vztahuje k požadavkům 266, 299, 320 a 343 přílohy 1C.

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

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

2.57 Datef

Datum vyjádřené v číselném tvaru, který lze snadno tisknout.

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

Přiřazení hodnoty:

yyyy	rok
mm	měsíc
dd	den
'00000000'H	explicitně označuje „žádné datum".

2.58 **DateOfDayDownloaded**

2. generace:

Datum a čas stahování.

```
DateOfDayDownloaded ::= TimeReal
```

Přiřazení hodnoty: není blíže specifikováno.

2.59 **DateOfDayDownloadedRecordArray**

2. generace:

Datum a čas stahování a metadata použitá v protokolu pro stahování.

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

recordType označuje typ záznamu (DateOfDayDownloaded). **Přiřazení hodnoty**: viz RecordType

recordSize je velikost záznamu CurrentDateTime v bajtech.

noOfRecords je počet záznamů v sadě záznamů.

records je sada záznamů o datu a čase stahování.

2.60 **Distance**

Ujetá vzdálenost (výsledek rozdílu mezi dvěma hodnotami počitadla ujetých kilometrů).

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

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

2.61 **DriverCardApplicationIdentification**

Informace uložené na kartě řidiče týkající se identifikace aplikace karty (požadavky 253 a 278 přílohy 1C).

1. generace:

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

typeOfTachographCardId udává implementovaný typ karty.

cardStructureVersion udává verzi struktury implementované v kartě.

noOfEventsPerType je počet událostí od každého typu události, které lze na kartu zaznamenat.

noOfFaultsPerType je počet závad od každého druhu závady, které lze na kartu zaznamenat.

activityStructureLength udává počet bajtů, které jsou k dispozici pro ukládání záznamů o činnosti.

noOfCardVehicleRecords je počet záznamů o vozidle, které může karta obsahovat.

noOfCardPlaceRecords je počet míst, která lze na kartu zaznamenat.

2. generace:

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

Kromě prvků 1. generace se používají tyto datové prvky:

noOfGNSSCDRecords je počet záznamů o nepřetržité době řízení dle GNSS, které lze na kartu uložit.

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

2.62 DriverCardHolderIdentification

Informace uložené na kartě řidiče týkající se identifikace držitele karty (požadavky 256 a 281 přílohy 1C).

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

cardHolderName je příjmení a jméno (jména) držitele karty řidiče.

cardHolderBirthDate je datum narození držitele karty řidiče.

cardHolderPreferredLanguage je upřednostňovaný jazyk držitele karty.

2.63 DSRCSecurityData

2. generace:

Nezašifrované informace a kód MAC předávané prostřednictvím DSRC z tachografu do dálkového dotazovače (RI), podrobnosti viz dodatek 11 část B kapitolu 13.

```
DSRCSecurityData ::= SEQUENCE {
   tagLenthPlainText                    OCTET STRING(SIZE(2)),
   currentDateTime                      CurrentDateTime,
   counter                              INTEGER(0..2^24-1),
   vuSerialNumber                       VuSerialNumber,
   dSRCMKVersionNumber                  INTEGER(SIZE(1)),
   tagLengthMac                         OCTET STRING(SIZE(2)),
   mac                                  MAC
}
```

tagLength je část kódování DER-TLV a je nastavena na '81 10' (viz dodatek 11 část B kapitolu 13).

currentDateTime je aktuální datum a čas celku ve vozidle.

counter je čítač zpráv RTM.

vuSerialNumber je výrobní číslo celku ve vozidle.

dSRCMKVersionNumber je číslo verze hlavního klíče DSRC, ze kterého byly odvozeny klíče DSRC specifické pro celek ve vozidle.

tagLengthMac je tag a délka datového objektu MAC jako součást kódování DER-TLV. Tag je nastaven na hodnotu '8E', délka musí kódovat délku MAC v oktetech (viz dodatek 11 část B kapitolu 13).

mac je hodnota kódu MAC vypočítaná pro zprávu RTM (viz dodatek 11 část B kapitolu 13).

2.64 EGFCertificate

2. generace:

Certifikát veřejného klíče vnějšího zařízení GNSS pro vzájemné ověření pravosti s celkem ve vozidle. Struktura tohoto certifikátu je specifikována v dodatku 11.

```
EGFCertificate ::= Certificate
```

2.65 EmbedderIcAssemblerId

Poskytuje informace o subjektu, který vkládá integrovaný obvod.

```
EmbedderIcAssemblerId ::= SEQUENCE{
   countryCode                          IA5String(SIZE(2)),
   moduleEmbedder                       BCDString(SIZE(2)),
   manufacturerInformation              OCTET STRING(SIZE(1))
}
```

countryCode je dvoupísmenný kód země subjektu, který vkládá modul, podle ISO 3166.

moduleEmbedder označuje subjekt, který vkládá modul.

manufacturerInformation slouží pro interní použití výrobcem.

2.66 EntryTypeDailyWorkPeriod

Kód k rozlišení mezi začátkem a koncem při zadání denní pracovní doby a podmínek zadání.

1. generace

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

Přiřazení hodnoty: dle ISO/IEC 8824-1.

2. generace

```
EntryTypeDailyWorkPeriod ::= INTEGER {
   Begin,  related time = card insertion time or time of entry          (0),
   End,    related time = card withdrawal time or time of entry        (1),
   Begin,  related time manually entered (start time)                  (2),
   End,    related time manually entered (end of work period)          (3),
   Begin,  related time assumed by VU                                  (4),
   End,    related time assumed by VU                                  (5),
   Begin,  related time based on GNSS data                             (6),
   End     related time based on GNSS data                             (7)
}
```

Přiřazení hodnoty: dle ISO/IEC 8824-1.

2.67 EquipmentType

Kód k rozlišení různých typů zařízení pro aplikaci tachografu.

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

1. generace:

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

Přiřazení hodnoty: dle ISO/IEC 8824-1.

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

2. generace:

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
--RFU                                    (17..255)
```

Poznámka: 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.

2.68 **EuropeanPublicKey**

1. generace:

Evropský veřejný klíč.

```
EuropeanPublicKey ::= PublicKey
```

2.69 **EventFaultRecordPurpose**

Kód vysvětlující, proč byla událost nebo závada zaznamenána.

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

Přiřazení hodnoty:

'00'H	jedna z 10 nejnovějších (nebo posledních) událostí nebo závad
'01'H	nejdelší událost v jednom z posledních 10 dnů výskytu
'02'H	jedna z 5 nejdelších událostí za posledních 365 dnů
'03'H	poslední událost v jednom z posledních 10 dnů výskytu
'04'H	nejzávažnější událost v jednom z posledních 10 dnů výskytu
'05'H	jedna z 5 nejzávažnějších událostí za posledních 365 dnů
'06'H	první událost nebo závada od poslední kalibrace
'07'H	aktivní/trvající událost nebo závada
'08'H to '7F'H	vyhrazeno pro budoucí použití
'80'H to 'FF'H	specifické pro výrobce

2.70 **EventFaultType**

Kód blíže určující událost nebo závadu.

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

Přiřazení hodnoty:

1. 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' to '0F'H	vyhrazeno pro budoucí použití,

	události pokusů o narušení zabezpečení souvisejících s celkem ve vozidle,
‘1x’H	žádné další podrobnosti,
‘10’H	chyba ověření pravosti snímače pohybu,
‘11’H	chyba ověření pravosti karty tachografu,
‘12’H	neoprávněná výměna snímače pohybu,
‘13’H	chyba integrity vstupních dat karty,
‘14’H	chyba integrity uložených uživatelských dat,
‘15’H	vnitřní chyba přenosu dat,
‘16’H	neoprávněné otevření krytu,
‘17’H	poškození technického vybavení,
‘18’H	vyhrazeno pro budoucí použití,
‘19’H to ‘1F’H	
‘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 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.

2. generace:

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

‘0B’H	časový nesoulad (GNSS vůči vnitřním hodinám VU),
‘0C’ to ‘0F’H	vyhrazeno pro budoucí použití,
‘5x’H	závady související s GNSS,
‘50’H	žádné další podrobnosti,
‘51’H	závada interního přijímače GNSS,
‘52’H	závada vnějšího přijímače GNSS,
‘53’H	závada vnější komunikace GNSS,
‘54’H	nejsou údaje GNSS poloze,
‘55’H	detekce nedovolené manipulace s GNSS,
‘56’H	skončila platnost certifikátu vnějšího zařízení GNSS,
‘57’H to ‘5F’H	vyhrazeno pro budoucí použití,
‘6x’H	závady související s modulem dálkové komunikace,
‘60’H	žádné další podrobnosti,
‘61’H	závada modulu dálkové komunikace,
‘62’H	závada komunikace s modulem dálkové komunikace,
‘63’H to ‘6F’H	vyhrazeno pro budoucí použití,
‘7x’H	závady rozhraní ITS,
‘70’H	žádné další podrobnosti,
‘71’H to ‘7F’H	vyhrazeno pro budoucí použití.

2.71 **ExtendedSealIdentifier**

2. generace:

Rozšířený identifikátor plomby jednoznačně identifikuje plombu (požadavek 401 přílohy 1C).

```
ExtendedSealIdentifier ::= SEQUENCE{
   manufacturerCode                    OCTET STRING (SIZE(2)),
   sealIdentifier                      OCTET STRING (SIZE(6))
}
```

manufacturerCode je kód výrobce plomby.

sealIdentifier je identifikátor plomby, který je jednoznačný pro výrobce.

2.72 ExtendedSerialNumber

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

1. generace:

```
ExtendedSerialNumber ::= SEQUENCE{
   serialNumber                        INTEGER(0..2^32-1),
   monthYear                           BCDString(SIZE(2)),
   type                                OCTET STRING(SIZE(1)),
   manufacturerCode                    ManufacturerCode
}
```

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

monthYear je identifikace měsíce a roku výroby (nebo přiřazení výrobního čísla).

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

type je identifikátor typu zařízení.

Přiřazení hodnoty: specifické pro výrobce, s vyhrazenou hodnotou 'FF'h.

manufacturerCode: je číselný kód výrobce typově schváleného zařízení.

2. generace:

```
ExtendedSerialNumber ::= SEQUENCE{
   serialNumber                        INTEGER(0..2^32-1),
   monthYear                           BCDString(SIZE(2)),
   type                                EquipmentType,
   manufacturerCode                    ManufacturerCode
}
```

serialNumber viz 1. generace

monthYear viz 1. generace

type je identifikátor typu zařízení

manufacturerCode: viz 1. generace.

2.73 FullCardNumber

Kód plně identifikující kartu tachografu.

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

cardType je typ karty tachografu.

cardIssuingMemberState je kód členského státu, který kartu vydal.

cardNumber je číslo karty.

2.74 FullCardNumberAndGeneration

2. generace:

Kód plně identifikující kartu tachografu a její generaci.

```
FullCardNumberAndGeneration ::= SEQUENCE {
   fullCardNumber                        FullCardNumber,
   generation                            Generation
}
```

fullcardNumber identifikuje kartu tachografu.

generation označuje generaci použité karty tachografu.

2.75 Generation

2. generace:

Označuje generaci použitého tachografu.

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

Přiřazení hodnoty:

'00'H	vyhrazeno pro budoucí použití
'01'H	1. generace
'02'H	2. generace
'03'H .. 'FF'H	vyhrazeno pro budoucí použití

2.76 GeoCoordinates

2. generace:

Zeměpisné souřadnice jsou kódovány jako celá čísla. Tato celá čísla jsou násobky kódování ±DDMM.M pro zeměpisnou šířku a ±DDDMM.M pro zeměpisnou délku. Zde ±DD případně ±DDD označuje stupně a MM.M minuty.

```
GeoCoordinates ::= SEQUENCE {
   latitude                              INTEGER(-90000..90001),
   longitude                             INTEGER(-180000..180001)
}
```

latitude je zeměpisná délka kódovaná jako desetinásobek reprezentace ±DDMM.M.

longitude je zeměpisná šířka kódovaná jako desetinásobek reprezentace ±DDDMM.M.

2.77 **GNSSAccuracy**

2. generace:

Přesnost údajů o poloze z GNSS (definice eee)). Tato přesnost je kódována jako celé číslo a je desetinásobkem hodnoty X.Y z věty GSA NMEA.

```
GNSSAccuracy ::= INTEGER(1..100)
```

2.78 **GNSSContinuousDriving**

2. generace:

Informace uložené na kartě řidiče nebo kartě dílny týkající se polohy vozidla dle GNSS, pokud nepřetržitá doba řízení řidiče dosáhne násobku tří hodin (požadavky 306 a 354 přílohy 1C).

```
GNSSContinuousDriving := SEQUENCE {
   gnssCDPointerNewestRecord            INTEGER(0..NoOfGNSSCDRecords -1),
   gnssContinuousDrivingRecords         SET SIZE(NoOfGNSSCDRecords) OF
                                        GNSSContinuousDrivingRecord
}
```

gnssCDPointerNewestRecord je index naposledy aktualizovaného záznamu o nepřetržité době řízení dle GNSS.

Přiřazení hodnoty: Číslo odpovídající čítači záznamů o nepřetržité době řízení dle GNSS, začínající hodnotou '0' pro první výskyt záznamu o nepřetržité době řízení dle GNSS ve struktuře.

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

2.79 **GNSSContinuousDrivingRecord**

2. generace:

Informace uložené na kartě řidiče nebo kartě dílny týkající se polohy vozidla dle GNSS, pokud nepřetržitá doba řízení řidiče dosáhne násobku tří hodin (požadavky 305 a 353 přílohy 1C).

```
GNSSContinuousDrivingRecord ::= SEQUENCE {
   timeStamp                            TimeReal,
   gnssPlaceRecord                      GNSSPlaceRecord
}
```

timeStamp je datum a čas, kdy nepřetržitá doba řízení držitele karty dosáhne násobku tří hodin.

gnssPlaceRecord obsahuje informace týkající se polohy vozidla.

2.80 **GNSSPlaceRecord**

2. generace:

Informace týkající se polohy vozidla dle GNSS (požadavky 108, 109, 110, 296, 305, 347 a 353 přílohy 1C).

```
GNSSPlaceRecord ::= SEQUENCE {
   timeStamp                            TimeReal,
   gnssAccuracy                         GNSSAccuracy,
   geoCoordinates                       GeoCoordinates
}
```

timeStamp je datum a čas, kdy byla určena poloha vozidla dle GNSS.

gnssAccuracy je přesnost údajů GNSS o poloze.

geoCoordinates je poloha zaznamenaná pomocí GNSS.

2.81 **HighResOdometer**

Hodnota počitadla ujetých kilometrů vozidla: celková vzdálenost ujetá vozidlem během jeho provozu.

```
HighResOdometer ::= INTEGER(0..2^32-1)
```

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

2.82 **HighResTripDistance**

Vzdálenost ujetá během cesty nebo její části.

```
HighResTripDistance ::= INTEGER(0..2^32-1)
```

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

2.83 **HolderName**

Příjmení a jméno (jména) držitele karty.

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

holderSurname je příjmení držitele. Toto příjmení neobsahuje tituly.

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

holderFirstNames jsou jméno (jména) a iniciály držitele.

2.84 **InternalGNSSReceiver**

2. generace:

Informace, zda je přijímač GNSS vnitřní nebo vnější vůči celku ve vozidle. Hodnota „true“ znamená, že přijímač GNSS je interní částí VU. Hodnota „false“ znamená, že přijímač GNSS je vnější.

```
InternalGNSSReceiver ::= BOOLEAN
```

2.85 **K-ConstantOfRecordingEquipment**

Konstanta záznamového zařízení (definice m)).

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

Přiřazení hodnoty: impulsy na kilometr v provozním rozsahu 0 až 64 255 impulsů/km.

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 nebo karty tachografu.

Druhá volba je vhodná k odkazu na veřejný klíč celku ve vozidle (pokud výrobní číslo celku ve vozidle nemůže být známé v čase generování certifikátu).

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

2.87 **KMWCKey**

2. generace:

Klíč AES a jeho příslušná verze používané pro párování celku ve vozidle se snímačem pohybu. Podrobnosti viz dodatek 11.

```
KMWCKey ::= SEQUENCE {
   kMWCKey                             AESKey,
   keyVersion                          INTEGER (SIZE(1))
}
```

kMWCKey je délka klíče AES zřetězená s klíčem, který se používá pro párování celku ve vozidle se snímačem pohybu.

keyVersion označuje verzi klíče AES.

2.88 **Language**

Kód identifikující jazyk.

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

Přiřazení hodnoty: Dvě malá písmena kódovaná dle ISO 639.

2.89 **LastCardDownload**

Datum a čas, uložené na kartě řidiče, posledního stažení dat z karty (pro jiné účely než pro kontrolu) – požadavky 257 a 282 přílohy 1C. Toto datum může být aktualizováno celkem ve vozidle nebo libovolnou čtečkou karet.

```
LastCardDownload ::= TimeReal
```

Přiřazení hodnoty: není blíže specifikováno.

2.90 **LinkCertificate**

2. generace:

Spojovací certifikát mezi páry klíčů evropského kořenového certifikačního úřadu.

```
LinkCertificate ::= Certificate
```

2.91 **L-TyreCircumference**

Účinný obvod pneumatik na kolech (definice u)).

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

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

2.92 **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(12))
}
```

2.93 **ManualInputFlag**

Kód udávající, zda držitel karty ručně zadal činnosti řidiče při vložení karty, či nikoliv (požadavek 081 přílohy 1B a požadavek 102 přílohy 1C).

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

Přiřazení hodnoty: není blíže specifikováno.

2.94 **ManufacturerCode**

Kód identifikující výrobce typově schváleného zařízení.

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

Zkušebna příslušná pro provádění zkoušek interoperability vede a zveřejňuje seznam kódů výrobců na svých webových stránkách (požadavek 454 přílohy 1C).

Kódy ManufacturerCode se předběžně přidělují vývojářům tachografových zařízení, když si podají žádost u zkušebny příslušné pro provádění zkoušek interoperability.

2.95 **ManufacturerSpecificEventFaultData**

2. generace:

Kódy chyb specifické pro výrobce zjednodušují analýzu chyb a údržbu celků ve vozidle.

```
ManufacturerSpecificEventFaultData ::= SEQUENCE {
   manufacturerCode                     ManufacturerCode,
   manufacturerSpecificErrorCode        OCTET STRING(SIZE(3))
}
```

manufacturerCode označuje výrobce celku ve vozidle.

manufacturerSpecificErrorCode je kód chyby specifický pro výrobce.

2.96 MemberStateCertificate

Certifikát veřejného klíče členského státu vydaný Evropským certifikačním úřadem.

```
MemberStateCertificate ::= Certificate
```

2.97 MemberStateCertificateRecordArray

2. generace:

Certifikát členského státu a metadata použitá v protokolu pro stahování.

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

recordType označuje typ záznamu (MemberStateCertificate). **Přiřazení hodnoty**: viz RecordType

recordSize je velikost záznamu MemberStateCertificate v bajtech.

noOfRecords je počet záznamů v sadě záznamů. Hodnota je nastavena na 1, protože certifikáty mohou mít různé délky.

records je sada certifikátů členských států.

2.98 MemberStatePublicKey

1. generace:

Veřejný klíč členského státu.

```
MemberStatePublicKey ::= PublicKey
```

2.99 Name

Název nebo jméno.

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

codePage určuje znakovou sadu definovanou v kapitole 4.

name je název nebo jméno kódované za použití určené znakové sady.

2.100 **NationAlpha**

Abecední označení země musí být v souladu s rozlišovacími značkami používanými na vozidlech v mezinárodním provozu (Vídeňská úmluva OSN o silničním provozu z roku 1968).

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

Abecední a číselné kódy zemí jsou uvedeny v seznamu vedeném na webových stránkách zkušebny příslušné pro provádění zkoušek interoperability, jak je stanoveno v požadavku 440 přílohy 1C.

2.101 **NationNumeric**

Číselné označení státu.

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

Přiřazení hodnoty: viz datový typ 2.100 (NationAlpha).

Jakákoli úprava nebo aktualizace specifikace abecedních nebo číselných kódů popsaných v předchozím odstavci se provede pouze poté, co určená zkušebna obdrží stanovisko výrobců typově schválených digitálních a inteligentních tachografových celků ve vozidle.

2.102 **NoOfCalibrationRecords**

Počet kalibračních záznamů, které lze uložit na kartu dílny.

1. generace:

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

Přiřazení hodnoty: viz dodatek 2.

2. generace:

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

Přiřazení hodnoty: viz dodatek 2.

2.103 **NoOfCalibrationsSinceDownload**

Čítač udávající počet kalibrací provedených s kartou dílny od posledního stahování (požadavky 317 a 340 přílohy 1C).

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

Přiřazení hodnoty: není specifikováno.

2.104 **NoOfCardPlaceRecords**

Počet záznamů míst, které lze uložit na kartu řidiče nebo kartu dílny.

1. generace:

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

Přiřazení hodnoty: viz dodatek 2.

2. generace:

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

Přiřazení hodnoty: viz dodatek 2.

2.105 **NoOfCardVehicleRecords**

Počet záznamů o použitých vozidlech, které lze uložit na kartu řidiče nebo kartu dílny.

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

Přiřazení hodnoty: viz dodatek 2.

2.106 **NoOfCardVehicleUnitRecords**

2. generace:

Počet záznamů o použitých celcích ve vozidle, které lze uložit na kartu řidiče nebo kartu dílny.

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

Přiřazení hodnoty: viz dodatek 2.

2.107 **NoOfCompanyActivityRecords**

Počet záznamů o činnosti podniku, které lze uložit na kartu podniku.

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

Přiřazení hodnoty: viz dodatek 2.

2.108 **NoOfControlActivityRecords**

Počet záznamů o kontrolní činnosti, které lze uložit na kontrolní kartu.

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

Přiřazení hodnoty: viz dodatek 2.

2.109 **NoOfEventsPerType**

Počet událostí od každého typu události, které lze na kartu uložit.

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

Přiřazení hodnoty: viz dodatek 2.

2.110 **NoOfFaultsPerType**

Počet závad od každého typu závady, které lze na kartu uložit.

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

Přiřazení hodnoty: viz dodatek 2.

2.111 **NoOfGNSSCDRecords**

2. generace:

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

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

Přiřazení hodnoty: viz dodatek 2.

2.112 **NoOfSpecificConditionRecords**

2. generace:

Počet záznamů o zvláštní podmínce, které lze na kartu uložit.

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

Přiřazení hodnoty: viz dodatek 2.

2.113 **OdometerShort**

Hodnota počitadla ujetých kilometrů vozidla ve zkrácené formě.

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

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

2.114 **OdometerValueMidnight**

Hodnota počitadla ujetých kilometrů vozidla k půlnoci daného dne (požadavek 090 přílohy 1B a požadavek 113 přílohy 1C).

```
OdometerValueMidnight ::= OdometerShort
```

Přiřazení hodnoty: není blíže specifikováno.

2.115 **OdometerValueMidnightRecordArray**

2. generace:

OdometerValueMidnight a metadata použitá v protokolu pro stahování.

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

recordType označuje typ záznamu (OdometerValueMidnight). **Přiřazení hodnoty**: viz RecordType

recordSize je velikost záznamu OdometerValueMidnight v bajtech.

noOfRecords je počet záznamů v sadě záznamů.

records je sada záznamů OdometerValueMidnight.

2.116 **OverspeedNumber**

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

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

Přiřazení hodnoty: 0 znamená, že nedošlo k žádnému překročení povolené rychlosti od poslední kontroly překročení povolené rychlosti, 1 znamená, že se vyskytla jedna událost překročení povolené rychlosti od poslední kontroly překročení povolené rychlosti, … 255 znamená, že se vyskytlo 255 nebo více událostí překročení povolené rychlosti od poslední kontroly překročení povolené rychlosti.

2.117 **PlaceRecord**

Informace týkající se místa, kde začíná nebo končí denní pracovní doba (požadavky 108, 271, 296, 324 a 347 přílohy 1C).

1. generace:

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

entryTime je datum a čas zadání.

entryTypeDailyWorkPeriod je typ zadání.

dailyWorkPeriodCountry je zadaná země.

dailyWorkPeriodRegion je zadaný region.

vehicleOdometerValue je hodnota počitadla ujetých kilometrů k okamžiku zadání místa.

2. generace:

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

Kromě 1. generace se používá tato komponenta:

entryGNSSPlaceRecord je zaznamenané místo a čas.

2.118 **PreviousVehicleInfo**

Informace související s předchozím vozidlem, které řidič použil, při vložení karty do celku ve vozidle (požadavek 081 přílohy 1B a požadavek 102 přílohy 1C).

1. generace:

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

vehicleRegistrationIdentification je registrační značka vozidla a členský stát registrace vozidla.

cardWithdrawalTime je datum a čas vyjmutí karty.

2. generace:

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

Kromě prvků 1. generace se použije tento datový prvek:

vuGeneration identifikuje generaci celku ve vozidle.

2.119 **PublicKey**

1. generace:

Veřejný klíč RSA.

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

rsaKeyModulus je modul páru klíčů.

rsaKeyPublicExponent je veřejný exponent páru klíčů.

2.120 **RecordType**

2. generace:

Odkaz na typ záznamu. Tento datový typ se používá v záznamu RecordArrays.

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

Přiřazení hodnoty:

'01'H	ActivityChangeInfo,
'02'H	CardSlotsStatus,
'03'H	CurrentDateTime,
'04'H	MemberStateCertificate,
'05'H	OdometerValueMidnight,
'06'H	DateOfDayDownloaded,
'07'H	SensorPaired,
'08'H	Signature,
'09'H	SpecificConditionRecord,
'0A'H	VehicleIdentificationNumber,
'0B'H	VehicleRegistrationNumber,
'0C'H	VuCalibrationRecord,
'0D'H	VuCardIWRecord,
'0E'H	VuCardRecord,
'0F'H	VuCertificate,
'10'H	VuCompanyLocksRecord,
'11'H	VuControlActivityRecord,
'12'H	VuDetailedSpeedBlock,
'13'H	VuDownloadablePeriod,
'14'H	VuDownloadActivityData,
'15'H	VuEventRecord,
'16'H	VuGNSSCDRecord,
'17'H	VuITSConsentRecord,
'18'H	VuFaultRecord,
'19'H	VuIdentification,
'1A'H	VuOverSpeedingControlData,
'1B'H	VuOverSpeedingEventRecord,
'1C'H	VuPlaceDailyWorkPeriodRecord,
'1D'H	VuTimeAdjustmentGNSSRecord,
'1E'H	VuTimeAdjustmentRecord,
'1F'H	VuPowerSupplyInterruptionRecord,
'20'H	SensorPairedRecord,
'21'H	SensorExternalGNSSCoupledRecord,
'22'H to '7F'H	vyhrazeno pro budoucí použití,
'80'H to 'FF'H	specifické pro výrobce.

2.121 **RegionAlpha**

Abecední odkaz na region uvnitř určitého státu.

```
RegionAlpha ::= IA5STRING(SIZE(3))
```

1. generace:

Přiřazení hodnoty:

```
'   '        No information available,
Spain:
'AN '        Andalucía,
'AR '        Aragón,
'AST'        Asturias,
'C  '        Cantabria,
'CAT'        Cataluña,
'CL '        Castilla-León,
'CM '        Castilla-La-Mancha,
'CV'         Valencia,
'EXT'        Extremadura,
'G  '        Galicia,
'IB '        Baleares,
'IC '        Canarias,
'LR '        La Rioja,
'M  '        Madrid,
'MU '        Murcia,
'NA '        Navarra,
'PV '        País Vasco
```

2. generace:

Kódy RegionAlpha jsou uvedeny v seznamu vedeném na webových stránkách zkušebny pověřené prováděním zkoušek interoperability.

2.122 **RegionNumeric**

Číselný odkaz na region uvnitř určitého státu.

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

1. generace:

Přiřazení hodnoty:

```
'00'H        No information available,
Spain:
'01'H        Andalucía,
'02'H        Aragón,
'03'H        Asturias,
'04'H        Cantabria,
'05'H        Cataluña,
'06'H        Castilla-León,
'07'H        Castilla-La-Mancha,
'08'H        Valencia,
'09'H        Extremadura,
'0A'H        Galicia,
'0B'H        Baleares,
'0C'H        Canarias,
'0D'H        La Rioja,
'0E'H        Madrid,
'0F'H        Murcia,
'10'H        Navarra,
'11'H        País Vasco
```

2. generace:

Kódy RegionNumeric jsou uvedeny v seznamu vedeném na webových stránkách zkušebny pověřené prováděním zkoušek interoperability.

2.123 **RemoteCommunicationModuleSerialNumber**

2. generace:

Výrobní číslo modulu dálkové komunikace.

```
RemoteCommunicationModuleSerialNumber ::= ExtendedSerialNumber
```

2.124 **RSAKeyModulus**

1. generace:

Modul páru klíčů RSA.

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

Přiřazení hodnoty: není specifikováno.

2.125 **RSAKeyPrivateExponent**

1. generace:

Soukromý exponent páru klíčů RSA.

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

Přiřazení hodnoty: není specifikováno.

2.126 **RSAKeyPublicExponent**

1. generace:

Veřejný exponent páru klíčů RSA.

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

Přiřazení hodnoty: není specifikováno.

2.127 **RtmData**

2. generace:

Definice tohoto datového typu viz dodatek 14.

2.128 **SealDataCard**

2. generace:

Tento datový typ ukládá informace o plombách, které jsou připojeny k různým částem vozidla, a je určen k uložení na kartě. Tento datový typ se vztahuje k požadavku 337 přílohy 1C.

```
SealDataCard ::= SEQUENCE {
   noOfSealRecords                        INTEGER(1..5),
   sealRecords                            SET SIZE(noOfSealRecords) OF SealRecord
}
```

noOfSealRecords je počet záznamů v sadě sealRecords.

sealRecords je sada záznamů o plombách.

2.129 **SealDataVu**

2. generace:

Tento datový typ ukládá informace o plombách, které jsou připojeny k různým částem vozidla, a je určen k uložení v celku ve vozidle.

```
SealDataVu ::= SEQUENCE SIZE(5) OF {
   sealRecords                            SealRecord
}
```

sealRecords je sada záznamů o plombách. Je-li dostupných plomb méně než 5, musí být hodnota EquipmentType ve všech nepoužitých záznamech sealRecords nastavena na 16, tj. nepoužité.

2.130 **SealRecord**

2. generace:

Tento datový typ ukládá informace o plombě, která je připojena k součásti. Tento datový typ se vztahuje k požadavku 337 přílohy 1C.

```
SealRecord ::= SEQUENCE {
   equipmentType                          EquipmentType,
   extendedSealIdentifier                 ExtendedSealIdentifier
}
```

equipmentType označuje typ zařízení, ke kterému je plomba připojena.

extendedSealIdentifier je identifikátor plomby připojené k zařízení.

2.131 **SensorApprovalNumber**

Číslo schválení typu snímače.

1. generace:

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

Přiřazení hodnoty: není specifikováno.

2. generace:

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

Přiřazení hodnoty:

Číslo schválení musí být uvedeno tak, jak bylo zveřejněno na příslušných webových stránkách Evropské komise, tj. např. včetně případných spojovníků. Číslo schválení musí být zarovnáno doleva.

2.132 **SensorExternalGNSSApprovalNumber**

2. generace:

Číslo schválení typu vnějšího zařízení GNSS.

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

Přiřazení hodnoty:

Číslo schválení musí být uvedeno tak, jak bylo zveřejněno na příslušných webových stránkách Evropské komise, tj. např. včetně případných spojovníků. Číslo schválení musí být zarovnáno doleva.

2.133 **SensorExternalGNSSCoupledRecord**

2. generace:

Informace uložené v celku ve vozidle týkající se identifikace vnějšího zařízení GNSS provázaného s celkem ve vozidle (požadavek 100 přílohy 1C).

```
SensorExternalGNSSCoupledRecord ::= SEQUENCE {
   sensorSerialNumber                  SensorGNSSSerialNumber,
   sensorApprovalNumber                SensorExternalGNSSApprovalNumber,
   sensorCouplingDate                  SensorGNSSCouplingDate
}
```

sensorSerialNumber je výrobní číslo vnějšího zařízení GNSS provázaného s celkem ve vozidle.

sensorApprovalNumber je číslo schválení tohoto vnějšího zařízení GNSS.

sensorCouplingDate je datum vazby tohoto vnějšího zařízení GNSS s celkem ve vozidle.

2.134 **SensorExternalGNSSIdentification**

2. generace:

Informace týkající se identifikace vnějšího zařízení GNSS (požadavek 98 přílohy 1C).

```
SensorExternalGNSSIdentification ::= SEQUENCE {
   sensorSerialNumber                  SensorGNSSSerialNumber,
   sensorApprovalNumber                SensorExternalGNSSApprovalNumber,
   sensorSCIdentifier                  SensorExternalGNSSSCIdentifier,
   sensorOSIdentifier                  SensorExternalGNSSOSIdentifier
}
```

sensorSerialNumber je rozšířené výrobní číslo vnějšího zařízení GNSS.

sensorApprovalNumber je číslo schválení vnějšího zařízení GNSS.

sensorSCIdentifier je identifikátor bezpečnostní komponenty vnějšího zařízení GNSS.

sensorOSIdentifier je identifikátor operačního systému vnějšího zařízení GNSS.

2.135 **SensorExternalGNSSInstallation**

2. generace:

Informace uložené ve vnějším zařízení GNSS týkající se montáže vnějšího snímače GNSS (požadavek 123 přílohy 1C).

```
SensorExternalGNSSInstallation ::= SEQUENCE {
   sensorCouplingDateFirst              SensorGNSSCouplingDate,
   firstVuApprovalNumber                VuApprovalNumber,
   firstVuSerialNumber                  VuSerialNumber,
   sensorCouplingDateCurrent            SensorGNSSCouplingDate,
   currentVuApprovalNumber              VuApprovalNumber,
   currentVUSerialNumber                VuSerialNumber
}
```

sensorCouplingDateFirst je datum první vazby vnějšího zařízení GNSS s celkem ve vozidle.

firstVuApprovalNumber je číslo schválení prvního celku ve vozidle provázaného s vnějším zařízením GNSS.

firstVuSerialNumber je výrobní číslo prvního celku ve vozidle provázaného s vnějším zařízením GNSS.

sensorCouplingDateCurrent je datum aktuální vazby vnějšího zařízení GNSS s celkem ve vozidle.

currentVuApprovalNumber je číslo schválení celku ve vozidle aktuálně provázaného s vnějším zařízením GNSS.

currentVUSerialNumber je výrobní číslo celku ve vozidle aktuálně provázaného s vnějším zařízením GNSS.

2.136 **SensorExternalGNSSOSIdentifier**

2. generace:

Identifikátor operačního systému vnějšího zařízení GNSS.

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

Přiřazení hodnoty: specifické pro výrobce.

2.137 **SensorExternalGNSSSCIdentifier**

2. generace:

Tento typ se používá např. pro identifikaci kryptografického modulu vnějšího zařízení GNSS.

Identifikátor bezpečnostní komponenty vnějšího zařízení GNSS.

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

Přiřazení hodnoty: specifické pro výrobce komponenty.

2.138 **SensorGNSSCouplingDate**

2. generace:

Datum vazby vnějšího zařízení GNSS s celkem ve vozidle.

```
SensorGNSSCouplingDate ::= TimeReal
```

Přiřazení hodnoty: není specifikováno.

2.139 **SensorGNSSSerialNumber**

2. generace:

Tento typ se používá k uložení výrobního čísla přijímače GNSS, ať už je uvnitř nebo vně celku ve vozidle.

Výrobní číslo přijímače GNSS.

```
SensorGNSSSerialNumber ::= ExtendedSerialNumber
```

2.140 **SensorIdentification**

Informace uložená ve snímači pohybu týkající se identifikace snímače pohybu (požadavek 077 přílohy 1B a požadavek 95 přílohy 1C).

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

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

sensorApprovalNumber je číslo schválení snímače pohybu.

sensorSCIdentifier je identifikátor bezpečnostní komponenty snímače pohybu.

sensorOSIdentifier je identifikátor operačního systému snímače pohybu.

2.141 **SensorInstallation**

Informace uložené ve snímači pohybu týkající se montáže snímače pohybu (požadavek 099 přílohy 1B a požadavek 122 přílohy 1C).

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

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

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

firstVuSerialNumber je výrobní číslo prvního celku ve vozidle spárovaného se snímačem pohybu.

sensorPairingDateCurrent je datum aktuálního párování snímače pohybu s celkem ve vozidle.

currentVuApprovalNumber je číslo schválení celku ve vozidle aktuálně spárovaného se snímačem pohybu.

currentVUSerialNumber je výrobní číslo celku ve vozidle aktuálně spárovaného se snímačem pohybu.

2.142 **SensorInstallationSecData**

Informace uložená na kartě dílny týkající se bezpečnostních dat potřebných pro párování snímačů pohybu s celky ve vozidlech (požadavky 308 a 331 přílohy 1C).

1. generace:

```
SensorInstallationSecData ::= TdesSessionKey
```

Přiřazení hodnoty: dle ISO 16844-3.

2. generace:

Jak je uvedeno v dodatku 11, karta dílny musí pojmout až tři klíče pro párování celku ve vozidle se snímačem pohybu. Tyto klíče mají různé verze.

```
SensorInstallationSecData ::= SEQUENCE {
   kMWCKey1                              KMWCKey,
   kMWCKey2                              KMWCKey OPTIONAL,
   kMWCKey3                              KMWCKey OPTIONAL
}
```

2.143 **SensorOSIdentifier**

Identifikátor operačního systému snímače pohybu.

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

Přiřazení hodnoty: specifické pro výrobce.

2.144 **SensorPaired**

1. generace:

Informace uložená v celku ve vozidle týkající se identifikace snímače pohybu spárovaného s celkem ve vozidle (požadavek 079 přílohy 1B).

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

sensorSerialNumber je výrobní číslo snímače pohybu aktuálně spárovaného s celkem ve vozidle.

sensorApprovalNumber je číslo schválení snímače pohybu aktuálně spárovaného s celkem ve vozidle.

sensorPairingDateFirst je datum prvního párování snímače pohybu, který je aktuálně spárován s celkem ve vozidle, s nějakým celkem ve vozidle.

2.145 **SensorPairedRecord**

2. generace:

Informace uložená v celku ve vozidle týkající se identifikace snímače pohybu spárovaného s celkem ve vozidle (požadavek 97 přílohy 1C).

```
SensorPairedRecord ::= SEQUENCE {
   sensorSerialNumber                  SensorSerialNumber,
   sensorApprovalNumber                SensorApprovalNumber,
   sensorPairingDate                   SensorPairingDate
}
```

sensorSerialNumber je výrobní číslo snímače pohybu spárovaného s celkem ve vozidle.

sensorApprovalNumber je číslo schválení tohoto snímače pohybu.

sensorPairingDate je datum spárování tohoto snímače pohybu s celkem ve vozidle.

2.146 **SensorPairingDate**

Datum spárování snímače pohybu s celkem ve vozidle.

```
SensorPairingDate ::= TimeReal
```

Přiřazení hodnoty: není specifikováno.

2.147 **SensorSCIdentifier**

Identifikátor bezpečnostní komponenty snímače pohybu.

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

Přiřazení hodnoty: specifické pro výrobce komponenty.

2.148 **SensorSerialNumber**

Výrobní číslo snímače pohybu.

```
SensorSerialNumber ::= ExtendedSerialNumber
```

2.149 **Signature**

Digitální podpis.

1. generace:

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

Přiřazení hodnoty: v souladu s dodatkem 11 „Společné bezpečnostní mechanismy“.

2. generace:

```
Signature ::= OCTET STRING (SIZE(64..132))
```

Přiřazení hodnoty: v souladu s dodatkem 11 „Společné bezpečnostní mechanismy“.

2.150 **SignatureRecordArray**

2. generace:

Sada podpisů a metadata použitá v protokolu pro stahování.

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

recordType označuje typ záznamu (Signature). **Přiřazení hodnoty**: viz RecordType

recordSize je velikost záznamu Signature v bajtech.

noOfRecords je počet záznamů v sadě záznamů. Hodnota je nastavena na 1, protože digitální podpisy mohou mít různé délky.

records je sada digitálních podpisů.

2.151 **SimilarEventsNumber**

Počet podobných událostí během daného dne (požadavek 094 přílohy 1B a požadavek 117 přílohy 1C).

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

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

2.152 **SpecificConditionRecord**

Informace uložené na kartě řidiče, kartě dílny nebo v celku ve vozidle týkající se zvláštní podmínky (požadavky 130, 276, 301, 328 a 355 přílohy 1C).

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

entryTime je datum a čas zadání.

specificConditionType je kód identifikující zvláštní podmínku.

2.153 **SpecificConditions**

Informace uložené na kartě řidiče, kartě dílny nebo v celku ve vozidle týkající se zvláštní podmínky (požadavky 131, 277, 302, 329 a 356 přílohy 1C).

2. generace:

```
SpecificConditions := SEQUENCE {
   conditionPointerNewestRecord        INTEGER(0..NoOfSpecificConditionRecords-1),
   specificConditionRecords            SET SIZE(NoOfSpecificConditionRecords) OF
                                       SpecificConditionRecord
}
```

conditionPointerNewestRecord je index naposledy aktualizovaného záznamu o zvláštní podmínce.

Přiřazení hodnoty: Číslo odpovídající čítači záznamů o zvláštní podmínce, začínající hodnotou '0' pro první výskyt záznamu o zvláštní podmínce ve struktuře.

specificConditionRecords je sada záznamů obsahujících informace o zaznamenaných zvláštních podmínkách.

2.154 **SpecificConditionType**

Kód identifikující zvláštní podmínku (požadavky 050b, 105a, 212a a 230a přílohy 1B a požadavek 62 přílohy 1C).

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

1. generace:

Přiřazení hodnoty:

'00'H	vyhrazeno pro budoucí použití
'01'H	mimo působnost – začátek
'02'H	mimo působnost – konec
'03'H	převoz lodí / převoz vlakem
'04'H .. 'FF'H	vyhrazeno pro budoucí použití

2. generace:

Přiřazení hodnoty:

'00'H	vyhrazeno pro budoucí použití
'01'H	mimo působnost – začátek
'02'H	mimo působnost – konec
'03'H	převoz lodí / převoz vlakem – začátek
'04'H	převoz lodí / převoz vlakem – konec
'05'H .. 'FF'H	vyhrazeno pro budoucí použití

2.155 **Speed**

Rychlost vozidla (km/h).

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

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

2.156 **SpeedAuthorised**

Maximální dovolená rychlost vozidla (definice hh)).

```
SpeedAuthorised ::= Speed
```

2.157 **SpeedAverage**

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

```
SpeedAverage ::= Speed
```

2.158 **SpeedMax**

Nejvyšší naměřená rychlost v dříve určené době trvání.

```
SpeedMax ::= Speed
```

2.159 **TachographPayload**

2. generace:

Definice tohoto datového typu viz dodatek 14.

2.160 **TachographPayloadEncrypted**

2. generace:

Šifrovaná přenášená data tachografu v kódování DER-TLV, tj. data odeslaná šifrovaně ve zprávě RTM. Šifrování viz dodatek 11 část B kapitolu 13.

```
TachographPayloadEncrypted ::= SEQUENCE {
   tag                                  OCTET STRING(SIZE(1)),
   length                               OCTET STRING(SIZE(1..2)),
   paddingContentIndicatorByte          OCTET STRING(SIZE(1)),
   encryptedData                        OCTET STRING(SIZE(16..192))
}
```

tag je část kódování DER-TLV a musí být nastaven na '87' (viz dodatek 11 část B kapitolu 13).

length je část kódování DER-TLV a musí kódovat délku následujících prvků paddingContentIndicatorByte a encryptedData.

paddingContentIndicatorByte musí být nastaven na '00'.

encryptedData jsou přenášená data tachographPayload šifrovaná podle dodatku 11 části B kapitoly 13. Délka těchto dat v oktetech musí být vždy násobkem 16.

2.161 **TDesSessionKey**

1. generace:

Klíč Triple-DES relace.

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

Přiřazení hodnoty: není blíže specifikováno.

2.162 **TimeReal**

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

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

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

Nejvyšší možný údaj data/času je v roce 2106.

2.163 **TyreSize**

Označení rozměrů pneumatik.

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

Přiřazení hodnoty: podle směrnice 92/23/EHS (Úř. věst. L 129, 31.3.1992, s. 95).

2.164 **VehicleIdentificationNumber**

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

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

Přiřazení hodnoty: podle ISO 3779.

2.165 **VehicleIdentificationNumberRecordArray**

2. generace:

Identifikační číslo vozidla a metadata použitá v protokolu pro stahování.

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

recordType označuje typ záznamu (VehicleIdentificationNumber). **Přiřazení hodnoty**: viz RecordType

recordSize je velikost záznamu VehicleIdentificationNumber v bajtech.

noOfRecords je počet záznamů v sadě záznamů.

records je sada identifikačních čísel vozidla.

2.166 **VehicleRegistrationIdentification**

Jednoznačná identifikace vozidla v Evropě (VRN a členský stát).

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

vehicleRegistrationNation je stát, ve kterém je vozidlo registrováno.

vehicleRegistrationNumber je registrační značka vozidla (VRN).

2.167 **VehicleRegistrationNumber**

Registrační značka vozidla (VRN). Registrační značka je přidělena orgánem registrujícím vozidlo.

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

codePage určuje znakovou sadu definovanou v kapitole 4.

vehicleRegNumber je registrační značka vozidla (VRN) kódovaná s použitím určené znakové sady.

Přiřazení hodnoty: specifické pro stát.

2.168 **VehicleRegistrationNumberRecordArray**

2. generace:

Registrační značka vozidla a metadata použitá v protokolu pro stahování.

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

recordType označuje typ záznamu (VehicleRegistrationNumber). **Přiřazení hodnoty**: viz RecordType

recordSize je velikost záznamu VehicleRegistrationNumber v bajtech.

noOfRecords je počet záznamů v sadě záznamů.

records je sada registračních značek vozidla.

2.169 **VuAbility**

2. generace:

Informace uložená v celku ve vozidle a týkající se schopnosti celku ve vozidle používat karty tachografu 1. generace (požadavek 121 přílohy 1C).

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

Přiřazení hodnoty – oktetové uspořádání: 'xxxxxxxa'B (8 bitů)

Pro schopnost podporovat 1. generaci:

'a'B Schopnost podporovat karty tachografu 1. generace:

'0'B 1. generace je podporována,

'1'B 1. generace není podporována,

'xxxxxxx'B vyhrazeno pro budoucí použití

2.170 **VuActivityDailyData**

1. generace:

Informace uložené v celku ve vozidle související se změnami činnosti a/nebo změnami statusu řízení a/nebo změnami statusu karty pro daný kalendářní den (požadavek 084 přílohy 1B a požadavky 105, 106 a 107 přílohy 1C) a se stavem otvorů pro kartu v 00.00 daného dne.

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

noOfActivityChanges je počet slov ActivityChangeInfo v sadě activityChangeInfos.

activityChangeInfos je sada slov ActivityChangeInfo uložených v celku ve vozidle pro daný den. Vždy obsahuje dvě slova ActivityChangeInfo udávající status dvou otvorů pro kartu v 00.00 daného dne.

2.171 **VuActivityDailyRecordArray**

2. generace:

Informace uložené v celku ve vozidle související se změnami činnosti a/nebo změnami statusu řízení a/nebo změnami statusu karty pro daný kalendářní den (požadavky 105, 106 a 107 přílohy 1C) a se stavem otvorů pro kartu v 00.00 daného dne.

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

recordType označuje typ záznamu (ActivityChangeInfo). **Přiřazení hodnoty**: viz RecordType

recordSize je velikost záznamu ActivityChangeInfo v bajtech.

noOfRecords je počet záznamů v sadě záznamů.

records je sada slov ActivityChangeInfo uložených v celku ve vozidle pro daný den. Vždy obsahuje dvě slova ActivityChangeInfo udávající status dvou otvorů pro kartu v 00.00 daného dne.

2.172 **VuApprovalNumber**

Číslo schválení typu celku ve vozidle.

1. generace:

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

Přiřazení hodnoty: není specifikováno.

2. generace:

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

Přiřazení hodnoty:

Číslo schválení musí být uvedeno tak, jak bylo zveřejněno na příslušných webových stránkách Evropské komise, tj. např. včetně případných spojovníků. Číslo schválení musí být zarovnáno doleva.

2.173 **VuCalibrationData**

1. generace:

Informace uložené v celku ve vozidle týkající se kalibrací záznamového zařízení (požadavek 098 přílohy 1B).

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

noOfVuCalibrationRecords je počet záznamů obsažených v sadě vuCalibrationRecords.

vuCalibrationRecords je sada kalibračních záznamů.

2.174 **VuCalibrationRecord**

Informace uložené v celku ve vozidle týkající se kalibrace záznamového zařízení (požadavek 098 přílohy 1B a požadavky 119 a 120 přílohy 1C).

1. generace:

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

calibrationPurpose je účel kalibrace.

workshopName, workshopAddress jsou název dílny a její adresa.

workshopCardNumber identifikuje kartu dílny použitou při kalibraci.

workshopCardExpiryDate je datum konce platnosti karty.

vehicleIdentificationNumber je identifikační číslo vozidla (VIN).

vehicleRegistrationIdentification obsahuje registrační značku (VRN) a členský stát registrace vozidla.

wVehicleCharacteristicConstant je charakteristický koeficient vozidla.

kConstantOfRecordingEquipment je konstanta záznamového zařízení.

lTyreCircumference je účinný obvod pneumatik na kolech.

tyreSize je označení rozměrů pneumatik namontovaných na vozidle.

authorisedSpeed je dovolená rychlost vozidla.

oldOdometerValue, newOdometerValue jsou stará a nová hodnota počitadla ujetých kilometrů.

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

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

2. generace:

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

Kromě prvků 1. generace se použije tento datový prvek:

sealDataVu uvádí informace o plombách, které jsou připojeny k různým částem vozidla.

2.175 **VuCalibrationRecordArray**

2. generace:

Informace uložené v celku ve vozidle týkající kalibrací záznamového zařízení (požadavky 119 a 120 přílohy 1C).

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

recordType označuje typ záznamu (VuCalibrationRecord). **Přiřazení hodnoty**: viz RecordType

recordSize je velikost záznamu VuCalibrationRecord v bajtech.

noOfRecords je počet záznamů v sadě záznamů.

records je sada kalibračních záznamů.

2.176 **VuCardIWData**

1. generace:

Informace uložené v celku ve vozidle týkající se cyklů vložení a vyjmutí karty řidiče nebo karty dílny do/z celku ve vozidle (požadavek 081 přílohy 1B a požadavek 103 přílohy 1C).

```
VuCardIWData ::= SEQUENCE {
   noOfIWRecords                       INTEGER(0..2^16-1),
   vuCardIWRecords                     SET SIZE(noOfIWRecords) OF VuCardIWRecord
}
```

noOfIWRecords je počet záznamů v sadě vuCardIWRecords.

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

2.177 **VuCardIWRecord**

Informace uložené v celku ve vozidle týkající se cyklů vložení a vyjmutí karty řidiče nebo karty dílny do/z celku ve vozidle (požadavek 081 přílohy 1B a požadavek 102 přílohy 1C).

1. generace:

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

cardHolderName je příjmení a jméno (jména) držitele karty řidiče nebo karty dílny ve tvaru, jak jsou uložena na kartě.

fullCardNumber je typ karty, členský stát, který ji vystavil, a její číslo ve tvaru, jak jsou uložené na kartě.

cardExpiryDate je datum konce platnosti karty ve tvaru, jak je uloženo na kartě.

cardInsertionTime je datum a čas vložení karty.

vehicleOdometerValueAtInsertion je hodnota počitadla ujetých kilometrů při vložení karty.

cardSlotNumber je otvor pro kartu, ve kterém je karta vložena.

cardWithdrawalTime je datum a čas vyjmutí karty.

vehicleOdometerValueAtWithdrawal je hodnota počitadla ujetých kilometrů při vyjmutí karty.

previousVehicleInfo obsahuje informaci o předchozím vozidle, které řidič použil, ve tvaru, jak je uložena na kartě.

manualInputFlag je příznak udávající, zda držitel karty při jejím vložení ručně zadal činnosti řidiče.

2. generace:

```
VuCardIWRecord ::= SEQUENCE {
   cardHolderName                         HolderName,
   fullCardNumberAndGeneration            FullCardNumberAndGeneration,
   cardExpiryDate                         TimeReal,
   cardInsertionTime                      TimeReal,
   vehicleOdometerValueAtInsertion        OdometerShort,
   cardSlotNumber                         CardSlotNumber,
   cardWithdrawalTime                     TimeReal,
   vehicleOdometerValueAtWithdrawal       OdometerShort,
   previousVehicleInfo                    PreviousVehicleInfo,
   manualInputFlag                        ManualInputFlag
}
```

Místo prvku fullCardNumber používá struktura dat 2. generace následující datový prvek.

fullCardNumberAndGeneration je typ karty, členský stát, který ji vydal, její číslo a generace, jak jsou na kartě uloženy.

2.178 VuCardIWRecordArray

2. generace:

Informace uložené v celku ve vozidle týkající se cyklů vložení a vyjmutí karet řidiče nebo karet dílny z/do celku ve vozidle (požadavek 103 přílohy 1C).

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

recordType označuje typ záznamu (VuCardIWRecord). **Přiřazení hodnoty**: viz RecordType

recordSize je velikost záznamu VuCardIWRecord v bajtech.

noOfRecords je počet záznamů v sadě záznamů.

records je sada záznamů týkajících se cyklů vložení a vyjmutí karty.

2.179 VuCardRecord

2. generace:

Informace uložené v celku ve vozidle o použité kartě tachografu (požadavek 132 přílohy 1C).

```
VuCardRecord ::= SEQUENCE {
   cardExtendedSerialNumber            ExtendedSerialNumber,
   cardPersonaliserID                  OCTET STRING(SIZE(1)),
   typeofTachographCardID              EquipmentType,
   cardStructureVersion                CardStructureVersion,
   cardNumber                          CardNumber
}
```

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

cardPersonaliserID se načte ze souboru EF_ICC pod MF karty.

typeOfTachographCardId se načte ze souboru EF_Application_Identification pod DF_Tachograph_G2.

cardStructureVersion se načte ze souboru EF_Application_Identification pod DF_Tachograph_G2.

cardNumber se načte ze souboru EF_Identification pod DF_Tachograph_G2.

2.180 **VuCardRecordArray**

2. generace:

Informace uložené v celku ve vozidle o kartách tachografu použitých s tímto celkem ve vozidle. Tyto informace jsou určeny pro analýzu problémů s celkem ve vozidle a kartou (požadavek 132 přílohy 1C).

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

recordType označuje typ záznamu (VuCardRecord). **Přiřazení hodnoty**: viz RecordType

recordSize je velikost záznamu VuCardRecord v bajtech.

noOfRecords je počet záznamů v sadě záznamů.

records je sada záznamů týkajících se karet tachografu použitých s celkem ve vozidle.

2.181 **VuCertificate**

Certifikát veřejného klíče celku ve vozidle.

```
VuCertificate ::= Certificate
```

2.182 **VuCertificateRecordArray**

2. generace:

Certifikát celku ve vozidle a metadata použitá v protokolu pro stahování.

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

recordType označuje typ záznamu (VuCertificate). **Přiřazení hodnoty**: viz RecordType

recordSize je velikost záznamu VuCertificate v bajtech.

noOfRecords je počet záznamů v sadě záznamů. Hodnota je nastavena na 1, protože certifikáty mohou mít různé délky.

records je sada certifikátů celků ve vozidle.

2.183 **VuCompanyLocksData**

1. generace:

Informace uložené v celku ve vozidle týkající se zámků podniku (požadavek 104 přílohy 1B).

```
VuCompanyLocksData ::= SEQUENCE {
   noOfLocks                          INTEGER(0..255),
   vuCompanyLocksRecords              SET SIZE(noOfLocks) OF VuCompanyLocksRecord
}
```

noOfLocks je počet zámků uvedených v sadě vuCompanyLocksRecords.

vuCompanyLocksRecords je sada záznamů zámků podniku.

2.184 **VuCompanyLocksRecord**

Informace uložená v celku ve vozidle týkající se jednoho zámku podniku (požadavek 104 přílohy 1B a požadavek 128 přílohy 1C).

1. generace:

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

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

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

companyCardNumber identifikuje kartu použitou při zamčení zámku.

2. generace:

```
VuCompanyLocksRecord ::= SEQUENCE {
   lockInTime                         TimeReal,
   lockOutTime                        TimeReal,
   companyName                        Name,
   companyAddress                     Address,
   companyCardNumberAndGeneration     FullCardNumberAndGeneration
}
```

Místo prvku companyCardNumber používá struktura dat 2. generace následující datový prvek.

companyCardNumberAndGeneration identifikuje kartu použitou při zamčení zámku včetně její generace.

2.185 **VuCompanyLocksRecordArray**

2. generace:

Informace uložené v celku ve vozidle týkající se zámků podniku (požadavek 128 přílohy 1C).

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

recordType označuje typ záznamu (VuCompanyLocksRecord). **Přiřazení hodnoty**: viz RecordType

recordSize je velikost záznamu VuCompanyLocksRecord v bajtech.

noOfRecords je počet záznamů v sadě záznamů. Hodnota 0..255.

records je sada záznamů zámků podniku.

2.186 **VuControlActivityData**

1. generace:

Informace uložené v celku ve vozidle týkající se kontrol provedených s použitím tohoto celku ve vozidle (požadavek 102 přílohy 1B).

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

noOfControls je počet kontrol uvedených v sadě vuControlActivityRecords.

vuControlActivityRecords je sada záznamů o kontrolních činnostech.

2.187 **VuControlActivityRecord**

Informace uložené v celku ve vozidle týkající se kontroly provedené s použitím tohoto celku ve vozidle (požadavek 102 přílohy 1B a požadavek 126 přílohy 1C).

1. generace:

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

controlType je typ kontroly.

controlTime je datum a čas kontroly.

controlCardNumber identifikuje kontrolní kartu použitou při kontrole.

downloadPeriodBeginTime je začátek staženého období, pokud jsou stahována data.

downloadPeriodEndTime je konec staženého období, pokud jsou stahována data.

2. generace:

```
VuControlActivityRecord ::= SEQUENCE {
   controlType                          ControlType,
   controlTime                          TimeReal,
   controlCardNumberAndGeneration       FullCardNumberAndGeneration,
   downloadPeriodBeginTime              TimeReal,
   downloadPeriodEndTime                TimeReal
}
```

Místo prvku controlCardNumber používá struktura dat 2. generace následující datový prvek.

controlCardNumberAndGeneration identifikuje kontrolní kartu použitou pro kontrolu včetně její generace.

2.188 VuControlActivityRecordArray

2. generace:

Informace uložené v celku ve vozidle týkající se kontrol provedených s použitím tohoto celku ve vozidle (požadavek 126 přílohy 1C).

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

recordType označuje typ záznamu (VuControlActivityRecord). **Přiřazení hodnoty**: viz RecordType

recordSize je velikost záznamu VuControlActivityRecord v bajtech.

noOfRecords je počet záznamů v sadě záznamů.

records je sada záznamů o kontrolních činnostech provedených s celkem ve vozidle.

2.189 VuDataBlockCounter

Čítač uložený na kartě identifikující postupně cykly vkládání a vyjímání karty z/do celků ve vozidle.

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

Přiřazení hodnoty: pořadové číslo s max. hodnotou 9 999, po níž začíná opět hodnotou 0.

2.190 VuDetailedSpeedBlock

Informace uložené v celku ve vozidle týkající se podrobností o rychlosti vozidla během jedné minuty, kdy se vozidlo pohybovalo (požadavek 093 přílohy 1B a požadavek 116 přílohy 1C).

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

speedBlockBeginDate je datum a čas první hodnoty rychlosti v rámci bloku.

speedsPerSecond je chronologická posloupnost naměřených rychlostí každou sekundu během minuty začínající v okamžiku speedBlockBeginDate (včetně).

2.191 **VuDetailedSpeedBlockRecordArray**

2. generace:

Informace uložené v celku ve vozidle týkající se podrobností o rychlosti vozidla.

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

recordType označuje typ záznamu (VuDetailedSpeedBlock). **Přiřazení hodnoty**: viz RecordType

recordSize je velikost záznamu VuDetailedSpeedBlock v bajtech.

noOfRecords je počet záznamů v sadě záznamů.

records je sada bloků podrobností o rychlosti.

2.192 **VuDetailedSpeedData**

1. generace:

Informace uložené v celku ve vozidle týkající se podrobností o rychlosti vozidla.

```
VuDetailedSpeedData ::= SEQUENCE {
   noOfSpeedBlocks                     INTEGER(0..2^16-1),
   vuDetailedSpeedBlocks               SET SIZE(noOfSpeedBlocks) OF
                                       VuDetailedSpeedBlock
}
```

noOfSpeedBlocks je počet bloků o rychlosti v sadě vuDetailedSpeedBlocks.

vuDetailedSpeedBlocks je sada bloků s podrobnostmi o rychlosti.

2.193 **VuDownloadablePeriod**

Nejstarší a nejnovější datum, pro které celek ve vozidle uchovává údaje týkající se činností řidičů (požadavky 081, 084 nebo 087 přílohy 1B a požadavky 102, 105 a 108 přílohy 1C).

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

minDownloadableTime je datum a čas nejstaršího záznamu o vložení karty, změně činnosti nebo zadání místa, který je uložen v celku ve vozidle.

maxDownloadableTime je datum a čas nejnovějšího záznamu o vyjmutí karty, změně činnosti nebo zadání místa, který je uložen v celku ve vozidle.

2.194 **VuDownloadablePeriodRecordArray**

2. generace:

VUDownloadablePeriod a metadata použitá v protokolu pro stahování.

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

recordType označuje typ záznamu (VuDownloadablePeriod). **Přiřazení hodnoty**: viz RecordType

recordSize je velikost záznamu VuDownloadablePeriod v bajtech.

noOfRecords je počet záznamů v sadě záznamů.

records je sada záznamů VuDownloadablePeriod.

2.195 **VuDownloadActivityData**

Informace uložené v celku ve vozidle týkající se posledního stažení dat z něj (požadavek 105 přílohy 1B a požadavek 129 přílohy 1C).

1. generace:

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

downloadingTime je datum a čas stažení dat.

fullCardNumber identifikuje kartu použitou k autorizaci stahování.

companyOrWorkshopName je název podniku nebo dílny.

2. generace:

```
VuDownloadActivityData ::= SEQUENCE {
   downloadingTime                     TimeReal,
   fullCardNumberAndGeneration         FullCardNumberAndGeneration,
   companyOrWorkshopName               Name
}
```

Místo prvku fullCardNumber používá struktura dat 2. generace následující datový prvek.

fullCardNumberAndGeneration identifikuje kartu použitou k autorizaci stahování, včetně její generace.

2.196 **VuDownloadActivityDataRecordArray**

2. generace:

Informace týkající se posledního stažení dat z celku ve vozidle (požadavek 129 přílohy 1C).

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

recordType označuje typ záznamu (VuDownloadActivityData). **Přiřazení hodnoty**: viz RecordType

recordSize je velikost záznamu VuDownloadActivityData v bajtech.

noOfRecords je počet záznamů v sadě záznamů.

records je sada datových záznamů o provedených staženích.

2.197 **VuEventData**

1. generace:

Informace uložené v celku ve vozidle týkající se událostí (požadavek 094 přílohy 1B kromě událostí překročení povolené rychlosti).

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

noOfVuEvents je počet událostí uvedených v sadě vuEventRecords.

vuEventRecords je sada záznamů o událostech.

2.198 **VuEventRecord**

Informace uložené v celku ve vozidle týkající se události (požadavek 094 přílohy 1B a požadavek 117 přílohy 1C kromě událostí překročení povolené rychlosti).

1. generace:

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

eventType je typ události.

eventRecordPurpose je účel, pro který byla tato událost zaznamenána.

eventBeginTime je datum a čas začátku události.

eventEndTime je datum a čas konce události.

cardNumberDriverSlotBegin identifikuje kartu vloženou v otvoru pro kartu řidiče na začátku události.

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

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

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

similarEventsNumber je počet podobných událostí v daný den.

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

2. generace:

```
VuEventRecord ::= SEQUENCE {
   eventType                              EventFaultType,
   eventRecordPurpose                     EventFaultRecordPurpose,
   eventBeginTime                         TimeReal,
   eventEndTime                           TimeReal,
   cardNumberAndGenDriverSlotBegin        FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotBegin      FullCardNumberAndGeneration,
   cardNumberAndGenDriverSlotEnd          FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotEnd        FullCardNumberAndGeneration,
   similarEventsNumber                    SimilarEventsNumber,
   manufacturerSpecificEventFaultData   ManufacturerSpecificEventFaultData
}
```

Kromě prvků 1. generace se používají tyto datové prvky:

manufacturerSpecificEventFaultData obsahuje dodatečné informace o události, které jsou specifické pro výrobce.

Místo prvků cardNumberDriverSlotBegin, cardNumberCodriverSlotBegin, cardNumberDriverSlotEnd a cardNumberCodriverSlotEnd používá struktura dat 2. generace následující datové prvky:

cardNumberAndGenDriverSlotBegin identifikuje kartu vloženou v otvoru pro kartu řidiče na začátku události, včetně její generace.

cardNumberAndGenCodriverSlotBegin identifikuje kartu vloženou v otvoru pro kartu druhého řidiče na začátku události, včetně její generace.

cardNumberAndGenDriverSlotEnd identifikuje kartu vloženou v otvoru pro kartu řidiče na konci události, včetně její generace.

cardNumberAndGenCodriverSlotEnd identifikuje kartu vloženou v otvoru pro kartu druhého řidiče na konci události, včetně její generace.

Je-li událost časovým nesouladem, interpretují se eventBeginTime a eventEndTime takto:

eventBeginTime je datum a čas záznamového zařízení.

eventEndTime je datum a čas GNSS.

2.199 **VuEventRecordArray**

2. generace:

Informace uložené v celku ve vozidle týkající se událostí (požadavek 117 přílohy 1C kromě událostí překročení povolené rychlosti).

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

recordType označuje typ záznamu (VuEventRecord). **Přiřazení hodnoty**: viz RecordType

recordSize je velikost záznamu VuEventRecord v bajtech.

noOfRecords je počet záznamů v sadě záznamů.

records je sada záznamů o událostech.

2.200 **VuFaultData**

1. generace:

Informace uložené v celku ve vozidle týkající se závad (požadavek 096 přílohy 1B).

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

noOfVuFaults je počet závad uvedených v sadě vuFaultRecords.

vuFaultRecords je sada záznamů o závadách.

2.201 **VuFaultRecord**

Informace uložené v celku ve vozidle týkající se závady (požadavek 096 přílohy 1B a požadavek 118 přílohy 1C).

1. generace:

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

faultType je typ závady záznamového zařízení.

faultRecordPurpose je účel, pro který byla tato závada zaznamenána.

faultBeginTime je datum a čas začátku závady.

faultEndTime je datum a čas konce závady.

cardNumberDriverSlotBegin identifikuje kartu vloženou v otvoru pro kartu řidiče na začátku závady.

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

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

cardNumberCodriverSlotEnd identifikuje kartu vloženou v otvoru pro kartu druhého řidiče na konci závady.

2. generace:

```
VuFaultRecord ::= SEQUENCE {
   faultType                              EventFaultType,
   faultRecordPurpose                     EventFaultRecordPurpose,
   faultBeginTime                         TimeReal,
   faultEndTime                           TimeReal,
   cardNumberAndGenDriverSlotBegin        FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotBegin      FullCardNumberAndGeneration,
   cardNumberAndGenDriverSlotEnd          FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotEnd        FullCardNumberAndGeneration,
   manufacturerSpecificEventFaultData   ManufacturerSpecificEventFaultData
}
```

Kromě prvků 1. generace se použije tento datový prvek:

manufacturerSpecificEventFaultData obsahuje dodatečné informace o závadě, které jsou specifické pro výrobce.

Místo prvků cardNumberDriverSlotBegin, cardNumberCodriverSlotBegin, cardNumberDriverSlotEnd a cardNumberCodriverSlotEnd používá struktura dat 2. generace následující datové prvky:

cardNumberAndGenDriverSlotBegin identifikuje kartu vloženou v otvoru pro kartu řidiče na začátku závady, včetně její generace.

cardNumberAndGenCodriverSlotBegin identifikuje kartu vloženou v otvoru pro kartu druhého řidiče na začátku závady, včetně její generace.

cardNumberAndGenDriverSlotEnd identifikuje kartu vloženou v otvoru pro kartu řidiče na konci závady, včetně její generace.

cardNumberAndGenCodriverSlotEnd identifikuje kartu vloženou v otvoru pro kartu druhého řidiče na konci závady, včetně její generace.

2.202 **VuFaultRecordArray**

2. generace:

Informace uložené v celku ve vozidle týkající se závad (požadavek 118 přílohy 1C).

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

recordType označuje typ záznamu (VuFaultRecord). **Přiřazení hodnoty**: viz RecordType

recordSize je velikost záznamu VuFaultRecord v bajtech.

noOfRecords je počet záznamů v sadě záznamů.

records je sada záznamů o závadách.

2.203 **VuGNSSCDRecord**

2. generace:

Informace uložené v celku ve vozidle týkající se polohy vozidla dle GNSS, pokud nepřetržitá doba řízení řidiče dosáhne násobku tří hodin (požadavky 108 a 110 přílohy 1C).

```
VuGNSSCDRecord ::= SEQUENCE {
   timeStamp                              TimeReal,
   cardNumberAndGenDriverSlot             FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlot           FullCardNumberAndGeneration,
   gnssPlaceRecord                        GNSSPlaceRecord
}
```

timeStamp je datum a čas, kdy nepřetržitá doba řízení držitele karty 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.

2.204 **VuGNSSCDRecordArray**

2. generace:

Informace uložené v celku ve vozidle týkající se polohy vozidla dle GNSS, pokud nepřetržitá doba řízení řidiče dosáhne násobku tří hodin (požadavek 108 a 110 přílohy 1C).

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

recordType označuje typ záznamu (VuGNSSCDRecord). **Přiřazení hodnoty**: viz RecordType

recordSize je velikost záznamu VuGNSSCDRecord v bajtech.

noOfRecords je počet záznamů v sadě záznamů.

records je sada záznamů o nepřetržité době řízení dle GNSS.

2.205 **VuIdentification**

Informace uložené v celku ve vozidle týkající se identifikace celku ve vozidle (požadavek 075 přílohy 1B a požadavky 93 a 121 přílohy 1C).

1. generace:

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

vuManufacturerName je název výrobce celku ve vozidle.

vuManufacturerAddress je adresa výrobce celku ve vozidle.

vuPartNumber je katalogové číslo dílu celku ve vozidle.

vuSerialNumber je výrobní číslo celku ve vozidle.

vuSoftwareIdentification identifikuje software implementovaný v celku ve vozidle.

vuManufacturingDate je datum výroby celku ve vozidle.

vuApprovalNumber je číslo schválení typu celku ve vozidle.

2. generace:

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

Kromě prvků 1. generace se používají tyto datové prvky:

vuGeneration identifikuje generaci celku ve vozidle.

vuAbility poskytuje informaci, zda celek ve vozidle podporuje karty tachografu 1. generace, či nikoli.

2.206 VuIdentificationRecordArray

2. generace:

VuIdentification a metadata použitá v protokolu pro stahování.

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

recordType označuje typ záznamu (VuIdentification). **Přiřazení hodnoty**: viz RecordType

recordSize je velikost záznamu VuIdentification v bajtech.

noOfRecords je počet záznamů v sadě záznamů.

records je sada záznamů VuIdentification.

2.207 VuITSConsentRecord

2. generace:

Informace uložené v celku ve vozidle týkající se souhlasu řidiče s používáním inteligentních dopravních systémů.

```
VuITSConsentRecord ::= SEQUENCE {
   cardNumberAndGen                    FullCardNumberAndGeneration,
   consent                             BOOLEAN
}
```

cardNumberAndGen identifikuje kartu včetně její generace. Musí se jednat o kartu řidiče nebo kartu dílny.

consent je příznak, který uvádí, zda řidič souhlasil s používáním inteligentních dopravních systémů ve spojitosti s tímto vozidlem / celkem ve vozidle.

Přiřazení hodnoty:

TRUE označuje souhlas řidiče s používáním inteligentních dopravních systémů

FALSE označuje nesouhlas řidiče s používáním inteligentních dopravních systémů

2.208 **VuITSConsentRecordArray**

2. generace:

Informace uložené v celku ve vozidle týkající se souhlasu řidiče s používáním inteligentních dopravních systémů (požadavek 200 přílohy 1C).

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

recordType označuje typ záznamu (VuITSConsentRecord). **Přiřazení hodnoty**: viz RecordType

recordSize je velikost záznamu VuITSConsentRecord v bajtech.

noOfRecords je počet záznamů v sadě záznamů.

records je sada záznamů o souhlasu s používáním ITS.

2.209 **VuManufacturerAddress**

Adresa výrobce celku ve vozidle.

```
VuManufacturerAddress ::= Address
```

Přiřazení hodnoty: není specifikováno.

2.210 **VuManufacturerName**

Název výrobce celku ve vozidle.

```
VuManufacturerName ::= Name
```

Přiřazení hodnoty: není specifikováno.

2.211 **VuManufacturingDate**

Datum výroby celku ve vozidle.

```
VuManufacturingDate ::= TimeReal
```

Přiřazení hodnoty: není specifikováno.

2.212 **VuOverSpeedingControlData**

Informace uložené v celku ve vozidle týkající se událostí překročení povolené rychlosti od poslední kontroly překročení povolené rychlosti (požadavek 095 přílohy 1B a požadavek 117 přílohy 1C).

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

lastOverspeedControlTime je datum a čas poslední kontroly překročení povolené rychlosti.

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

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

2.213 **VuOverSpeedingControlDataRecordArray**

2. generace:

VuOverSpeedingControlData a metadata použitá v protokolu pro stahování.

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

recordType označuje typ záznamu (VuOverSpeedingControlData). **Přiřazení hodnoty**: viz RecordType

recordSize je velikost záznamu VuOverSpeedingControlData v bajtech.

noOfRecords je počet záznamů v sadě záznamů.

records je sada datových záznamů o kontrole překročení povolené rychlosti.

2.214 **VuOverSpeedingEventData**

1. generace:

Informace uložené v celku ve vozidle týkající se událostí překročení povolené rychlosti (požadavek 094 přílohy 1B).

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

noOfVuOverSpeedingEvents je počet událostí uvedených v sadě vuOverSpeedingEventRecords.

vuOverSpeedingEventRecords je sada záznamů o událostech překročení povolené rychlosti.

2.215 **VuOverSpeedingEventRecord**

1. generace:

Informace uložené v celku ve vozidle týkající se událostí překročení povolené rychlosti (požadavek 094 přílohy 1B a požadavek 117 přílohy 1C).

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

eventType je typ události.

eventRecordPurpose je účel, pro který byla tato událost zaznamenána.

eventBeginTime je datum a čas začátku události.

eventEndTime je datum a čas konce události.

maxSpeedValue je nejvyšší rychlost naměřená během události.

averageSpeedValue je průměrná rychlost naměřená během události.

cardNumberDriverSlotBegin identifikuje kartu vloženou v otvoru pro kartu řidiče na začátku události.

similarEventsNumber je počet podobných událostí v daný den.

2. generace:

Informace uložené v celku ve vozidle týkající se událostí překročení povolené rychlosti (požadavek 094 přílohy 1B a požadavek 117 přílohy 1C).

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

Namísto prvku cardNumberDriverSlotBegin používá struktura dat 2. generace následující datový prvek:

cardNumberAndGenDriverSlotBegin identifikuje kartu vloženou v otvoru pro kartu řidiče na začátku události, včetně její generace.

2.216 **VuOverSpeedingEventRecordArray**

2. generace:

Informace uložené v celku ve vozidle týkající se událostí překročení povolené rychlosti (požadavek 117 přílohy 1C).

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

recordType označuje typ záznamu (VuOverSpeedingEventRecord). **Přiřazení hodnoty**: viz RecordType

recordSize je velikost záznamu VuOverSpeedingEventRecord v bajtech.

noOfRecords je počet záznamů v sadě záznamů.

records je sada záznamů o událostech překročení povolené rychlosti.

2.217 **VuPartNumber**

Katalogové číslo dílu celku ve vozidle.

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

Přiřazení hodnoty: specifické pro výrobce celku ve vozidle.

2.218 **VuPlaceDailyWorkPeriodData**

1. generace:

Informace uložené v celku ve vozidle týkající se míst, kde řidiči začínají nebo končí denní pracovní dobu (požadavek 087 přílohy 1B a požadavky 108 a 110 přílohy 1C).

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

noOfPlaceRecords je počet záznamů uvedených v sadě vuPlaceDailyWorkPeriodRecords.

vuPlaceDailyWorkPeriodRecords je sada záznamů týkajících se míst.

2.219 **VuPlaceDailyWorkPeriodRecord**

1. generace:

Informace uložené v celku ve vozidle týkající se místa, kde řidič začíná nebo končí denní pracovní dobu (požadavek 087 přílohy 1B a požadavky 108 a 110 přílohy 1C).

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

fullCardNumber je typ karty řidiče, členský stát, který ji vydal, a číslo karty.

placeRecord obsahuje informace týkající se zadaného místa.

2. generace:

Informace uložené v celku ve vozidle týkající se místa, kde řidič začíná nebo končí denní pracovní dobu (požadavek 087 přílohy 1B a požadavky 108 a 110 přílohy 1C).

```
VuPlaceDailyWorkPeriodRecord ::= SEQUENCE {
   fullCardNumberAndGeneration         FullCardNumberAndGeneration,
   placeRecord                         PlaceRecord
}
```

Místo prvku fullCardNumber používá struktura dat 2. generace následující datový prvek:

fullCardNumberAndGeneration je typ karty, členský stát, který ji vydal, její číslo a generace, jak jsou na kartě uloženy.

2.220 **VuPlaceDailyWorkPeriodRecordArray**

2. generace:

Informace uložené v celku ve vozidle týkající se míst, kde řidič začíná nebo končí denní pracovní dobu (požadavky 108 a 110 přílohy 1C).

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

recordType označuje typ záznamu (VuPlaceDailyWorkPeriodRecord). **Přiřazení hodnoty**: viz RecordType

recordSize je velikost záznamu VuPlaceDailyWorkPeriodRecord v bajtech.

noOfRecords je počet záznamů v sadě záznamů.

records je sada záznamů týkajících se míst.

2.221 **VuPrivateKey**

1. generace:

Soukromý klíč celku ve vozidle.

```
VuPrivateKey ::= RSAKeyPrivateExponent
```

2.222 **VuPublicKey**

1. generace:

Veřejný klíč celku ve vozidle.

```
VuPublicKey ::= PublicKey
```

2.223 **VuSerialNumber**

Výrobní číslo celku ve vozidle (požadavek 075 přílohy 1B a požadavek 93 přílohy 1C).

```
VuSerialNumber ::= ExtendedSerialNumber
```

2.224 **VuSoftInstallationDate**

Datum instalace verze softwaru celku ve vozidle.

```
VuSoftInstallationDate ::= TimeReal
```

Přiřazení hodnoty: není specifikováno.

2.225 **VuSoftwareIdentification**

Informace uložená v celku ve vozidle týkající se instalovaného softwaru.

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

vuSoftwareVersion je číslo verze softwaru v celku ve vozidle.

vuSoftInstallationDate je datum instalace verze softwaru.

2.226 **VuSoftwareVersion**

Číslo verze softwaru celku ve vozidle.

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

Přiřazení hodnoty: není specifikováno.

2.227 **VuSpecificConditionData**

1. generace:

Informace uložené v celku ve vozidle týkající se zvláštních podmínek.

```
VuSpecificConditionData ::= SEQUENCE {
   noOfSpecificConditionRecords         INTEGER(0..2^16-1)
   specificConditionRecords             SET SIZE (noOfSpecificConditionRecords) OF
                                        SpecificConditionRecord
}
```

noOfSpecificConditionRecords je počet záznamů uvedených v sadě specificConditionRecords.

specificConditionRecords je sada záznamů týkajících se zvláštních podmínek.

2.228 **VuSpecificConditionRecordArray**

2. generace:

Informace uložené v celku ve vozidle týkající se zvláštních podmínek (požadavek 130 přílohy 1C).

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

recordType označuje typ záznamu (SpecificConditionRecord). **Přiřazení hodnoty**: viz RecordType

recordSize je velikost záznamu SpecificConditionRecord v bajtech.

noOfRecords je počet záznamů v sadě záznamů.

records je sada záznamů týkajících se zvláštních podmínek.

2.229 **VuTimeAdjustmentData**

1. generace:

Informace uložené v celku ve vozidle týkající se nastavení času provedených mimo pravidelnou kalibraci (požadavek 101 přílohy 1B).

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

noOfVuTimeAdjRecords je počet záznamů v sadě vuTimeAdjustmentRecords.

vuTimeAdjustmentRecords je sada záznamů o nastavení času.

2.230 **VuTimeAdjustmentGNSSRecord**

2. generace:

Informace uložené v celku ve vozidle týkající se nastavení času na základě časových údajů z GNSS (požadavky 124 a 125 přílohy 1C).

```
VuTimeAdjustmentGNSSRecord ::= SEQUENCE {
   oldTimeValue                        TimeReal,
   newTimeValue                        TimeReal
}
```

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

2.231 **VuTimeAdjustmentGNSSRecordArray**

2. generace:

Informace uložené v celku ve vozidle týkající se nastavení času provedeného na základě časových údajů z GNSS (požadavky 124 a 125 přílohy 1C).

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

recordType označuje typ záznamu (VuTimeAdjustmentGNSSRecord). **Přiřazení hodnoty**: viz RecordType

recordSize je velikost záznamu VuTimeAdjustmentGNSSRecord v bajtech.

noOfRecords je počet záznamů v sadě záznamů.

records je sada záznamů o nastavení času podle GNSS.

2.232 **VuTimeAdjustmentRecord**

Informace uložené v celku ve vozidle týkající se nastavení času provedeného mimo pravidelnou kalibraci (požadavek 101 přílohy 1B a požadavky 124 a 125 přílohy 1C).

1. generace:

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

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

workshopName, workshopAddress jsou název dílny a její adresa.

workshopCardNumber identifikuje kartu dílny použitou k nastavení času.

2. generace:

```
VuTimeAdjustmentRecord ::= SEQUENCE {
   oldTimeValue                         TimeReal,
   newTimeValue                         TimeReal,
   workshopName                         Name,
   workshopAddress                      Address,
   workshopCardNumberAndGeneration      FullCardNumberAndGeneration
}
```

Místo prvku workshopCardNumber používá struktura dat 2. generace následující datový prvek.

workshopCardNumberAndGeneration identifikuje kartu dílny použitou k nastavení času, včetně její generace.

2.233 **VuTimeAdjustmentRecordArray**

2. generace:

Informace uložené v celku ve vozidle týkající se nastavení času provedených mimo pravidelnou kalibraci (požadavky 124 a 125 přílohy 1C).

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

recordType označuje typ záznamu (VuTimeAdjustmentRecord). **Přiřazení hodnoty**: viz RecordType

recordSize je velikost záznamu VuTimeAdjustmentRecord v bajtech.

noOfRecords je počet záznamů v sadě záznamů.

records je sada záznamů o nastavení času.

2.234 **WorkshopCardApplicationIdentification**

Informace uložené na kartě dílny týkající se identifikace aplikace karty (požadavky 307 a 330 přílohy 1C).

1. generace:

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

typeOfTachographCardId udává implementovaný typ karty.

cardStructureVersion udává verzi struktury implementované v kartě.

noOfEventsPerType je počet událostí od každého typu události, které lze na kartu zaznamenat.

noOfFaultsPerType je počet závad od každého druhu závady, které lze na kartu zaznamenat.

activityStructureLength udává počet bajtů, které jsou k dispozici pro ukládání záznamů o činnosti.

noOfCardVehicleRecords je počet záznamů o vozidle, které může karta obsahovat.

noOfCardPlaceRecords je počet míst, která lze na kartu zaznamenat.

noOfCalibrationRecords je počet záznamů o kalibraci, který lze na kartu uložit.

2. generace:

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

Kromě prvků 1. generace se používají tyto datové prvky:

noOfGNSSCDRecords je počet záznamů o nepřetržité době řízení dle GNSS, které lze na kartu uložit.

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

2.235 **WorkshopCardCalibrationData**

Informace uložené na kartě dílny týkající se činnosti dílny provedené s kartou (požadavky 314, 316, 337 a 339 přílohy 1C).

```
WorkshopCardCalibrationData ::= SEQUENCE {
   calibrationTotalNumber              INTEGER(0 .. 2^16-1),
   calibrationPointerNewestRecord      INTEGER(0 .. NoOfCalibrationRecords-1),
   calibrationRecords                  SET SIZE(NoOfCalibrationRecords) OF
                                       WorkshopCardCalibrationRecord
}
```

calibrationTotalNumber je celkový počet kalibrací provedených s kartou.

calibrationPointerNewestRecord je index naposledy aktualizovaného záznamu o kalibraci.

Přiřazení hodnoty: číslo odpovídající čítači záznamů o kalibraci začínající hodnotou „0“ u prvního výskytu záznamu o kalibraci ve struktuře.

calibrationRecords je sada záznamů obsahujících informace o kalibraci a/nebo nastavení času.

2.236 **WorkshopCardCalibrationRecord**

Informace uložené na kartě dílny týkající se kalibrace provedené s kartou (požadavky 314 a 337 přílohy 1C).

1. generace:

```
WorkshopCardCalibrationRecord ::= SEQUENCE {
   calibrationPurpose                  CalibrationPurpose,
   vehicleIdentificationNumber         VehicleIdentificationNumber,
   vehicleRegistration                 VehicleRegistrationIdentification,
   wVehicleCharacteristicConstant      W-VehicleCharacteristicConstant,
   kConstantOfRecordingEquipment       K-ConstantOfRecordingEquipment,
   lTyreCircumference                  L-TyreCircumference,
   tyreSize                            TyreSize,
   authorisedSpeed                     SpeedAuthorised,
   oldOdometerValue                    OdometerShort,
   newOdometerValue                    OdometerShort,
   oldTimeValue                        TimeReal,
   newTimeValue                        TimeReal,
   nextCalibrationDate                 TimeReal,
   vuPartNumber                        VuPartNumber,
   vuSerialNumber                      VuSerialNumber,
   sensorSerialNumber                  SensorSerialNumber
}
```

calibrationPurpose je účel kalibrace.

vehicleIdentificationNumber je identifikační číslo vozidla (VIN).

vehicleRegistration obsahuje registrační značku (VRN) a členský stát registrace vozidla.

wVehicleCharacteristicConstant je charakteristický koeficient vozidla.

kConstantOfRecordingEquipment je konstanta záznamového zařízení.

lTyreCircumference je účinný obvod pneumatik na kolech.

tyreSize je označení rozměrů pneumatik namontovaných na vozidle.

authorisedSpeed je maximální dovolená rychlost vozidla.

oldOdometerValue, newOdometerValue jsou stará a nová hodnota počitadla ujetých kilometrů.

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

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

vuPartNumber, **vuSerialNumber** a **sensorSerialNumber** jsou datové prvky pro identifikaci záznamového zařízení.

2. generace:

```
WorkshopCardCalibrationRecord ::= SEQUENCE {
   calibrationPurpose                  CalibrationPurpose,
   vehicleIdentificationNumber         VehicleIdentificationNumber,
   vehicleRegistration                 VehicleRegistrationIdentification,
   wVehicleCharacteristicConstant      W-VehicleCharacteristicConstant,
   kConstantOfRecordingEquipment       K-ConstantOfRecordingEquipment,
   lTyreCircumference                  L-TyreCircumference,
   tyreSize                            TyreSize,
   authorisedSpeed                     SpeedAuthorised,
   oldOdometerValue                    OdometerShort,
   newOdometerValue                    OdometerShort,
   oldTimeValue                        TimeReal,
   newTimeValue                        TimeReal,
   nextCalibrationDate                 TimeReal,
   vuPartNumber                        VuPartNumber,
   vuSerialNumber                      VuSerialNumber,
   sensorSerialNumber                  SensorSerialNumber,
   sensorGNSSSerialNumber              SensorGNSSSerialNumber,
   rcmSerialNumber                     RemoteCommunicationModuleSerialNumber,
   sealDataCard                        SealDataCard
}
```

Kromě prvků 1. generace se používají tyto datové prvky:

sensorGNSSSerialNumber identifikuje vnější zařízení GNSS.

rcmSerialNumber identifikuje modul dálkové komunikace.

sealDataCard udává informace o plombách, které jsou připojeny k různým částem vozidla.

2.237 **WorkshopCardHolderIdentification**

Informace uložené na kartě dílny týkající se identifikace držitele karty (požadavky 311 a 334 přílohy 1C).

```
WorkshopCardHolderIdentification ::= SEQUENCE {
   workshopName                        Name,
   workshopAddress                     Address,
   cardHolderName                      HolderName,
   cardHolderPreferredLanguage         Language
}
```

workshopName je název dílny držitele karty.

workshopAddress je adresa dílny držitele karty.

cardHolderName je příjmení a jméno (jména) držitele (např. jméno mechanika).

cardHolderPreferredLanguage je upřednostňovaný jazyk držitele karty.

2.238 **WorkshopCardPIN**

Kód PIN karty dílny (požadavky 309 a 332 přílohy 1C).

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

Přiřazení hodnoty: Kód PIN známý držiteli karty, zprava doplněný bajty „FF“ na délku 8 bajtů.

2.239 **W-VehicleCharacteristicConstant**

Charakteristický koeficient vozidla (definice k)).

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

Přiřazení hodnoty: impulsy na kilometr v provozním rozsahu 0 až 64 255 impulsů/km.

2.240 **VuPowerSupplyInterruptionRecord**

2. generace:

Informace uložené v celku ve vozidle týkající se událostí přerušení napájení (požadavek 117 přílohy 1C).

```
VuPowerSupplyInterruptionRecord ::= SEQUENCE {
   eventType                          EventFaultType,
   eventRecordPurpose                 EventFaultRecordPurpose,
   eventBeginTime                     TimeReal,
   eventEndTime                       TimeReal,
   cardNumberAndGenDriverSlotBegin    FullCardNumberAndGeneration,
   cardNumberAndGenDriverSlotEnd      FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotBegin  FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotEnd    FullCardNumberAndGeneration,
   similarEventsNumber                SimilarEventsNumber
}
```

eventType je typ události.

eventRecordPurpose je účel, pro který byla tato událost zaznamenána.

eventBeginTime je datum a čas začátku události.

eventEndTime je datum a čas konce události.

cardNumberAndGenDriverSlotBegin identifikuje kartu vloženou do otvoru pro kartu řidiče na začátku události, včetně její generace.

cardNumberAndGenDriverSlotEnd identifikuje kartu vloženou do otvoru pro kartu řidiče na konci události, včetně její generace.

cardNumberAndGenCodriverSlotBegin identifikuje kartu vloženou do otvoru pro kartu druhého řidiče na začátku události, včetně její generace.

cardNumberAndGenCodriverSlotEnd identifikuje kartu vloženou do otvoru pro kartu druhého řidiče na konci události, včetně její generace.

similarEventsNumber je počet podobných událostí v daný den.

2.241 **VuPowerSupplyInterruptionRecordArray**

2. generace:

Informace uložené v celku ve vozidle týkající se událostí přerušení napájení (požadavek 117 přílohy 1C).

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

recordType označuje typ záznamu (VuPowerSupplyInterruptionRecord). **Přiřazení hodnoty**: viz RecordType

recordSize je velikost záznamu VuPowerSupplyInterruptionRecord v bajtech.

noOfRecords je počet záznamů v sadě záznamů.

records je sada záznamů o událostech přerušení napájení.

2.242 **VuSensorExternalGNSSCoupledRecordArray**

2. generace:

Sada záznamů SensorExternalGNSSCoupledRecord a metadata použitá v protokolu pro stahování.

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

recordType označuje typ záznamu (SensorExternalGNSSCoupledRecord). **Přiřazení hodnoty**: viz RecordType

recordSize je velikost záznamu SensorExternalGNSSCoupledRecord v bajtech.

noOfRecords je počet záznamů v sadě záznamů.

records je sada záznamů o vazbě externího snímače GNSS.

2.243 **VuSensorPairedRecordArray**

2. generace:

Sada záznamů SensorPairedRecord a metadata použitá v protokolu pro stahování.

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

recordType označuje typ záznamu (SensorPairedRecord). **Přiřazení hodnoty**: viz RecordType

recordSize je velikost záznamu SensorPairedRecord v bajtech.

noOfRecords je počet záznamů v sadě záznamů.

records je sada záznamů o párování snímače.

3. DEFINICE HODNOT A ROZSAHŮ VELIKOSTÍ

Definice hodnot proměnných použitých pro definice v odstavci 2.

```
TimeRealRange ::= 2^32-1
```

4. ZNAKOVÉ SADY

V řetězcích IA5Strings se používají znaky ASCII dle definice v ISO/IEC 8824-1. Pro čitelnost a snadné odkazování je přiřazení hodnoty uvedeno dále. V případě nesrovnalostí má norma ISO/IEC 8824-1 přednost před touto informativní poznámkou.

```
  ! " # $ % & ' ( ) * + , - . / 0 1 2 3 4 5 6 7 8 9 : ; < = > ?
@ A B C D E F G H I J K L M N O P Q R S T U V W X Y Z [ \ ] ^ _
` a b c d e f g h i j k l m n o p q r s t u v w x y z { | } ~
```

Další řetězce znaků (Address, Name, VehicleRegistrationNumber) navíc používají i znaky z rozsahu dekadických kódů znaků 161–255 z následujících 8-bitových standardních znakových sad určených číslem kódové stránky: Standardní znaková sada	Kódová stránka (dekadicky)
ISO/IEC 8859-1 Latinka 1 – západoevropské jazyky	1
ISO/IEC 8859-2 Latinka 2 – středoevropské jazyky	2
ISO/IEC 8859-3 Latinka 3 – jihoevropské jazyky	3
ISO/IEC 8859-5 Latinka / cyrilice	5
ISO/IEC 8859-7 Latinka / řecká abeceda	7
ISO/IEC 8859-9 Latinka 5 – turečtina	9
ISO/IEC 8859-13 Latinka 7 – pobaltské jazyky	13
ISO/IEC 8859-15 Latinka 9	15
ISO/IEC 8859-16 Latinka 10 – jazyky jihovýchodní Evropy	16
KOI8-R Latinka / cyrilice	80
KOI8-U Latinka / cyrilice	85

5. KÓDOVÁNÍ

Při kódování dle pravidel ASN.1 musí být všechny datové typy kódovány podle ISO/IEC 88252 v zarovnané variantě.

6. IDENTIFIKÁTORY OBJEKTŮ A IDENTIFIKÁTORY APLIKACÍ

6.1 **Identifikátory objektů**

Identifikátory objektů (OID) uvedené v této kapitole se vztahují pouze na 2. generaci. Tyto OID jsou stanoveny v TR-03110-3 a zde jsou zopakovány z důvodu úplnosti. Tyto OID jsou obsaženy v podstromu bsi-de:

```
bsi-de OBJECT IDENTIFIER ::= {
   itu-t(0) identified-organization(4) etsi(0)
   reserved(127) etsi-identified-organization(0) 7
}
```

Identifikátory protokolu ověření pravosti celku ve vozidle

```
id-TA         OBJECT IDENTIFIER ::= {bsi-de protocols(2) smartcard(2) 2}
id-TA-ECDSA                 OBJECT IDENTIFIER ::= {id-TA 2}
id-TA-ECDSA-SHA-256 OBJECT IDENTIFIER ::= {id-TA-ECDSA 3}
id-TA-ECDSA-SHA-384 OBJECT IDENTIFIER ::= {id-TA-ECDSA 4}
id-TA-ECDSA-SHA-512 OBJECT IDENTIFIER ::= {id-TA-ECDSA 5}
```

Příklad: Má-li být ověření pravosti celku ve vozidle prováděno pomocí SHA-384, musí být použit identifikátor objektu (v notaci ASN.1) `bsi-de protocols(2) smartcard(2) 2 2 4`. Hodnota tohoto identifikátoru objektu v tečkové notaci je `0.4.0.127.0.7.2.2.2.2.4`.

	Tečková notace	Bajtová notace
id-TA-ECDSA-SHA-256	0.4.0.127.0.7.2.2.2.2.3	'04 00 7F 00 07 02 02 02 02 03'
id-TA-ECDSA-SHA-384	0.4.0.127.0.7.2.2.2.2.4	'04 00 7F 00 07 02 02 02 02 04'
id-TA-ECDSA-SHA-512	0.4.0.127.0.7.2.2.2.2.5	'04 00 7F 00 07 02 02 02 02 05'

Identifikátory protokolu ověření pravosti čipu

```
id-CA         OBJECT IDENTIFIER ::= {bsi-de protocols(2) smartcard(2) 3}
id-CA-ECDH                          OBJECT IDENTIFIER ::= {id-CA 2}
id-CA-ECDH-AES-CBC-CMAC-128         OBJECT IDENTIFIER ::= {id-CA-ECDH 2}
id-CA-ECDH-AES-CBC-CMAC-192         OBJECT IDENTIFIER ::= {id-CA-ECDH 3}
id-CA-ECDH-AES-CBC-CMAC-256         OBJECT IDENTIFIER ::= {id-CA-ECDH 4}
```

Příklad: Ověření pravosti čipu má být provedeno pomocí algoritmu ECDH a jeho výsledkem klíč relace AES o délce 128 bitů. Tento klíč relace bude následně použit v režimu CBC k zajištění důvěrnosti dat a v algoritmu CMAC k zaručení pravosti dat. Použije se tedy identifikátor objektu (v notaci ASN.1) `bsi-de protocols(2) smartcard(2) 3 2 2`. Hodnota tohoto identifikátoru objektu v tečkové notaci je `0.4.0.127.0.7.2.2.3.2.2`.

	Tečková notace	Bajtová notace
id-CA-ECDH-AES-CBC-CMAC-128	0.4.0.127.0.7.2.2.3.2.2	'04 00 7F 00 07 02 02 03 02 02'
id-CA-ECDH-AES-CBC-CMAC-192	0.4.0.127.0.7.2.2.3.2.3	'04 00 7F 00 07 02 02 03 02 03'
id-CA-ECDH-AES-CBC-CMAC-256	0.4.0.127.0.7.2.2.3.2.4	'04 00 7F 00 07 02 02 03 02 04'

6.2 Identifikátory aplikací

2. generace:

Identifikátor aplikace (AID) pro vnější zařízení GNSS (2. generace) je dán řetězcem 'FF 44 54 45 47 4D'. Jde o proprietární AID podle ISO/IEC 7816-4.

Poznámka: Posledních 5 bajtů kóduje DTEGM pro vnější zařízení GNSS inteligentního tachografu.

Identifikátor aplikace pro aplikaci karty tachografu 2. generace je dán řetězcem 'FF 53 4D 52 44 54'. Jde o proprietární AID podle ISO/IEC 7816-4.

Dodatek 2

SPECIFIKACE KARET TACHOGRAFU

OBSAH

1. ÚVOD

1.1 **Zkratky**

Pro účely tohoto dodatku se použijí tyto zkratky:

AC	podmínky přístupu (*Access conditions*)
AES	pokročilý standard pro šifrování (*Advanced Encryption Standard*)
AID	identifikátor aplikace (*Application Identifier*)
ALW	vždy (*Always*)
APDU	datová jednotka aplikačního protokolu (*Application Protocol Data Unit*, struktura příkazu)
ATR	odpověď na reset (*Answer To Reset*)
AUT	ověřena pravost (*Authenticated*)
C6, C7	kontakty č. 6 a 7 karty, jak popisuje norma ISO/IEC 7816-2
cc	hodinové takty (*clock cycles*)
CHV	informace k ověření držitele karty (*Card holder Verification Information*)
CLA	bajt třídy (*Class*) příkazu APDU
DSRC	vyhrazené komunikace krátkého dosahu (*Dedicated Short Range Communication*)
DF	vyhrazený soubor (*Dedicated File*). DF může obsahovat jiné soubory (EF nebo DF)
ECC	kryptografie na bázi eliptických křivek (*Elliptic Curve Cryptography*)
EF	elementární soubor (*Elementary File*)
etu	základní časová jednotka (*elementary time unit*)
G1	1. generace
G2	2. generace
IC	integrovaný obvod (*Integrated Circuit*)
ICC	karta s integrovaným obvodem, čipová karta (*Integrated Circuit Card*)
ID	identifikátor
IFD	zařízení rozhraní (*Interface Device*)
IFS	velikost informačního pole (*Information Field Size*)
IFSC	velikost informačního pole pro kartu (*Information Field Size for the card*)

IFSD	velikost informačního pole zařízení (*Information Field Size Device*, pro terminál)
INS	bajt instrukce (*Instruction*) příkazu APDU
Lc	délka vstupních dat pro příkaz APDU
Le	délka očekávaných dat (výstupních dat pro příkaz)
MF	hlavní soubor (*Master File*, kořenový DF)
NAD	adresa uzlu (*Node Address*) používaná v protokolu T=1
NEV	nikdy (*Never*)
P1-P2	bajty parametrů
PIN	kód PIN (*Personal Identification Number*)
PRO SM	chráněno bezpečným předáváním zpráv (*Protected with secure messaging*)
PTS	výběr přenosového protokolu (*Protocol Transmission Selection*)
RFU	vyhrazeno pro budoucí použití (*Reserved for Future Use*)
RST	reset (karty)
SFID	krátký identifikátor EF (*Short EF Identifier*)
SM	bezpečné předávání zpráv (*Secure Messaging*)
SW1-SW2	stavové bajty
TS	počáteční znak ATR
VPP	programovací napětí
VU	celek ve vozidle (*Vehicle Unit*)
XXh	hodnota XX v hexadecimální notaci
'XXh'	hodnota XX v hexadecimální notaci
||	symbol zřetězení: 03||04=0304

1.2 **Odkazy**

V tomto dodatku se používají tyto odkazy:

ISO/IEC 7816-2 *Identification cards – Integrated circuit cards – Part 2: Dimensions and location of the contacts.* ISO/IEC 7816-2:2007.

ISO/IEC 7816-3 *Identification cards – Integrated circuit cards – Part 3: Electrical interface and transmission protocols.* ISO/IEC 7816-3:2006.

ISO/IEC 7816-4 *Identification cards – Integrated circuit cards – Part 4: Organization, security and commands for interchange.* ISO/IEC 7816-4:2013 + Cor 1: 2014.

ISO/IEC 7816-6 *Identification cards – Integrated circuit cards – Part 6: Interindustry data elements for interchange.* ISO/IEC 7816-6:2004 + Cor 1: 2006.

ISO/IEC 7816-8 *Identification cards – Integrated circuit cards – Part 8: Commands for security operations.* ISO/IEC 7816-8:2004.

ISO/IEC 9797-2 *Information technology – Security techniques – Message Authentication Codes (MACs) – Part 2: Mechanisms using a dedicated hash-function.* ISO/IEC 9797-2:2011

2. ELEKTRICKÉ A FYZICKÉ VLASTNOSTI

TCS_01 Všechny elektronické signály musí být v souladu s normou ISO/IEC 7816-3, pokud není uvedeno jinak.

TCS_02 Umístění kontaktů karty a jejich rozměry musí být v souladu s normou ISO/IEC 7816-2.

2.1 **Napájecí napětí a spotřeba proudu**

TCS_03 Karta pracuje podle specifikace uvnitř hranic spotřeby podle ISO/IEC 7816-3.

TCS_04 Karta pracuje při Vcc = 3 V (± 0,3 V) nebo při Vcc = 5 V (± 0,5 V).

Volba napětí se provádí v souladu s ISO/IEC 7816-3.

2.2 **Programovací napětí V_{pp}**

TCS_05 Karta nevyžaduje na kontaktu C6 programovací napětí. Předpokládá se, že kontakt C6 není v zařízení rozhraní (IFD) zapojen. Kontakt C6 může být na kartě spojen s napětím V_{cc}, nesmí být ale uzemněn. Toto napětí nesmí být v žádném případě interpretováno.

2.3 **Generátor hodinových impulsů a frekvence**

TCS_06 Karta pracuje v rozsahu frekvencí 1 až 5 MHz a může podporovat vyšší frekvence. V rámci jedné relace karty se hodinová frekvence může měnit ± 2 %. Hodinová frekvence je generována celkem ve vozidle, ne kartou. Střída se může pohybovat od 40 do 60 %.

TCS_07 Za podmínek obsažených v souboru EF ICC karty mohou být vnější hodiny zastaveny. První bajt těla souboru EF ICC kóduje podmínky režimu Clockstop:

Úroveň L	Úroveň H		
Bit 3	Bit 2	Bit 1	
0	0	1	Režim Clockstop dovolen, žádná preferovaná úroveň
0	1	1	Režim Clockstop dovolen, preferována úroveň H
1	0	1	Režim Clockstop dovolen, preferována úroveň L
0	0	0	Režim Clockstop není dovolen
0	1	0	Režim Clockstop dovolen pouze při úrovni H
1	0	0	Režim Clockstop dovolen pouze při úrovni L

Bity 4 až 8 nejsou použity.

2.4 **Kontakt I/O**

TCS_08 Kontakt I/O (C7) slouží pro příjem dat ze zařízení rozhraní (IFD) a pro vysílání dat do IFD. Během provozu se nachází v režimu vysílání buď jen karta, nebo IFD. Jsou-li v režimu vysílání obě jednotky, nesmí tím být karta poškozena. Pokud karta nevysílá, musí být v režimu příjmu.

2.5 **Stavy karty**

TCS_09 Při připojeném napájecím napětí pracuje karta ve dvou stavech:

provozním stavu během vykonávání příkazů nebo během propojení s digitální jednotkou,

klidovém stavu v ostatním čase; v tomto stavu musejí být zachována všechna data na kartě.

3. HARDWARE A KOMUNIKACE

3.1 **Úvod**

Tento odstavec popisuje minimální funkčnost požadovanou kartami tachografu a celky ve vozidle k zajištění správného provozu a interoperability.

Karty tachografu jsou v maximální možné míře v souladu s dostupnými normami ISO/IEC (především ISO/IEC 7816). Příkazy a protokoly jsou nicméně plně popsány, aby bylo specifikováno určité omezené použití nebo některé rozdíly, pokud existují. Specifikované příkazy plně odpovídají normám, na něž se odkazuje, pokud není uvedeno jinak.

3.2 **Protokol pro přenos dat**

TCS_10 Protokol pro přenos dat je v souladu s normou ISO/IEC 7816-3 pro T = 0 a T = 1. Celek ve vozidle konkrétně respektuje prodloužení čekací doby odesílaná kartou.

3.2.1 *Protokoly*

TCS_11 Karta podporuje jak protokol **T=0**, tak protokol **T=1**. Karta může navíc podporovat další protokoly založené na kontaktech.

TCS_12 **T=0** je výchozí protokol, pro změnu na protokol **T=1** je tedy nutný příkaz **PTS**.

TCS_13 Zařízení podporují v obou protokolech „**přímou konvenci**“, která je proto pro kartu povinná.

TCS_14 Bajt **IFSC** (velikost informačního pole karty) je uveden v ATR ve znaku TA3. Tato hodnota činí nejméně ‘F0h’ (= 240 bajtů).

Pro protokoly platí následující omezení:

TCS_15 **T=0**

— Zařízení rozhraní podporuje odpověď na I/O po náběžné hraně signálu RST od 400 cc.

— Zařízení rozhraní musí být schopno číst znaky oddělené 12 etu.

— Zařízení rozhraní čte chybný znak a jeho opakování, jestliže jsou odděleny 13 etu. Jestliže je detekován chybný znak, signál chyby se na I/O může objevit mezi 1 etu a 2 etu. Zařízení podporuje prodlevu 1 etu.

— Zařízení rozhraní akceptuje 33 bajtů ATR (TS+32).

— Jestliže se v ATR nachází TC1, použije se u znaků odesílaných zařízením rozhraní prodloužená ochranná doba *Extra Guard Time*, ačkoliv znaky odesílané kartou mohou být nadále odděleny 12 etu. To také platí pro znak ACK odeslaný kartou po vyslání znaku P3 zařízením rozhraní.

— Zařízení rozhraní bere v úvahu znak NUL odeslaný kartou.

— Zařízení rozhraní akceptuje komplementární režim pro ACK.

— Příkaz get-response nelze použít v režimu zřetězení k získání dat, jejichž délka by mohla přesáhnout 255 bajtů.

TCS_16 **T=1**

— Bajt NAD: nepoužívá se (NAD se nastaví na ‘00’).

— S-blok ABORT: nepoužívá se.

— S-blok VPP state error: nepoužívá se.

— Celková délka zřetězení pro datové pole nepřesáhne 255 bajtů (zajistí IFD).

— IFD bezprostředně po ATR uvede velikost informačního pole zařízení (IFSD): IFD vyšle S-blok IFS request po ATR a karta pošle zpět S-blok IFS. Doporučená hodnota IFSD je 254 bajtů.

— Karta nežádá o nové nastavení IFS.

3.2.2 *ATR*

TCS_17 Zařízení kontroluje bajty ATR podle normy ISO/IEC 7816-3. Historické znaky ATR se nekontrolují.

Příklad základní ATR pro dva protokoly podle normy ISO/IEC 7816-3

Znak	Hodnota	Poznámky
TS	'3Bh'	Indikuje přímou konvenci
T0	'85h'	TD1 přítomen; přítomno 5 historických bajtů
TD1	'80h'	TD2 přítomen; použije se T=0
TD2	'11h'	TA3 přítomen; použije se T=1
TA3	'XXh' (minimálně 'F0h')	Information Field Size Card (IFSC)
TH1 až TH5	'XXh'	Historické znaky
TCK	'XXh'	Kontrolní znak (XOR)

TCS_18 Po odpovědi na reset (ATR) je implicitně vybrán hlavní soubor (MF) a stává se aktuálním adresářem.

3.2.3 *PTS*

TCS_19 Výchozí protokol je T=0. Pro nastavení protokolu T=1 musí zařízení kartě poslat příkaz PTS (také známý jako PPS).

TCS_20 Poněvadž protokoly T=0 i T=1 jsou pro kartu povinné, základní PTS pro přepínání protokolů je pro kartu povinný.

Jak je uvedeno v normě ISO/IEC 7816-3, lze PTS použít pro přepnutí na vyšší rychlost přenosu dat než rychlost výchozí, kterou karta případně navrhla v ATR (bajt TA(1)).

Vyšší rychlosti přenosu dat jsou pro kartu volitelné.

TCS_21 Jestliže žádné jiné rychlosti přenosu dat kromě výchozí rychlosti nejsou podporovány (nebo není podporována zvolená rychlost přenosu dat), odpoví karta na PTS korektně podle normy ISO/IEC 7816-3 vynecháním bajtu PPS1.

Příklady základního PTS pro výběr protokolu:

Znak	Hodnota	Poznámky
PPSS	'FFh'	Zahajovací znak.
PPS0	'00h' nebo '01h'	PPS1 až PPS3 nejsou přítomny; '00h' pro výběr T0, '01h' pro výběr T1.
PK	'XXh'	Kontrolní znak: 'XXh' = 'FFh' pokud PPS0 = '00h', 'XXh' = 'FEh' pokud PPS0 = '01h'.

3.3 **Pravidla přístupu**

TCS_22 Pravidlo přístupu specifikuje pro režim přístupu, např. příkaz, příslušné bezpečnostní podmínky. Příslušný příkaz je zpracován, pokud jsou tyto bezpečnostní podmínky splněny.

TCS_23 Pro kartu tachografu se používají tyto bezpečnostní podmínky:

Zkratka	Význam
ALW	Akce je vždy možná a může být provedena bez omezení. APDU příkazu a odpovědi se posílá jako otevřený text, tj. bez bezpečného předávání zpráv.
NEV	Akce není nikdy možná.
PLAIN-C	APDU příkazu se posílá otevřeně, tj. bez bezpečného předávání zpráv.
PWD	Akce může být provedena pouze v případě, že byl úspěšně ověřen kód PIN karty dílny, tj. je nastaven vnitřní bezpečnostní status karty „PIN_Verified“. Příkaz musí být odeslán bez bezpečného předávání zpráv.
EXT-AUT-G1	Akce může být provedena pouze v případě, že byl úspěšně proveden příkaz EXTERNAL AUTHENTICATE k ověření pravosti 1. generace (viz rovněž dodatek 11 část A).
SM-MAC-G1	APDU (příkaz a odezva) se musí použít s bezpečným předáváním zpráv 1. generace v režimu pouze s ověřením pravosti (viz dodatek 11 část A).
SM-C-MAC-G1	APDU příkazu se musí použít s bezpečným předáváním zpráv 1. generace v režimu pouze s ověřením pravosti (viz dodatek 11 část A).
SM-R-ENC-G1	APDU odpovědi se musí použít s bezpečným předáváním zpráv 1. generace v režimu šifrování (viz dodatek 11 část A), tj. nevrací se ověřovací kód zprávy (MAC).
SM-R-ENC-MAC-G1	APDU odpovědi se musí použít s bezpečným předáváním zpráv 1. generace v režimu šifrování a následného ověření pravosti (viz dodatek 11 část A).
SM-MAC-G2	APDU (příkaz a odezva) se musí použít s bezpečným předáváním zpráv 2. generace v režimu pouze s ověřením pravosti (viz dodatek 11 část B).
SM-C-MAC-G2	APDU příkazu se musí použít s bezpečným předáváním zpráv 2. generace v režimu pouze s ověřením pravosti (viz dodatek 11 část B).
SM-R-ENC-MAC-G2	APDU odpovědi se musí použít s bezpečným předáváním zpráv 2. generace v režimu šifrování a následného ověření pravosti (viz dodatek 11 část B).

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 k systému 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.

TCS_25 V aplikaci DF Tachograph G1 se používají tato pravidla přístupu:

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
PSO: 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

TCS_26 V aplikaci DF Tachograph_G2 se používají tato pravidla přístupu:

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

Příkaz	Karta řidiče	Karta dílny	Kontrolní karta	Karta podniku
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
PSO: 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

TCS_27 V MF se používají tato pravidla přístupu:

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

Příkaz	Karta řidiče	Karta dílny	Kontrolní karta	Karta podniku
PSO: Compute Digital Signature	Nepoužije se	Nepoužije se	Nepoužije se	Nepoužije se
PSO: Hash	Nepoužije se	Nepoužije se	Nepoužije se	Nepoužije se
PSO: Hash of File	Nepoužije se	Nepoužije se	Nepoužije se	Nepoužije se
PSO: Verify Certificate	ALW	ALW	ALW	ALW
Verify	Nepoužije se	ALW	Nepoužije se	Nepoužije se

TCS_28 Karta tachografu může, ale nemusí přijmout příkaz s vyšší úrovní zabezpečení, než jaká je uvedena v bezpečnostních podmínkách. Tj. je-li bezpečnostní podmínka ALW (nebo PLAIN-C), karta může přijmout příkaz s bezpečným předáváním zpráv (v režimu šifrování a/nebo ověření pravosti). Vyžaduje-li bezpečnostní podmínka bezpečné předávání zpráv s režimem ověření pravosti, karta tachografu může přijmout příkaz s bezpečným předáváním zpráv téže generace v režimu ověření pravosti a šifrování.

Poznámka: Více informací o podpoře příkazů pro různé typy karet tachografů a různé DF je uvedeno v popisech příkazů.

3.4 **Přehled příkazů a kódů chyb**

Příkazy a organizace souborů jsou odvozeny od normy ISO/IEC 7816-4 a jsou s ní v souladu.

Tato část popisuje následující páry APDU příkaz-odpověď. Varianty příkazů, které jsou podporovány aplikací 1. a 2. generace, jsou uvedeny v příslušných popisech příkazů.

Příkaz	INS
SELECT	‘A4h’
READ BINARY	‘B0h’, ‘B1h’
UPDATE BINARY	‘D6h’, ‘D7h’
GET CHALLENGE	‘84h’
VERIFY	‘20h’
GET RESPONSE	‘C0h’
PERFORM SECURITY OPERATION	‘2Ah’
— VERIFY CERTIFICATE	
— COMPUTE DIGITAL SIGNATURE	
— VERIFY DIGITAL SIGNATURE	
— HASH	
— PERFORM HASH OF FILE	
— PROCESS DSRC MESSAGE	

Příkaz	INS
INTERNAL AUTHENTICATE	'88h'
EXTERNAL AUTHENTICATE	'82h'
MANAGE SECURITY ENVIRONMENT	'22h'
— SET DIGITAL SIGNATURE TEMPLATE	
— SET AUTHENTICATION TEMPLATE	
GENERAL AUTHENTICATE	'86h'

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.
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	82	Bezpečné předávání zpráv není podporováno
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)

SW1	SW2	Význam
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
6 B	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

TCS_30 Nastane-li v jednom APDU příkazu více než jedna chybová podmínka, může karta vrátit kterékoli příslušné stavové slovo.

3.5 **Popisy příkazů**

V této kapitole jsou popsány povinné příkazy pro karty tachografu.

Další významné podrobnosti vztahující se k obsaženým kryptografickým operacím jsou uvedeny v dodatku 11 „Společné bezpečnostní mechanismy“ pro tachograf 1. a 2. generace.

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

TCS_31 Jsou-li požadovány oba bajty délky (Lc a Le), je třeba v případě, že IFD používá protokol T=0, popisovaný příkaz rozdělit na dvě části: IFD odešle příkaz podle popisu s P3=Lc + data a pak odešle příkaz GET RESPONSE (viz část 3.5.6) s P3=Le.

TCS_32 Jsou-li požadovány oba bajty délky a Le=0 (bezpečné předávání zpráv):

— při použití protokolu T=1 karta na Le=0 odpoví odesláním všech výstupních dat, která jsou k dispozici,

— při použití protokolu T=0 vyšle IFD první příkaz s P3=Lc + data a karta odpoví (na toto implicitní Le=0) stavovými bajty '**61La**', kde La je počet dostupných bajtů odpovědi. IFD potom generuje příkaz GET RESPONSE s P3=La pro čtení dat.

TCS_33 Karta tachografu může jako volitelnou funkci podporovat rozšířená pole délky podle ISO/IEC 7816-4. Karta tachografu, která podporuje rozšířená pole délky, musí:

— uvádět podporu rozšířených polí délky v ATR,

— uvádět podporované velikosti vyrovnávacích pamětí v rámci informací o rozšířené délce v EF ATR/INFO, viz TCS_146,

— uvádět, zda podporuje rozšířená pole délky pro T = 1 a/nebo T = 0, v EF Extended Length, viz TCS_147,

— podporovat rozšířená pole délky pro aplikaci tachografu 1. a 2. generace.

Poznámky:

Všechny příkazy jsou specifikovány pro krátká pole délky. Použití APDU s rozšířenou délkou je zřejmé z normy ISO/IEC 7816-4.

Příkazy jsou obecně specifikovány pro otevřený režim, tj. bez bezpečného předávání zpráv, přičemž vrstva bezpečného předávání zpráv je specifikována v dodatku 11. Z pravidel přístupu pro daný příkaz je zřejmé, zda příkaz podporuje bezpečné předávání zpráv či nikoli a zda příkaz musí podporovat bezpečné předávání zpráv 1. generace a/nebo 2. generace. Některé varianty příkazů jsou popsány s bezpečným předáváním zpráv, aby bylo znázorněno použití bezpečného předávání zpráv.

TCS_34 Celek ve vozidle musí pro danou relaci provést celý protokol 2. generace pro vzájemné ověření pravosti celku ve vozidle a karty, včetně ověření certifikátu (je-li požadováno), buď v DF Tachograph, v DF Tachograph_G2, nebo v MF.

3.5.1 *SELECT*

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

Příkaz SELECT se používá:

— k výběru DF aplikace (musí být použit výběr podle názvu),

— k výběru elementárního souboru odpovídajícího uvedenému ID souboru.

3.5.1.1 Výběr podle názvu (AID)

Tento příkaz umožňuje výběr DF aplikace na kartě.

TCS_35 Tento příkaz lze provést odkudkoli ve struktuře souborů (po ATR nebo kdykoliv).

TCS_36 Výběrem aplikace se resetuje aktuální bezpečnostní prostředí. Po provedení výběru aplikace již není vybrán žádný aktuální veřejný klíč. Přístupová podmínka EXT-AUT-G1 je rovněž ztracena. Byl-li příkaz proveden bez bezpečného předávání zpráv, předchozí klíče relace bezpečného předávání zpráv již nejsou dostupné.

TCS_37 **Zpráva s příkazem**

Bajt	Délka	Hodnota	Popis
CLA	1	'00h'	
INS	1	'A4h'	
P1	1	'04h'	Výběr podle názvu (AID)
P2	1	'0Ch'	Neočekává se žádná odpověď
Lc	1	'NNh'	Počet bajtů odeslaných kartě (délka AID): '06h' pro aplikaci tachografu
#6-#(5+NN)	NN	'XX..XXh'	AID: 'FF 54 41 43 48 4F' pro aplikaci tachografu 1. generace AID: 'FF 53 4D 52 44 54' pro aplikaci tachografu 2. generace

Na příkaz SELECT není nutná žádná odpověď (Le chybí v T=1 nebo se nepožaduje odpověď v T=0).

TCS_38 **Zpráva s odpovědí (nepožaduje se odpověď)**

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

— Je-li příkaz úspěšný, karta vrátí '**9000**'.

— Pokud aplikace odpovídající AID není nalezena, je vrácen stav zpracování '**6A82**'.

— Pokud je v T=1 přítomen bajt Le, je vrácen stav zpracování '**6700**'.

— Pokud je v T=0 po příkazu SELECT vyžadována odpověď, je vrácen stav '**6900**'.

— Je-li vybraná aplikace považována za poškozenou (v atributech souboru je detekována chyba integrity), je vrácen stav zpracování '**6400**' nebo '**6581**'.

3.5.1.2 Výběr elementárního souboru pomocí jeho identifikátoru souboru

TCS_39 **Zpráva s příkazem**

TCS_40 Karta tachografu musí pro tuto variantu příkazu podporovat bezpečné předávání zpráv 2. generace, jak je specifikováno v dodatku 11 části B.

Bajt	Délka	Hodnota	Popis
CLA	1	'00h'	
INS	1	'A4h'	
P1	1	'02h'	Výběr EF v rámci aktuálního DF
P2	1	'0Ch'	Neočekává se žádná odpověď
Lc	1	'02h'	Počet bajtů odeslaných kartě
#6-#7	2	'XXXXh'	Identifikátor souboru

Na příkaz SELECT není nutná žádná odpověď (Le chybí v T=1 nebo se nepožaduje odpověď v T=0).

TCS_41 **Zpráva s odpovědí (nepožaduje se odpověď)**

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

— Je-li příkaz úspěšný, karta vrátí '**9000**'.

— Pokud soubor odpovídající identifikátoru souborů není nalezen, je vrácen stav zpracování '**6A82**'.

— Pokud je v T=1 přítomen bajt Le, je vrácen stav zpracování '**6700**'.

— Pokud je v T=0 po příkazu SELECT vyžadována odpověď, je vrácen stav '**6900**'.

— Je-li vybraný soubor považován za poškozený (v atributech souboru je detekována chyba integrity), je vrácen stav zpracování '**6400**' nebo '**6581**'.

3.5.2 *READ BINARY*

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

Příkaz READ BINARY se používá ke čtení dat z transparentního souboru.

Odpověď karty sestává z vrácení přečtených dat, volitelně zapouzdřených ve struktuře bezpečného předávání zpráv.

3.5.2.1 Příkaz s offsetem v P1-P2

Tento příkaz umožňuje IFD číst data z aktuálně vybraného EF bez bezpečného předávání zpráv.

Poznámka: Tento příkaz bez bezpečného předávání zpráv lze použít pouze pro čtení souboru, který podporuje bezpečnostní podmínku ALW pro režim přístupu pro čtení.

TCS_42 **Zpráva s příkazem**

Bajt	Délka	Hodnota	Popis
CLA	1	'00h'	
INS	1	'B0h'	Read Binary
P1	1	'XXh'	Offset v bajtech od začátku souboru: nejvýznamnější bajt
P2	1	'XXh'	Offset v bajtech od začátku souboru: nejméně významný bajt
Le	1	'XXh'	Délka očekávaných dat. Počet bajtů ke čtení.

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

TCS_43 **Zpráva s odpovědí**

Bajt	Délka	Hodnota	Popis
#1-#X	X	'XX..XXh'	Přečtená data
SW	2	'XXXXh'	Stavová slova (SW1, SW2)

— Je-li příkaz úspěšný, karta vrátí '**9000**'.

— Není-li vybrán žádný EF, je vrácen stav zpracování '**6986**'.

— Nejsou-li splněny bezpečnostní podmínky zvoleného souboru, příkaz se přeruší se stavem '**6982**'.

— Není-li offset kompatibilní s velikostí EF (offset > velikost EF), je vrácen stav zpracování '**6B00**'.

— Není-li velikost dat ke čtení kompatibilní s velikostí EF (offset + Le > velikost EF), je vrácen stav zpracování '**6700**' nebo '**6Cxx**', kde 'xx' je přesná délka.

— Je-li v atributech souboru zjištěna chyba integrity, karta považuje soubor za poškozený a neopravitelný a je vrácen stav zpracování '**6400**' nebo '**6581**'.

— Je-li v uložených datech zjištěna chyba integrity, karta vrátí požadovaná data a je vrácen stav zpracování '**6281**'.

3.5.2.1.1 Příkaz s bezpečným předáváním zpráv (příklady)

Tento příkaz umožňuje IFD číst data z aktuálně vybraného EF s bezpečným předáváním zpráv za účelem ověření integrity přijatých dat a ochrany důvěrnosti dat v případě, že se použije bezpečnostní podmínka SM-R-ENC-MAC-G1 (1. generace) nebo SM-R-ENC-MAC-G2 (2. generace).

TCS_44 **Zpráva s příkazem**

Bajt	Délka	Hodnota	Popis
CLA	1	'0Ch'	Požadavek na bezpečné předávání zpráv
INS	1	'B0h'	Read Binary
P1	1	'XXh'	P1 (offset v bajtech od začátku souboru): nejvýznamnější bajt
P2	1	'XXh'	P2 (offset v bajtech od začátku souboru): nejméně významný bajt
Lc	1	'XXh'	Délka vstupních dat pro bezpečné předávání zpráv
#6	1	'97h'	T_{LE}: tag pro specifikaci očekávané délky
#7	1	'01h'	L_{LE}: délka očekávané délky
#8	1	'NNh'	Specifikace očekávané délky (původní Le): počet bajtů ke čtení
#9	1	'8Eh'	T_{CC}: tag pro kryptografický kontrolní součet
#10	1	'XXh'	L_{CC}: 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)
#11-#(10+L)	L	'XX..XXh'	Kryptografický kontrolní součet
Le	1	'00h'	Podle specifikace v ISO/IEC 7816-4

TCS_45 **Zpráva s odpovědí, pokud není požadována podmínka SM-R-ENC-MAC-G1 (1. generace) / SM-R-ENC-MAC-G2 (2. generace) a pokud je správný vstupní formát bezpečného předávání zpráv:**

Bajt	Délka	Hodnota	Popis
#1	1	'99h'	Tag pro stav zpracování (SW1-SW2) – volitelný pro bezpečné předávání zpráv 1. generace
#2	1	'02h'	Délka stavu zpracování
#3 – #4	2	'XX XXh'	Stav zpracování nechráněné APDU odpovědi
#5	1	'81h'	T_{PV}: tag pro otevřená data
#6	L	'NNh' nebo '81 NNh'	L_{PV}: délka vrácených dat (= původní Le). L jsou 2 bajty, jestliže L_{PV} > 127 bajtů.

Bajt	Délka	Hodnota	Popis
#(6+L)-#(5+L+NN)	NN	'XX..XXh'	Otevřená data
#(6+L+NN)	1	'8Eh'	T_{CC}: tag pro kryptografický kontrolní součet
#(7+L+NN)	1	'XXh'	L_{CC}: 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+NN)-#(7+M+L+NN)	M	'XX..XXh'	Kryptografický kontrolní součet
SW	2	'XXXXh'	Stavová slova (SW1, SW2)

TCS_46 **Zpráva s odpovědí, pokud je požadována podmínka SM-R-ENC-MAC-G1 (1. generace) / SM-R-ENC-MAC-G2 (2. generace) a pokud je správný vstupní formát bezpečného předávání zpráv:**

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 $L_{PI\ CG}$ > 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
#(4+L+MM) – #(5+L+MM)	2	'XX XXh'	Stav zpracování nechráněné APDU odpovědi
#(6+L+MM)	1	'8Eh'	T_{CC}: tag pro kryptografický kontrolní součet
#(7+L+MM)	1	'XXh'	L_{CC}: 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)

Příkaz READ BINARY může vracet běžné stavy zpracování uvedené v TCS_43 pod tagem '99h', jak popisuje TCS_59, pomocí struktury odpovědi v rámci bezpečného předávání zpráv.

Navíc se mohou vyskytnout některé chyby, které se týkají konkrétně bezpečného předávání zpráv. V takovém případě je jednoduše vrácen stav zpracování bez použití struktury bezpečného předávání zpráv:

TCS_47 **Zpráva s odpovědí, jestliže je chybný vstupní formát bezpečného předávání zpráv**

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

— Není-li k dispozici žádný aktuální klíč relace, je vrácen stav zpracování '**6A88**'. To se stane tehdy, jestliže klíč relace dosud není vygenerován, nebo jestliže skončila platnost klíče relace (v tomto případě musí IFD zopakovat vzájemný proces ověření totožnosti za účelem stanovení nového klíče relace).

— Jestliže některé očekávané datové objekty (jak je uvedeno výše) ve formátu bezpečného předávání zpráv chybějí, je vrácen stav zpracování '**6987**': tato chyba se objeví, jestliže chybí očekávaný tag nebo jestliže tělo příkazu není správně sestaveno.

— Jsou-li některé datové objekty chybné, je vrácen stav zpracování '**6988**': tato chyba se objeví, jestliže jsou přítomny všechny požadované tagy, ale některé délky se liší od očekávaných.

— Selže-li ověření kryptografického kontrolního součtu, je vrácen stav zpracování '**6688**'.

3.5.2.2 Příkaz s krátkým identifikátorem EF (elementárního souboru)

Tato varianta příkazu umožňuje IFD vybrat EF pomocí krátkého identifikátoru EF a číst data z tohoto EF.

TCS_48 Karta tachografu musí podporovat tuto variantu příkazu pro všechny elementární soubory se specifikovaným krátkým identifikátorem EF. Tyto krátké identifikátory EF jsou specifikovány v kapitole 4.

TCS_49 **Zpráva s příkazem**

Bajt	Délka	Hodnota	Popis
CLA	1	'00h'	
INS	1	'B0h'	Read Binary
P1	1	'XXh'	Bit 8 je nastaven na 1 Bity 7 a 6 jsou nastaveny na 00 Bity 5 – 1 kódují krátký identifikátor EF příslušného EF
P2	1	'XXh'	Kóduje offset od 0 do 255 bajtů v EF, na který odkazuje P1
Le	1	'XXh'	Délka očekávaných dat. Počet bajtů ke čtení.

Poznámka: Krátké identifikátory EF používané pro aplikaci tachografu 2. generace jsou specifikovány v kapitole 4.

Pokud P1 kóduje krátký identifikátor EF a příkaz je úspěšný, identifikovaný EF se stává aktuálně vybraným EF (aktuálním EF).

TCS_50 **Zpráva s odpovědí**

Bajt	Délka	Hodnota	Popis
#1-#L	L	'XX..XXh'	Přečtená data
SW	2	'XXXXh'	Stavová slova (SW1, SW2)

— Je-li příkaz úspěšný, karta vrátí '**9000**'.

— Není-li soubor odpovídající krátkému identifikátoru EF nalezen, je vrácen stav zpracování '**6A82**'.

— Nejsou-li splněny bezpečnostní podmínky zvoleného souboru, příkaz se přeruší se stavem '**6982**'.

— Není-li offset kompatibilní s velikostí EF (offset > velikost EF), je vrácen stav zpracování '**6B00**'.

— Není-li velikost dat ke čtení kompatibilní s velikostí EF (offset + Le > velikost EF), je vrácen stav zpracování '**6700**' nebo '**6Cxx**', kde 'xx' je přesná délka.

— Je-li v atributech souboru zjištěna chyba integrity, karta považuje soubor za poškozený a neopravitelný a je vrácen stav zpracování '**6400**' nebo '**6581**'.

— Je-li v uložených datech zjištěna chyba integrity, karta vrátí požadovaná data a je vrácen stav zpracování '**6281**'.

3.5.2.3 Příkaz s lichým bajtem instrukce

Tato varianta příkazu umožňuje IFD číst data z EF s 32 768 nebo více bajty.

TCS_51 Karta tachografu, která podporuje EF s 32 768 nebo více bajty, podporuje tuto variantu příkazu pro tyto EF. Karta tachografu může, ale nemusí podporovat tuto variantu příkazu pro ostatní EF kromě EF Sensor_Installation_Data, viz TCS_156 a TCS_160.

TCS_52 **Zpráva s příkazem**

Bajt	Délka	Hodnota	Popis
CLA	1	'00h'	
INS	1	'B1h'	Read Binary
P1	1	'00h'	Aktuální EF
P2	1	'00h'	
Lc	1	'NNh'	Lc délka datového objektu offsetu
#6-#(5+NN)	NN	'XX..XXh'	Datový objekt offsetu: Tag '54h' Délka '01h' nebo '02h' Hodnota offset
Le	1	'XXh'	Počet bajtů ke čtení.

IFD kóduje délku datového objektu offsetu s použitím minimálního možného počtu oktetů, tj. s použitím bajtu délky '01h' musí IFD kódovat offset od 0 do 255 a s použitím bajtu délky '02h' offset od 256 do 65 535 bajtů.

TCS_53 **Zpráva s odpovědí**

Bajt	Délka	Hodnota	Popis
#1-#L	L	'XX..XXh'	Čtená data zapouzdřená ve volném datovém objektu s tagem '53h'
SW	2	'XXXXh'	Stavová slova (SW1, SW2)

— Je-li příkaz úspěšný, karta vrátí '**9000**'.

— Není-li vybrán žádný EF, je vrácen stav zpracování '**6986**'.

— Nejsou-li splněny bezpečnostní podmínky zvoleného souboru, příkaz se přeruší se stavem '**6982**'.

— Není-li offset kompatibilní s velikostí EF (offset > velikost EF), je vrácen stav zpracování '**6B00**'.

— Není-li velikost dat ke čtení kompatibilní s velikostí EF (offset + Le > velikost EF), je vrácen stav zpracování '**6700**' nebo '**6Cxx**', kde 'xx' je přesná délka.

— Je-li v atributech souboru zjištěna chyba integrity, karta považuje soubor za poškozený a neopravitelný a je vrácen stav zpracování '**6400**' nebo '**6581**'.

— Je-li v uložených datech zjištěna chyba integrity, karta vrátí požadovaná data a je vrácen stav zpracování '**6281**'.

3.5.2.3.1 Příkaz s bezpečným předáváním zpráv (příklad)

Následující příklad znázorňuje použití bezpečného předávání zpráv, použije-li se bezpečnostní podmínka SM-MAC-G2.

TCS_54 Zpráva s příkazem

Bajt	Délka	Hodnota	Popis
CLA	1	'0Ch'	Požadavek na bezpečné předávání zpráv
INS	1	'B1h'	Read Binary
P1	1	'00h'	Aktuální EF
P2	1	'00h'	
Lc	1	'XXh'	Délka zabezpečeného datového pole
#6	1	'B3h'	Tag pro otevřená data v kódování BER-TLV
#7	1	'NNh'	L_{PV}: délka přenášených dat
#(8)-#(7+NN)	NN	'XX..XXh'	Otevřená data v kódování BER-TLV, tj. datový objekt offsetu s tagem '54'
#(8+NN)	1	'97h'	T_{LE}: tag pro specifikaci očekávané délky
#(9+NN)	1	'01h'	L_{LE}: délka očekávané délky
#(10+NN)	1	'XXh'	Specifikace očekávané délky (původní Le): počet bajtů ke čtení
#(11+NN)	1	'8Eh'	T_{CC}: tag pro kryptografický kontrolní součet
#(12+NN)	1	'XXh'	L_{CC}: délka následujícího kryptografického kontrolního součtu '08h', '0Ch' nebo '10h' v závislosti na délce klíče AES pro bezpečné předávání zpráv 2. generace (viz dodatek 11 část B)
#(13+NN)-#(12+M+NN)	M	'XX..XXh'	Kryptografický kontrolní součet
Le	1	'00h'	Podle specifikace v ISO/IEC 7816-4

TCS_55 Zpráva s odpovědí, je-li příkaz úspěšný

Bajt	Délka	Hodnota	Popis
#1	1	'B3h'	Otevřená data v kódování BER-TLV
#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 v kódování BER-TLV, tj. přečtená data zapouzdřená ve volném datovém objektu s tagem '53h'
#(2+L+NN)	1	'99h'	Stav zpracování nechráněné APDU odpovědi
#(3+L+NN)	1	'02h'	Délka stavu zpracování
#(4+L+NN) – #(5+L+NN)	2	'XX XXh'	Stav zpracování nechráněné APDU odpovědi
#(6+L+NN)	1	'8Eh'	T_{CC}: tag pro kryptografický kontrolní součet
#(7+L+NN)	1	'XXh'	L_{CC}: délka následujícího kryptografického kontrolního součtu '08h', '0Ch' nebo '10h' v závislosti na délce klíče AES pro bezpečné předávání zpráv 2. generace (viz dodatek 11 část B)
#(8+L+NN)-#(7+M+L+NN)	M	'XX..XXh'	Kryptografický kontrolní součet
SW	2	'XXXXh'	Stavová slova (SW1, SW2)

3.5.3 *UPDATE BINARY*

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

Zpráva s příkazem UPDATE BINARY spouští přepis (výmaz + zápis) bitů již přítomných v binárním EF bity poskytnutými v APDU příkazu.

3.5.3.1 Příkaz s offsetem v P1-P2

Tento příkaz umožňuje IFD zapsat data do aktuálně vybraného EF bez toho, aby karta ověřovala integritu přijatých dat.

Poznámka: Tento příkaz bez bezpečného předávání zpráv lze použít pouze pro aktualizaci souboru, který podporuje bezpečnostní podmínku ALW pro režim přístupu pro aktualizaci.

TCS_56 **Zpráva s příkazem**

Bajt	Délka	Hodnota	Popis
CLA	1	'00h'	
INS	1	'D6h'	Update Binary

Bajt	Délka	Hodnota	Popis
P1	1	'XXh'	Offset v bajtech od začátku souboru: nejvýznamnější bajt
P2	1	'XXh'	Offset v bajtech od začátku souboru: nejméně významný bajt
Lc	1	'NNh'	Lc: délka dat k aktualizaci. Počet bajtů k zápisu.
#6-#(5+NN)	NN	'XX..XXh'	Data k zápisu

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

TCS_57 **Zpráva s odpovědí**

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

— Je-li příkaz úspěšný, karta vrátí '**9000**'.

— Není-li vybrán žádný EF, je vrácen stav zpracování '**6986**'.

— Nejsou-li splněny bezpečnostní podmínky zvoleného souboru, příkaz se přeruší se stavem '**6982**'.

— Není-li offset kompatibilní s velikostí EF (offset > velikost EF), je vrácen stav zpracování '**6B00**'.

— Není-li velikost dat k zápisu kompatibilní s velikostí EF (Offset + Lc > velikost EF), je vrácen stav zpracování '**6700**'.

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

— Je-li zápis neúspěšný, je vrácen stav zpracování '**6581**'.

3.5.3.1.1 Příkaz s bezpečným předáváním zpráv (příklady)

Tento příkaz umožňuje IFD zapsat data do aktuálně vybraného EF, přičemž karta ověřuje integritu přijatých dat. Protože není požadováno zajištění důvěrnosti, data nejsou šifrována.

TCS_58 **Zpráva s příkazem**

Bajt	Délka	Hodnota	Popis
CLA	1	'0Ch'	Požadavek na bezpečné předávání zpráv
INS	1	'D6h'	Update Binary
P1	1	'XXh'	Offset v bajtech od začátku souboru: nejvýznamnější bajt
P2	1	'XXh'	Offset v bajtech od začátku souboru: nejméně významný bajt
Lc	1	'XXh'	Délka zabezpečeného datového pole

Bajt	Délka	Hodnota	Popis
#6	1	'81h'	T_{PV}: tag pro otevřená data
#7	L	'NNh' nebo '81 NNh'	L_{PV}: délka přenášených dat. L jsou 2 bajty, jestliže L_{PV} > 127 bajtů.
#(7+L)-#(6+L+NN)	NN	'XX..XXh'	Otevřená data (data k zápisu)
#(7+L+NN)	1	'8Eh'	T_{CC}: tag pro kryptografický kontrolní součet
#(8+L+NN)	1	'XXh'	L_{CC}: 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)
#(9+L+NN)-#(8+M+L+NN)	M	'XX..XXh'	Kryptografický kontrolní součet
Le	1	'00h'	Podle specifikace v ISO/IEC 7816-4

TCS_59 **Zpráva s odpovědí, jestliže je vstupní formát bezpečného předávání zpráv správný**

Bajt	Délka	Hodnota	Popis
#1	1	'99h'	T_{SW}: tag pro stavová slova (chráněna pomocí CC)
#2	1	'02h'	L_{SW}: délka vrácených stavových slov
#3-#4	2	'XXXXh'	Stav zpracování nechráněné APDU odpovědi
#5	1	'8Eh'	T_{CC}: tag pro kryptografický kontrolní součet
#6	1	'XXh'	L_{CC}: 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)
#7-#(6+L)	L	'XX..XXh'	Kryptografický kontrolní součet
SW	2	'XXXXh'	Stavová slova (SW1, SW2)

Běžné stavy zpracování, popsané pro příkaz UPDATE BINARY bez bezpečného předávání zpráv (viz část 3.5.3.1), mohou být vráceny pomocí výše uvedené struktury zprávy s odpovědí.

Navíc se mohou vyskytnout některé chyby, které se týkají konkrétně bezpečného předávání zpráv. V takovém případě je jednoduše vrácen stav zpracování bez použití struktury bezpečného předávání zpráv:

TCS_60 **Zpráva s odpovědí v případě chyby v bezpečném předávání zpráv**

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

— Není-li k dispozici aktuální klíč relace, je vrácen stav zpracování '**6A88**'.

— Jestliže některé očekávané datové objekty (jak je uvedeno výše) ve formátu bezpečného předávání zpráv chybějí, je vrácen stav zpracování '**6987**': tato chyba se objeví, jestliže chybí očekávaný tag nebo jestliže tělo příkazu není správně sestaveno.

— Jsou-li některé datové objekty chybné, je vrácen stav zpracování '**6988**': tato chyba se objeví, jestliže jsou přítomny všechny požadované tagy, ale některé délky se liší od očekávaných.

— Selže-li ověření kryptografického kontrolního součtu, je vrácen stav zpracování '**6688**'.

3.5.3.2 Příkaz s krátkým identifikátorem EF

Tato varianta příkazu umožňuje IFD vybrat EF pomocí krátkého identifikátoru EF a zapsat data z tohoto EF.

TCS_61 Karta tachografu musí podporovat tuto variantu příkazu pro všechny elementární soubory se specifikovaným krátkým identifikátorem EF. Tyto krátké identifikátory EF jsou specifikovány v kapitole 4.

TCS_62 **Zpráva s příkazem**

Bajt	Délka	Hodnota	Popis
CLA	1	'00h'	
INS	1	'D6h'	Update Binary
P1	1	'XXh'	Bit 8 je nastaven na 1 Bity 7 a 6 jsou nastaveny na 00 Bity 5 – 1 kódují krátký identifikátor EF příslušného EF
P2	1	'XXh'	Kóduje offset od 0 do 255 bajtů v EF, na který odkazuje P1
Lc	1	'NNh'	Lc: délka dat k aktualizaci. Počet bajtů k zápisu.
#6-#(5+NN)	NN	'XX..XXh'	Data k zápisu

TCS_63 **Zpráva s odpovědí**

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

Poznámka: Krátké identifikátory EF používané pro aplikaci tachografu 2. generace jsou specifikovány v kapitole 4.

Pokud P1 kóduje krátký identifikátor EF a příkaz je úspěšný, identifikovaný EF se stává aktuálně vybraným EF (aktuálním EF).

— Je-li příkaz úspěšný, karta vrátí '**9000**'.

— Není-li soubor odpovídající krátkému identifikátoru EF nalezen, je vrácen stav zpracování '**6A82**'.

— Nejsou-li splněny bezpečnostní podmínky zvoleného souboru, příkaz se přeruší se stavem '**6982**'.

— Není-li offset kompatibilní s velikostí EF (offset > velikost EF), je vrácen stav zpracování '**6B00**'.

— Není-li velikost dat k zápisu kompatibilní s velikostí EF (Offset + Lc > velikost EF), je vrácen stav zpracování '**6700**'.

— Je-li v atributech souboru zjištěna chyba integrity, karta považuje soubor za poškozený a neopravitelný a je vrácen stav zpracování '**6400**' nebo '**6581**'.

— Je-li zápis neúspěšný, je vrácen stav zpracování '**6581**'.

3.5.3.3 Příkaz s lichým bajtem instrukce

Tato varianta příkazu umožňuje IFD zapisovat data do EF s 32 768 nebo více bajty.

TCS_64 Karta tachografu, která podporuje EF s 32 768 nebo více bajty, podporuje tuto variantu příkazu pro tyto EF. Karta tachografu může, ale nemusí podporovat tuto variantu příkazu pro ostatní EF.

TCS_65 **Zpráva s příkazem**

Bajt	Délka	Hodnota	Popis
CLA	1	'00h'	
INS	1	'D7h'	Update Binary
P1	1	'00h'	Aktuální EF
P2	1	'00h'	
Lc	1	'NNh'	Lc délka dat v datovém poli příkazu
#6-#(5+NN)	NN	'XX..XXh'	Datový objekt offsetu s tagem '54h' || volný datový objekt s tagem '53h', který zapouzdřuje data k zápisu

IFD kóduje délku datového objektu offsetu a volného datového objektu s použitím minimálního možného počtem oktetů, tj. pomocí bajtu délky '01h' musí IFD kódovat offset/délku od 0 do 255 a pomocí bajtu délky '02h' offset/délku od 256 do 65 535 bajtů.

TCS_66 **Zpráva s odpovědí**

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

— Je-li příkaz úspěšný, karta vrátí '**9000**'.

— Není-li vybrán žádný EF, je vrácen stav zpracování '**6986**'.

— Nejsou-li splněny bezpečnostní podmínky zvoleného souboru, příkaz se přeruší se stavem '**6982**'.

— Není-li offset kompatibilní s velikostí EF (offset > velikost EF), je vrácen stav zpracování '**6B00**'.

— Není-li velikost dat k zápisu kompatibilní s velikostí EF (Offset + Lc > velikost EF), je vrácen stav zpracování '**6700**'.

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

— Je-li zápis neúspěšný, je vrácen stav zpracování '**6581**'.

3.5.3.3.1 Příkaz s bezpečným předáváním zpráv (příklad)

Následující příklad znázorňuje použití bezpečného předávání zpráv, použije-li se bezpečnostní podmínka SM-MAC-G2.

TCS_67 Zpráva s příkazem

Bajt	Délka	Hodnota	Popis
CLA	1	'0Ch'	Požadavek na bezpečné předávání zpráv
INS	1	'D7h'	Update Binary
P1	1	'00h'	Aktuální EF
P2	1	'00h'	
Lc	1	'XXh'	Délka zabezpečeného datového pole
#6	1	'B3h'	Tag pro otevřená data v kódování BER-TLV
#7	L	'NNh' nebo '81 NNh'	L_{PV}: délka přenášených dat. L jsou 2 bajty, jestliže L_{PV} > 127 bajtů.
#(7+L)-#(6+L+NN)	NN	'XX..XXh'	Otevřená data v kódování BER-TLV, tj. datový objekt offsetu s tagem '54h' || volný datový objekt s tagem '53h', který zapouzdřuje data k zápisu
#(7+L+NN)	1	'8Eh'	T_{CC}: tag pro kryptografický kontrolní součet
#(8+L+NN)	1	'XXh'	L_{CC}: délka následujícího kryptografického kontrolního součtu '08h', '0Ch' nebo '10h' v závislosti na délce klíče AES pro bezpečné předávání zpráv 2. generace (viz dodatek 11 část B)
#(9+L+NN)-#(8+M+L+NN)	M	'XX..XXh'	Kryptografický kontrolní součet
Le	1	'00h'	Podle specifikace v ISO/IEC 7816-4

TCS_68 Zpráva s odpovědí, je-li příkaz úspěšný

Bajt	Délka	Hodnota	Popis
#1	1	'99h'	T_{SW}: tag pro stavová slova (chráněna pomocí CC)
#2	1	'02h'	L_{SW}: délka vrácených stavových slov
#3-#4	2	'XXXXh'	Stav zpracování nechráněné APDU odpovědi
#5	1	'8Eh'	T_{CC}: tag pro kryptografický kontrolní součet

Bajt	Délka	Hodnota	Popis
#6	1	'XXh'	L_{CC}: délka následujícího kryptografického kontrolního součtu '08h', '0Ch' nebo '10h' v závislosti na délce klíče AES pro bezpečné předávání zpráv 2. generace (viz dodatek 11 část B)
#7-#(6+L)	L	'XX..XXh'	Kryptografický kontrolní součet
SW	2	'XXXXh'	Stavová slova (SW1, SW2)

3.5.4 *GET CHALLENGE*

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

Příkaz GET CHALLENGE žádá kartu o vyslání výzvy pro použití v postupu souvisejícím se zabezpečením, v rámci nějž se kartě pošle kryptogram nebo šifrovaná data.

TCS_69 Kartou vydaná výzva je platná pouze pro následující příkaz poslaný kartě, který výzvu používá.

TCS_70 **Zpráva s příkazem**

Bajt	Délka	Hodnota	Popis
CLA	1	'00h'	
INS	1	'84h'	INS
P1	1	'00h'	P1
P2	1	'00h'	P2
Le	1	'08h'	Le (očekávaná délka výzvy).

TCS_71 **Zpráva s odpovědí**

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

— Je-li příkaz úspěšný, karta vrátí '**9000**'.

— Pokud se Le liší od '08h', stav zpracování je '**6700**'.

— Jestliže jsou chybné parametry P1-P2, stav zpracování je '**6A86**'.

3.5.5 *VERIFY*

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

Tento příkaz musí podporovat pouze karta dílny.

Ostatní typy karet tachografu mohou, ale nemusí tento příkaz implementovat, ale pro tyto karty není personalizována žádná referenční hodnota CHV. Proto tyto karty nemohou tento příkaz úspěšně provést. Pro typy karet tachografu jiné než kartu dílny je chování, tj. vracený chybový kód, mimo oblast působnosti této specifikace, je-li tento příkaz odeslán.

Příkaz VERIFY spouští na kartě porovnání dat CHV (kódu PIN) zaslaných z příkazu s referenční hodnotou CHV uloženou na kartě.

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.

TCS_73 Aplikace tachografu 1. a 2. generace používají stejnou referenční hodnotu CHV.

TCS_74 Karta tachografu zkontroluje, zda je příkaz správně kódován. Není-li příkaz kódován správně, karta neporovná hodnoty CHV, nesníží čítač zbývajících pokusů o ověření CHV a neresetuje bezpečnostní status „PIN_Verified", ale příkaz přeruší. Příkaz je kódován správně, mají-li bajty CLA, INS, P1, P2, Lc stanovené hodnoty, Le chybí a datové pole příkazu má správnou délku.

TCS_75 Je-li příkaz úspěšný, je čítač zbývajících pokusů o ověření CHV nastaven zpět na počáteční hodnotu. Počáteční hodnota čítače zbývajících pokusů o ověření CHV je 5. Je-li příkaz úspěšný, musí karta nastavit vnitřní bezpečnostní status „PIN_Verified". Karta resetuje tento bezpečnostní status, pokud je resetována karta nebo pokud kód CHV přenesený v příkazu neodpovídá uložené referenční hodnotě CHV.

Poznámka: používání stejné referenční hodnoty CHV a globálního bezpečnostního statusu zabraňují tomu, aby pracovník dílny musel po výběru jiného DF aplikace tachografu znovu zadávat PIN.

TCS_76 Neúspěšné porovnání se na kartě zaznamená, tj. čítač zbývajících pokusů o ověření CHV se sníží o jedničku, aby se omezil počet dalších pokusů o použití referenční hodnoty CHV.

TCS_77 **Zpráva s příkazem**

Bajt	Délka	Hodnota	Popis
CLA	1	'00h'	
INS	1	'20h'	INS
P1	1	'00h'	P1
P2	1	'00h'	P2 (ověřovaná hodnota CHV je implicitně známa)
Lc	1	'08h'	Délka přenášeného kódu CHV
#6-#13	8	'XX..XXh'	CHV

TCS_78 **Zpráva s odpovědí**

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

— Je-li příkaz úspěšný, karta vrátí '**9000**'.

— Není-li referenční hodnota CHV nalezena, je vrácen stav zpracování '**6A88**'.

— Je-li CHV zablokována (čítač zbývajících pokusů o ověření CHV je na nule), je vrácen stav zpracování '**6983**'. Po dosažení tohoto stavu už nelze nikdy úspěšně předložit CHV.

— Jestliže je porovnání neúspěšné, čítač zbývajících pokusů se sníží a je vrácen stav '**63CX**' (X>0 a X se rovná čítači zbývajících pokusů o ověření CHV).

— Je-li referenční hodnota CHV považována za poškozenou, je vrácen stav zpracování '**6400**' nebo '**6581**'.

— Pokud se Lc liší od '08h', stav zpracování je '**6700**'.

3.5.6 *GET RESPONSE*

Tento příkaz je v souladu s normou ISO/IEC 7816-4.

Tento příkaz (potřebný a dostupný pouze pro protokol T=0) slouží k přenosu připravených dat z karty do zařízení rozhraní (případ, kdy příkaz obsahoval jak Lc, tak Le).

Příkaz GET RESPONSE musí být vydán ihned po příkazu, který připravuje data, jinak jsou data ztracena. Po provedení příkazu GET RESPONSE (nevyskytne-li se chyba '**61xx**' nebo '**6Cxx**', viz dále) dříve připravená data již nejsou k dispozici.

TCS_79 **Zpráva s příkazem**

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

TCS_80 **Zpráva s odpovědí**

Bajt	Délka	Hodnota	Popis
#1-#X	X	'XX..XXh'	Data
SW	2	'XXXXh'	Stavová slova (SW1, SW2)

— Je-li příkaz úspěšný, karta vrátí '**9000**'.

— Pokud karta nepřipravila žádná data, je vrácen stav zpracování '**6900**' nebo '**6F00**'.

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

— Jestliže Le není nula a je menší než počet dostupných bajtů, karta normálně pošle požadovaná data a je vrácen stav zpracování '**61xx**', kde 'xx' udává počet dodatečných bajtů, které jsou nadále k dispozici pro následný příkaz GET RESPONSE.

— Jestliže příkaz není podporován (protokol T=1), karta vrátí '**6D00**'.

3.5.7 *PSO: VERIFY CERTIFICATE*

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

Příkaz VERIFY CERTIFICATE je používán kartou k získání veřejného klíče zvenku a ke kontrole jeho platnosti.

3.5.7.1 Pár příkaz – odpověď 1. generace

TCS_81 Tuto variantu příkazu podporuje pouze aplikace tachografu 1. generace.

TCS_82 Pokud je příkaz VERIFY CERTIFICATE úspěšný, veřejný klíč je uložen k budoucímu použití v bezpečnostním prostředí. Tento klíč je explicitně nastaven pro použití v příkazech vztahujících se k zabezpečení (INTERNAL AUTHENTICATE, EXTERNAL AUTHENTICATE nebo VERIFY CERTIFICATE) pomocí příkazu MSE (viz část 3.5.11) s použitím jeho identifikátoru klíče.

TCS_83 V každém případě příkaz VERIFY CERTIFICATE používá veřejný klíč dříve vybraný příkazem MSE k otevření certifikátu. Musí se jednat o veřejný klíč členského státu nebo Evropy.

TCS_84 **Zpráva s příkazem**

Bajt	Délka	Hodnota	Popis
CLA	1	'00h'	
INS	1	'2Ah'	Perform Security Operation
P1	1	'00h'	P1
P2	1	'AEh'	P2: data, která nejsou v kódování BER-TLV (zřetězení datových prvků)
Lc	1	'C2h'	Lc: délka certifikátu, 194 bajtů
#6-#199	194	'XX..XXh'	Certifikát: zřetězení datových prvků (jak je popsáno v dodatku 11)

TCS_85 **Zpráva s odpovědí**

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

— Je-li příkaz úspěšný, karta vrátí '**9000**'.

— Jestliže se ověření certifikátu nezdaří, je vrácen stav zpracování '**6688**'. Proces ověření a rozbalení certifikátu je popsán v dodatku 11 pro G1 a G2.

— Jestliže v bezpečnostním prostředí není žádný veřejný klíč, je vráceno '**6A88**'.

— Jestliže se vybraný veřejný klíč (použitý k rozbalení certifikátu) považuje za poškozený, je vrácen stav zpracování '**6400**' nebo '**6581**'.

— Pouze 1. generace: Jestliže má vybraný veřejný klíč (použitý k rozbalení certifikátu) CHA.LSB (`CertificateHolderAuthorisation.equipmentType`) rozdílný od '00' (např. nejde o certifikát členského státu nebo Evropy), je vrácen stav zpracování '**6985**'.

3.5.7.2 Pár příkaz – odpověď 2. generace

V závislosti na velikosti křivky mohou být certifikáty ECC tak dlouhé, že je nelze přenést v jedné APDU. V takovém případě je třeba použít zřetězení příkazů podle ISO/IEC 7816-4 a přenést certifikát ve dvou po sobě následujících APDU příkazu PSO: VERIFY CERTIFICATE.

Struktura certifikátu a parametry domény jsou definovány v dodatku 11.

TCS_86 Příkaz lze provést v MF, DF Tachograph a DF Tachograph_G2, viz rovněž TCS_33.

TCS_87 **Zpráva s příkazem**

Bajt	Délka	Hodnota	Popis
CLA	1	'X0h'	Bajt CLA označující zřetězení příkazů: '00h' – jediný nebo poslední příkaz řetězce '10h' – nikoli poslední příkaz řetězce
INS	1	'2Ah'	Perform Security Operation
P1	1	'00h'	
P2	1	'BEh'	Verify self-descriptive certificate
Lc	1	'XXh'	Délka datového pole příkazu, viz TCS_88 a TCS_89
#6-#5+L	L	'XX..XXh'	Data v kódování DER-TLV: datový objekt těla certifikátu ECC jako první datový objekt zřetězený s datovým objektem podpisu certifikátu ECC jako druhým datovým objektem, nebo část tohoto zřetězení. Tag '7F21' a příslušná délka se nepřenášejí. Pořadí těchto datových objektů je pevné.

TCS_88 Pro APDU s krátkou délkou platí tato ustanovení: IFD musí použít minimální počet APDU potřebných pro přenesení přenášených dat příkazu a přenést maximální počet bajtů v APDU prvního příkazu podle hodnoty bajtu IFSC, viz TCS_14. Chová-li se IFD odlišně, je chování karty mimo oblast působnosti.

TCS_89 Pro APDU s rozšířenou délkou platí tato ustanovení: Nevejde-li se certifikát do jedné APDU, musí karta podporovat řetězení příkazů. IFD musí použít minimální počet APDU potřebných pro přenesení přenášených dat příkazu a přenést maximální počet bajtů v APDU prvního příkazu. Chová-li se IFD odlišně, je chování karty mimo oblast působnosti.

Poznámka: V souladu s dodatkem 11 uloží karta certifikát nebo relevantní obsah certifikátu a aktualizuje svou hodnotu currentAuthenticatedTime.

Struktura zprávy s odpovědí a stavové bajty jsou definovány v TCS_85.

TCS_90 Kromě chybových kódů uvedených v TCS_85 může karta vrátit tyto chybové kódy:

— Jestliže vybraný veřejný klíč (použitý k rozbalení certifikátu) má CHA.LSB (CertificateHolderAuthorisation.equipmentType), který není vhodný pro ověření certifikátu podle dodatku 11, je vrácen stav zpracování '**6985**'.

— Je-li currentAuthenticatedTime karty pozdější než datum skončení platnosti certifikátu, je vrácen stav zpracování '**6985**'.

— Je-li očekáván poslední příkaz řetězce, karta vrátí '**6883**'.

— Jsou-li v datovém poli příkazu odeslány chybné parametry, karta vrátí '**6A80**' (použije se rovněž v případě, že datové objekty nejsou odeslány ve stanoveném pořadí).

3.5.8 *INTERNAL AUTHENTICATE*

Tento příkaz je v souladu s normou ISO/IEC 7816-4.

TCS_91 Všechny karty tachografu podporují tento příkaz v DF Tachograph 1. generace. Příkaz může, ale nemusí být přístupný v MF a/nebo DF Tachograph_G2. Pokud je příkaz dostupný, skončí vhodným chybovým kódem, protože soukromý klíč karty (Card.SK) pro protokol ověření pravosti 1. generace je přístupný pouze v DF_Tachograph 1. generace.

Použitím příkazu INTERNAL AUTHENTICATE může IFD ověřit pravost karty. Proces ověření pravosti je popsán v dodatku 11. Zahrnuje následující výroky:

TCS_92 Příkaz INTERNAL AUTHENTICATE pomocí soukromého klíče karty (implicitně vybraného) podepíše data pro ověření pravosti včetně K1 (první element pro dohodu na klíči relace) a RND1 a pomocí aktuálně vybraného (pomocí posledního příkazu MSE) veřejného klíče zašifruje podpis a vytvoří ověřovací token (další podrobnosti v dodatku 11).

TCS_93 **Zpráva s příkazem**

Bajt	Délka	Hodnota	Popis
CLA	1	'00h'	CLA
INS	1	'88h'	INS
P1	1	'00h'	P1
P2	1	'00h'	P2
Lc	1	'10h'	Délka dat poslaných kartě
#6 – #13	8	'XX..XXh'	Výzva použitá k ověření pravosti karty
#14 -#21	8	'XX..XXh'	VU.CHR (viz dodatek 11)
Le	1	'80h'	Délka dat očekávaných z karty

TCS_94 **Zpráva s odpovědí**

Bajt	Délka	Hodnota	Popis
#1-#128	128	'XX..XXh'	Ověřovací token karty (viz dodatek 11)
SW	2	'XXXXh'	Stavová slova (SW1, SW2)

— Je-li příkaz úspěšný, karta vrátí '**9000**'.

— Jestliže v bezpečnostním prostředí není žádný veřejný klíč, je vrácen stav zpracování '**6A88**'.

— Jestliže v bezpečnostním prostředí není žádný soukromý klíč, je vrácen stav zpracování '**6A88**'.

— Jestliže VU.CHR neodpovídá identifikátoru aktuálního veřejného klíče, je vrácen stav zpracování '**6A88**'.

— Je-li vybraný soukromý klíč považován za poškozený, je vrácen stav zpracování '**6400**' nebo '**6581**'.

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

3.5.9 *EXTERNAL AUTHENTICATE*

Tento příkaz je v souladu s normou ISO/IEC 7816-4.

Použitím příkazu EXTERNAL AUTHENTICATE může karta ověřit pravost IFD. Proces ověření pravosti je popsán v dodatku 11 pro Tachograph G1 a G2 (ověření pravosti celku ve vozidle).

TCS_96 Varianta příkazu pro mechanismus vzájemného ověření pravosti 1. generace je podporována pouze aplikací tachografu 1. generace.

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.

TCS_98 **Zpráva s příkazem**

Bajt	Délka	Hodnota	Popis
CLA	1	'00h'	CLA
INS	1	'82h'	INS
P1	1	'00h'	Klíče a algoritmy jsou implicitně známé
P2	1	'00h'	
Lc	1	'XXh'	Lc (délka dat poslaných kartě)
#6-#(5+L)	L	'XX..XXh'	Ověření pravosti 1. generace: kryptogram (viz dodatek 11 část A) Ověření pravosti 2. generace: podpis vytvořený IFD (viz dodatek 11 část B)

TCS_99 **Zpráva s odpovědí**

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

— Je-li příkaz úspěšný, karta vrátí '**9000**'.

— Jestliže CHA aktuálně nastaveného veřejného klíče není zřetězením AID aplikace tachografu a typu zařízení celku ve vozidle, je vrácen stav zpracování '**6F00**'.

— Nepředchází-li příkazu bezprostředně příkaz GET CHALLENGE, je vrácen stav zpracování '**6985**'.

Aplikace tachografu 1. generace může vrátit tyto další chybové kódy:

— Jestliže v bezpečnostním prostředí není žádný veřejný klíč, je vráceno '**6A88**'.

— Jestliže v bezpečnostním prostředí není žádný soukromý klíč, je vrácen stav zpracování '**6A88**'.

— Je-li ověření kryptogramu chybné, je vrácen stav zpracování '**6688**'.

— Je-li vybraný soukromý klíč považován za poškozený, je vrácen stav zpracování '**6400**' nebo '**6581**'.

Varianta příkazu pro ověření pravosti 2. generace může vrátit tento další chybový kód:

— Nezdaří-li se ověření podpisu, karta vrátí '**6300**'.

3.5.10 *GENERAL AUTHENTICATE*

Tento příkaz se používá pro protokol ověření pravosti čipu 2. generace stanovený v dodatku 11 části B a je v souladu s ISO/IEC 7816-4.

TCS_100 Příkaz lze provést v MF, DF Tachograph a DF Tachograph_G2, viz rovněž TCS_34.

TCS_101 **Zpráva s příkazem**

Bajt	Délka	Hodnota	Popis
CLA	1	'00h'	
INS	1	'86h'	
P1	1	'00h'	Klíče a protokol jsou implicitně známé
P2	1	'00h'	
Lc	1	'NNh'	Lc: délka následujícího datového pole
#6-#(5+L)	L	'7Ch' + L_{7C} + '80h' + L_{80} + 'XX..XXh'	Hodnota dočasného veřejného klíče v kódování DER-TLV (viz dodatek 11) Celek ve vozidle odešle datové objekty v tomto pořadí

TCS_102 **Zpráva s odpovědí**

Bajt	Délka	Hodnota	Popis
#1-#L	L	'7Ch' + L_{7C} + '81h' + '08h' + 'XX..XXh' + '82h' + L_{82} + 'XX..XXh'	Data pro dynamické ověření pravosti v kódování DER-TLV: hodnota nonce a ověřovací token (viz dodatek 11)
SW	2	'XXXXh'	Stavová slova (SW1, SW2)

— Je-li příkaz úspěšný, karta vrátí '**9000**'.

— Karta vrátí '**6A80**' k indikaci chybných parametrů v datovém poli.

— Karta vrátí '**6982**', nebyl-li úspěšně proveden příkaz EXTERNAL AUTHENTICATE.

Datový objekt pro dynamické ověření pravosti '7Ch' v odpovědi

— musí být přítomen, je-li operace úspěšná, tj. stavová slova jsou '**9000**',

— nesmí být přítomen v případě chyby provádění nebo chyby kontroly, tj. jsou-li stavová slova v rozsahu '**6400**'–'**6FFF**', a

— nemusí být přítomen v případě varování, tj. jsou-li stavová slova v rozsahu '**6200**'–'**63FF**'.

3.5.11 *MANAGE SECURITY ENVIRONMENT*

Tento příkaz slouží k nastavení veřejného klíče pro účely ověření pravosti.

3.5.11.1 Pár příkaz – odpověď 1. generace

Tento příkaz je v souladu s normou ISO/IEC 7816-4. Jeho použití je ale ve srovnání se související normou omezené.

TCS_103 Tento příkaz je podporován pouze aplikací tachografu 1. generace.

TCS_104 Klíč, na který se odkazuje v datovém poli MSE, zůstává aktuálním veřejným klíčem až do příštího správného příkazu MSE, výběru DF nebo resetu karty.

TCS_105 Jestliže klíč, na který se odkazuje, není (dosud) na kartě k dispozici, bezpečnostní prostředí zůstává nezměněno.

TCS_106 **Zpráva s příkazem**

Bajt	Délka	Hodnota	Popis
CLA	1	'00h'	CLA
INS	1	'22h'	INS
P1	1	'C1h'	P1: odkazovaný klíč, platí pro všechny kryptografické operace
P2	1	'B6h'	P2 (odkazovaná data týkající se digitálního podpisu)
Lc	1	'0Ah'	Lc: délka následujícího datového pole
#6	1	'83h'	Tag pro odkaz na veřejný klíč v asymetrických případech
#7	1	'08h'	Délka odkazu na klíč (identifikátoru klíče)
#8-#15	8	'XX..XXh'	Identifikátor klíče podle specifikace v dodatku 11

TCS_107 **Zpráva s odpovědí**

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

— Je-li příkaz úspěšný, karta vrátí '**9000**'.

— Pokud klíč, na který se odkazuje, není na kartě přítomen, je vrácen stav zpracování '**6A88**'.

— Pokud ve formátu bezpečného předávání zpráv chybějí některé očekávané datové objekty, je vrácen stav zpracování '**6987**'. To může nastat, když chybí tag '83h'.

— Jsou-li některé datové objekty chybné, je vrácen stav zpracování '**6988**'. To může nastat, když délka identifikátoru klíče není '08h'.

— Je-li vybraný klíč považován za poškozený, je vrácen stav zpracování '**6400**' nebo '**6581**'.

3.5.11.2 Páry příkaz – odpověď 2. generace

Pro ověření pravosti 2. generace karta tachografu podporuje následující verze příkazu MSE: Set, které jsou v souladu s normou ISO/IEC 7816-4. Tyto verze příkazu nejsou podporovány pro ověření pravosti 1. generace.

3.5.11.2.1 MSE:SET AT pro ověření pravosti čipu

Následující příkaz MSE:SET AT se používá pro výběr parametrů k ověření pravosti čipu, které se provádí následným příkazem GENERAL AUTHENTICATE.

TCS_108 Příkaz lze provést v MF, DF Tachograph a DF Tachograph_G2, viz rovněž TCS_34.

TCS_109 **Zpráva s příkazem MSE:SET AT pro ověření pravosti čipu**

Bajt	Délka	Hodnota	Popis
CLA	1	'00h'	
INS	1	'22h'	

Bajt	Délka	Hodnota	Popis
P1	1	'41h'	Nastavit pro interní ověření pravosti
P2	1	'A4h'	Ověření pravosti
Lc	1	'NNh'	Lc: délka následujícího datového pole
#6-#(5+L)	L	'80h' + '0Ah' + 'XX..XXh'	Odkaz na kryptografický mechanismus v kódování DER-TLV: identifikátor objektu ověření pravosti čipu (pouze hodnota, tag '06h' je vynechán). Hodnoty identifikátorů objektů viz dodatek 1; používá se bajtová notace. Pokyny, jak vybrat jeden z těchto identifikátorů objektů, viz dodatek 11.

3.5.11.2.2 MSE:SET AT pro ověření pravosti celku ve vozidle

Následující příkaz MSE:SET AT se používá pro výběr parametrů a klíčů pro ověření pravosti celku ve vozidle, které se provádí pomocí následného příkazu EXTERNAL AUTHENTICATE.

TCS_110 Příkaz lze provést v MF, DF Tachograph a DF Tachograph_G2, viz rovněž TCS_34.

TCS_111 **Zpráva s příkazem MSE:SET AT pro ověření pravosti celku ve vozidle**

Bajt	Délka	Hodnota	Popis
CLA	1	'00h'	
INS	1	'22h'	
P1	1	'81h'	Nastavit pro externí ověření pravosti
P2	1	'A4h'	Ověření pravosti
Lc	1	'NNh'	Lc: délka následujícího datového pole
#6-#(5+L)	L	'80h' + '0Ah' + 'XX..XXh'	Odkaz na kryptografický mechanismus v kódování DER-TLV: identifikátor objektu ověření pravosti celku ve vozidle (pouze hodnota, tag '06h' je vynechán). Hodnoty identifikátorů objektů viz dodatek 1; používá se bajtová notace. Pokyny, jak vybrat jeden z těchto identifikátorů objektů, viz dodatek 11.
		'83h' + '08h' + 'XX..XXh'	Odkaz na veřejný klíč VU v kódování DER-TLV s využitím reference držitele certifikátu uvedené v jeho certifikátu
		'91h' + L_{91} + 'XX..XXh'	Komprimovaná podoba dočasného veřejného klíče celku ve vozidle v kódování DER-TLV, která se použije při ověření pravosti čipu (viz dodatek 11)

3.5.11.2.3 MSE:SET DST

Následující příkaz MSE:SET DST se používá pro nastavení veřejného klíče, a to buď

— pro ověření podpisu, který je poskytnut v následném příkazu PSO: VERIFY DIGITAL SIGNATURE, nebo

— pro ověření podpisu certifikátu, který je poskytnut v následném příkazu PSO: VERIFY CERTIFICATE.

TCS_112 Příkaz lze provést v MF, DF Tachograph a DF Tachograph_G2, viz rovněž TCS_33.

TCS_113 **Zpráva s příkazem MSE:SET DST**

Bajt	Délka	Hodnota	Popis
CLA	1	'00h'	
INS	1	'22h'	
P1	1	'81h'	Nastavit pro ověření
P2	1	'B6h'	Digitální podpis
Lc	1	'NNh'	Lc: délka následujícího datového pole
#6-#(5+L)	L	'83h' + '08h' + 'XX...XXh'	Odkaz na veřejný klíč v kódování DER-TLV, tj. reference držitele certifikátu v certifikátu veřejného klíče (viz dodatek 11)

Pro všechny verze příkazu jsou struktura zprávy s odpovědí a stavová slova dány takto:

TCS_114 **Zpráva s odpovědí**

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

— Je-li příkaz úspěšný, karta vrátí '**9000**'. Protokol byl vybrán a inicializován.

— '**6A80**' označuje nesprávné parametry v datovém poli příkazu.

— '**6A88**' označuje, že data, na která se odkazuje (tj. klíč, na který se odkazuje), nejsou k dispozici.

3.5.12 *PSO: HASH*

Tento příkaz slouží k přenosu výsledku výpočtu hodnoty hash nějakých dat na kartu. Tento příkaz se používá k ověření digitálních podpisů. Hodnota hash se dočasně uloží pro následný příkaz PSO: VERIFY DIGITAL SIGNATURE.

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

Tento příkaz musí podporovat pouze kontrolní karta v DF Tachograph a DF Tachograph_G2.

Ostatní typy karet tachografu mohou, ale nemusí tento příkaz implementovat. Příkaz může, ale nemusí být přístupný v MF.

Aplikace kontrolní karty 1. generace podporuje pouze SHA-1.

TCS_115 Dočasně uložená hodnota hash se smaže, pokud je pomocí příkazu PSO: HASH vypočítána nová hodnota hash, pokud je zvolen DF a pokud je resetována karta tachografu.

TCS_116 **Zpráva s příkazem**

Bajt	Délka	Hodnota	Popis
CLA	1	'00h'	CLA
INS	1	'2Ah'	Perform Security Operation
P1	1	'90h'	Vrátit hodnotu hash
P2	1	'A0h'	Tag: datové pole obsahuje příslušné DO pro hašování
Lc	1	'XXh'	Délka Lc následujícího datového pole
#6	1	'90h'	Tag pro hodnotu hash
#7	1	'XXh'	Délka L hodnoty hash: '14h' v aplikaci 1. generace (viz dodatek 11 část A) '20h', '30h' nebo '40h' v aplikaci 2. generace (viz dodatek 11 část B)
#8-#(7+L)	L	'XX..XXh'	Hodnota hash

TCS_117 **Zpráva s odpovědí**

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

— Je-li příkaz úspěšný, karta vrátí '**9000**'.

— Chybějí-li některé očekávané datové objekty (jak je specifikováno výše), je vrácen stav zpracování '**6987**'. To může nastat, když chybí jeden z tagů '90h'.

— Jsou-li některé datové objekty chybné, je vrácen stav zpracování '**6988**'. Tato chyba nastane, když je přítomen potřebný tag, ale s jinou délkou než '14h' pro SHA-1, '20h' pro SHA-256, '30h' pro SHA-384, '40h' pro SHA-512 (aplikace 2. generace).

3.5.13 *PERFORM HASH of FILE*

Tento příkaz není v souladu s normou ISO/IEC 7816-8. Proto bajt CLA tohoto příkazu indikuje proprietární použití příkazu PERFORM SECURITY OPERATION / HASH.

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 tento příkaz implementuje karta podniku nebo kontrolní karta, je příkaz implementován podle specifikace v této kapitole.

Příkaz může, ale nemusí být přístupný v MF. Pokud je přístupný, je implementován podle specifikace v této kapitole, tj. neumožní výpočet hodnoty hash, ale skončí s vhodným chybovým kódem.

TCS_118 Příkaz PERFORM HASH OF FILE se používá pro výpočet hodnoty hash datové oblasti aktuálně vybraného transparentního EF.

TCS_119 Karta tachografu podporuje tento příkaz pouze pro ty EF, které jsou uvedeny v kapitole 4 v rámci DF_Tachograph a DF_Tachograph_G2 s následující výjimkou. Karta tachografu nepodporuje tento příkaz pro EF Sensor_Installation_Data v DF Tachograph_G2.

TCS_120 Výsledek operace hašování se dočasně uloží na kartě. Poté může být použit k získání digitálního podpisu souboru pomocí příkazu PSO: COMPUTE DIGITAL SIGNATURE.

TCS_121 Dočasně uložená hodnota hash souboru se smaže, pokud je pomocí příkazu PSO: HASH OF FILE vypočítána nová hodnota hash souboru, pokud je zvolen DF a pokud je resetována karta tachografu.

TCS_122 Aplikace tachografu 1. generace podporuje algoritmus SHA-1.

TCS_123 Aplikace tachografu 2. generace podporuje algoritmy SHA-1 a SHA-2 (256, 384 a 512 bitů).

TCS_124 **Zpráva s příkazem**

Bajt	Délka	Hodnota	Popis
CLA	1	'80h'	CLA
INS	1	'2Ah'	Perform Security Operation
P1	1	'90h'	Tag: Hash
P2	1	'XXh'	P2: označuje algoritmus, který se má použít pro výpočet hodnoty hash z dat aktuálně vybraného transparentního souboru: '00h' pro SHA-1 '01h' pro SHA-256 '02h' pro SHA-384 '03h' pro SHA-512

TCS_125 **Zpráva s odpovědí**

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

— Je-li příkaz úspěšný, karta vrátí '**9000**'.

— Pokud aktuální EF nedovoluje tento příkaz (EF Sensor_Installation_Data v DF Tachograph_G2), je vrácen stav zpracování '**6985**'.

— Je-li vybraný EF považován za poškozený (chyby integrity atributů souboru nebo uložených dat), je vrácen stav zpracování '**6400**' nebo '**6581**'.

— Pokud zvolený soubor není transparentním souborem nebo neexistuje aktuální EF, je vrácen stav zpracování '**6986**'.

3.5.14 *PSO: COMPUTE DIGITAL SIGNATURE*

Tento příkaz se používá pro výpočet digitálního podpisu dříve vypočtené hodnoty hash (viz PERFORM HASH OF FILE, část 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, nemají však podpisový klíč. Proto tyto karty nemohou příkaz úspěšně provést, ale ukončí jej s vhodným chybovým kódem.

Příkaz může, ale nemusí být přístupný v MF. Pokud je přístupný, skončí s vhodným chybovým kódem.

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

TCS_126 Tento příkaz nevypočítá digitální podpis hodnoty hash dříve vypočtené příkazem PSO: HASH.

TCS_127 K výpočtu digitálního podpisu se použije soukromý klíč karty, který je kartě implicitně znám.

TCS_128 Aplikace tachografu 1. generace provede digitální podpis s použitím metody doplnění, která je v souladu s PKCS1 (podrobnosti viz dodatek 11).

TCS_129 Aplikace tachografu 2. generace vypočítá digitální podpis na bázi eliptických křivek (podrobnosti viz dodatek 11).

TCS_130 **Zpráva s příkazem**

Bajt	Délka	Hodnota	Popis
CLA	1	'00h'	CLA
INS	1	'2Ah'	Perform Security Operation
P1	1	'9Eh'	Má být vrácen digitální podpis
P2	1	'9Ah'	Tag: datové pole obsahuje data k podpisu. Jelikož žádné datové pole není zahrnuto, očekává se, že data jsou již na kartě (hash souboru).
Le	1	'NNh'	Délka očekávaného podpisu

TCS_131 **Zpráva s odpovědí**

Bajt	Délka	Hodnota	Popis
#1-#L	L	'XX..XXh'	Podpis dříve vypočítané hodnoty hash
SW	2	'XXXXh'	Stavová slova (SW1, SW2)

— Je-li příkaz úspěšný, karta vrátí '**9000**'.

— Jestliže se implicitně vybraný soukromý klíč považuje za poškozený, je vrácen stav zpracování '**6400**' nebo '**6581**'.

— Není-li k dispozici hodnota hash vypočítaná předchozím příkazem PERFORM HASH OF FILE, je vrácen stav zpracování '**6985**'.

3.5.15 *PSO: VERIFY DIGITAL SIGNATURE*

Tento příkaz se používá k ověření digitálního podpisu poskytnutého jako vstup, jehož hodnota hash je kartě známa. Algoritmus podpisu je kartě implicitně znám.

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

Tento příkaz musí podporovat pouze kontrolní karta v DF Tachograph a DF Tachograph_G2.

Ostatní typy karet tachografu mohou, ale nemusí tento příkaz implementovat. Příkaz může, ale nemusí být přístupný v MF.

TCS_132 Příkaz VERIFY DIGITAL SIGNATURE vždy používá veřejný klíč vybraný předchozím příkazem MANAGE SECURITY ENVIRONMENT MSE: Set DST a předchozí hodnotu hash vloženou příkazem PSO: HASH.

TCS_133 **Zpráva s příkazem**

Bajt	Délka	Hodnota	Popis
CLA	1	'00h'	CLA
INS	1	'2Ah'	Perform Security Operation
P1	1	'00h'	
P2	1	'A8h'	Tag: datové pole obsahuje datové objekty relevantní pro ověření
Lc	1	'83h'	Délka Lc následujícího datového pole
6	1	'9Eh'	Tag pro digitální podpis
#7-#8	2	'81 XXh'	Délka digitálního podpisu: 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)
#9-#(8+L)	L	'XX..XXh'	Obsah digitálního podpisu

TCS_134 **Zpráva s odpovědí**

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

— Je-li příkaz úspěšný, karta vrátí '**9000**'.

— Jestliže se ověření podpisu nezdaří, je vrácen stav zpracování '**6688**'. Postup ověření je popsán v dodatku 11.

— Jestliže není vybrán žádný veřejný klíč, je vrácen stav zpracování '**6A88**'.

— Chybějí-li některé očekávané datové objekty (jak je specifikováno výše), je vrácen stav zpracování '**6987**'. To může nastat, když chybí jeden z požadovaných tagů.

— Jestliže není k dispozici žádná hodnota hash pro zpracování příkazu (jako výsledek předchozího příkazu PSO: HASH), je vrácen stav zpracování '**6985**'.

— Jsou-li některé datové objekty chybné, je vrácen stav zpracování '**6988**'. To může nastat, když je chybná délka jednoho z požadovaných datových objektů.

— Je-li vybraný veřejný klíč považován za poškozený, je vrácen stav zpracování '**6400**' nebo '**6581**'.

3.5.16 *PROCESS DSRC MESSAGE*

Tento příkaz se používá k ověření integrity a pravosti zprávy DSRC a pro dešifrování dat předaných z celku ve vozidle kontrolnímu orgánu nebo dílně pomocí spojení DSRC. Karta odvodí šifrovací klíč a klíč MAC používané pro zabezpečení zprávy DSRC podle dodatku 11 části B kapitoly 13.

Tento příkaz musí podporovat pouze kontrolní karta a karta dílny v DF Tachograph_G2.

Ostatní typy karet tachografu mohou, ale nemusí tento příkaz implementovat, ale nemají hlavní klíč DSRC. Proto tyto karty nemohou příkaz úspěšně provést, ale ukončí jej s vhodným chybovým kódem.

Příkaz může, ale nemusí být přístupný v MF a/nebo DF Tachograph. Pokud je přístupný, skončí s vhodným chybovým kódem.

TCS_135 Hlavní klíč DSRC je přístupný pouze v DF Tachograph_G2, tj. kontrolní karta a karta dílny podporují úspěšné provedení příkazu pouze v DF Tachograph_G2.

TCS_136 Příkaz pouze dešifruje data DSRC a ověřuje kryptografický kontrolní součet, ale neinterpretuje vstupní data.

TCS_137 Pořadí datových objektů v datovém poli příkazu je určeno touto specifikací.

TCS_138 **Zpráva s příkazem**

Bajt	Délka	Hodnota	Popis
CLA	1	'80h'	Proprietární CLA
INS	1	'2Ah'	Perform Security Operation
P1	1	'80h'	Data odpovědi: otevřená hodnota
P2	1	'B0h'	Data příkazu: otevřená hodnota v kódování BER-TLV a včetně datových objektů bezpečného předávání zpráv
Lc	1	'NNh'	Délka Lc následujícího datového pole
#6-#(5+L)	L	'87h' + L_{87} + 'XX..XXh'	Bajt indikující obsah doplnění v kódování DER-TLV následovaný šifrovanými přenášenými daty tachografu. Pro bajt indikující obsah doplnění se používá hodnota '00h' („žádná další indikace" podle ISO/IEC 7816-4:2013 tabulky 52). Mechanismus šifrování viz dodatek 11 část B kapitolu 13. Povolené hodnoty délky L_{87} jsou násobky délky bloku AES plus 1 pro bajt indikující obsah doplnění, tj. od 17 bajtů do 193 bajtů včetně. *Poznámka:* Datový objekt bezpečného předávání zpráv s tagem '87h' viz ISO/IEC 7816-4:2013 tabulka 49.
		'81h' + '10h'	Šablona řídicích odkazů pro důvěrnost v kódování DER-TLV, která obsahuje zřetězení následujících datových prvků (viz dodatek 1 DSRCSecurityData a dodatek 11 část B kapitolu 13): — 4 bajty – časové razítko — 3 bajty – čítač — 8 bajtů – výrobní číslo celku ve vozidle — 1 bajt – verze hlavního klíče DSRC *Poznámka:* Datový objekt bezpečného předávání zpráv s tagem '81h' viz ISO/IEC 7816-4:2013 tabulka 49.
		'8Eh' + L_{8E} + 'XX..XXh'	MAC zprávy DSRC v kódování DER-TLV. Algoritmus a výpočet MAC viz dodatek 11 část B kapitolu 13. *Poznámka:* Datový objekt bezpečného předávání zpráv s tagem '8Eh' viz ISO/IEC 7816-4:2013 tabulka 49.

TCS_139 **Zpráva s odpovědí**

Bajt	Délka	Hodnota	Popis
#1-#L	L	'XX..XXh'	Chybí (v případě chyby) nebo dešifrovaná data (doplnění odstraněno)
SW	2	'XXXXh'	Stavová slova (SW1, SW2)

— Je-li příkaz úspěšný, karta vrátí '**9000**'.

— '**6A80**' označuje nesprávné parametry v datovém poli příkazu (používá se rovněž v případě, že datové objekty nejsou odeslány ve stanoveném pořadí).

— '**6A88**' označuje, že data, na která se odkazuje, tj. hlavní klíč DSRC, nejsou k dispozici.

— '**6900**' označuje, že se nezdařilo ověření kryptografického kontrolního součtu nebo dešifrování dat.

4. STRUKTURA KARET TACHOGRAFU

V tomto odstavci jsou specifikovány struktury souborů, které slouží pro uložení přístupných dat na kartách tachografu.

Nejsou specifikovány vnitřní struktury závislé na výrobci karty, jako například hlavičky souborů, ani ukládání a zpracování datových prvků potřebných pouze pro interní použití, například `EuropeanPublicKey`, `CardPrivateKey`, `TdesSessionKey` nebo `WorkshopCardPin`.

TCS_140 Na kartě tachografu 2. generace je uložen hlavní soubor (MF) a aplikace tachografu stejného typu (např. aplikace karty řidiče) 1. generace a 2. generace.

TCS_141 Karta tachografu musí podporovat alespoň minimální počet záznamů specifikovaný pro příslušné aplikace a nesmí podporovat více záznamů než maximální počet specifikovaný pro příslušné aplikace.

Maximální a minimální počty záznamů jsou pro různé aplikace specifikovány v této kapitole.

Bezpečnostní podmínky používané v pravidlech přístupu v této kapitole jsou uvedeny v kapitole 3.3. Režim přístupu „čtení" obecně označuje příkaz READ BINARY se sudým a – je-li podporován – lichým bajtem INS, s výjimkou EF Sensor_Installation_Data na kartě dílny, viz TCS_156 a TCS_160. Režim přístupu „aktualizace" označuje příkaz UPDATE BINARY se sudým a – je-li podporován – lichým bajtem INS a režim přístupu „výběr" označuje příkaz SELECT.

4.1 Hlavní soubor MF

TCS_142 Po personalizaci má hlavní soubor MF následující trvalou strukturu souborů a pravidla přístupu k souborům:

Poznámka: Krátký identifikátor EF SFID je uváděn jako číslo v desítkové soustavě, tj. hodnota 30 odpovídá binární hodnotě 11110.

			Pravidla přístupu	
Soubor	**ID souboru**	**SFID**	**Čtení / výběr**	**Aktualizace**
MF	'3F00h'			
├─ EF ICC	'0002h'		ALW	NEV
├─ EF IC	'0005h'		ALW	NEV
├─ EF DIR	'2F00h'	30	ALW	NEV
├─ EF ATR/INFO (conditional)	'2F01h'	29	ALW	NEV
├─ EF Extended_Length (conditional)	'0006h'	28	ALW	NEV
├─ DF Tachograph	'0500h'		SC1	
└─ DF Tachograph_G2			SC1	

V této tabulce je použita tato zkratka pro bezpečnostní podmínku:

SC1 ALW OR SM-MAC-G2

TCS_143 Všechny struktury EF jsou transparentní.

TCS_144 Hlavní soubor MF má tuto strukturu dat:

Soubor / datový prvek	Počet záznamů	Velikost (bajty) Min	Max	Výchozí hodnoty
MF		*63*	*184*	
EF ICC		*25*	*25*	
CardIccIdentification		*25*	*25*	
clockStop		1	1	{00}
cardExtendedSerialNumber		8	8	{00..00}
cardApprovalNumber		8	8	{20..20}
cardPersonaliserID		1	1	{00}
embedderIcAssemblerId		5	5	{00..00}
icIdentifier		2	2	{00 00}
EF IC		*8*	*8*	
CardChipIdentification		*8*	*8*	
icSerialNumber		4	4	{00..00}
icManufacturingReferences		4	4	{00..00}
EF DIR		*20*	*20*	
See TCS_145		*20*	*20*	{00..00}
EF ATR/INFO		*7*	*128*	
See TCS_146		*7*	*128*	{00..00}
EF EXTENDED_LENGTH		*3*	*3*	
See TCS_147		*3*	*3*	{00..00}
DF Tachograph				
DF Tachograph_G2				

TCS_145 Elementární soubor EF DIR obsahuje tyto datové objekty týkající se aplikace: '61 08 4F 06 FF 54 41 43 48 4F 61 08 4F 06 FF 53 4D 52 44 54'

TCS_146 Elementární soubor EF ATR/INFO je přítomen, pokud karta tachografu v ATR uvádí, že podporuje rozšířená pole délky. V tomto případě EF ATR/INFO obsahuje datový objekt s informací o rozšířené délce (DO'7F66'), jak je uvedeno v ISO/IEC 7816-4:2013 bodě 12.7.1.

TCS_147 Elementární soubor EF Extended_Length je přítomen, pokud karta tachografu v ATR uvádí, že podporuje rozšířená pole délky. V tomto případě tento EF obsahuje tento datový objekt: '02 01 xx', kde hodnota 'xx' označuje, zda jsou rozšířená pole délky podporována pro protokol T = 1 a/nebo T = 0.

Hodnota '01' označuje, že rozšířená pole délky jsou podporována pro protokol T = 1.

Hodnota '10' označuje, že rozšířená pole délky jsou podporována pro protokol T = 0.

Hodnota '11' označuje, že rozšířená pole délky jsou podporována pro protokol T = 1 a T = 0.

4.2 Aplikace karty řidiče

4.2.1 *Aplikace karty řidiče 1. generace*

TCS_148 Po personalizaci má aplikace karty řidiče 1. generace následující trvalou strukturu souborů a pravidla přístupu k souborům:

Soubor	ID souboru	Pravidla přístupu		
		Čtení	Výběr	Aktualizace
└─DF Tachograph	'0500h'		SC1	
├─EF Application_Identification	'0501h'	SC2	SC1	NEV
├─EF Card_Certificate	'C100h'	SC2	SC1	NEV
├─EF CA_Certificate	'C108h'	SC2	SC1	NEV
├─EF Identification	'0520h'	SC2	SC1	NEV
├─EF Card_Download	'050Eh'	SC2	SC1	SC1
├─EF Driving_Licence_Info	'0521h'	SC2	SC1	NEV
├─EF Events_Data	'0502h'	SC2	SC1	SC3
├─EF Faults_Data	'0503h'	SC2	SC1	SC3
├─EF Driver_Activity_Data	'0504h'	SC2	SC1	SC3
├─EF Vehicles_Used	'0505h'	SC2	SC1	SC3
├─EF Places	'0506h'	SC2	SC1	SC3
├─EF Current_Usage	'0507h'	SC2	SC1	SC3
├─EF Control_Activity_Data	'0508h'	SC2	SC1	SC3
└─EF Specific_Conditions	'0522h'	SC2	SC1	SC3

V této tabulce jsou použity tyto zkratky pro bezpečnostní podmínky:

SC1 ALW OR SM-MAC-G2

SC2 ALW OR SM-MAC-G1 OR SM-MAC-G2

SC3 SM-MAC-G1 OR SM-MAC-G2

TCS_149 Všechny struktury EF jsou transparentní.

TCS_150 Aplikace karty řidiče 1. generace musí mít tuto strukturu dat:

Soubor / datový prvek	Počet záznamů	Velikost (bajty) Min	Max	Výchozí hodnoty
DF Tachograph		*11378*	*24926*	
EF Application_Identification		*10*	*10*	
DriverCardApplicationIdentification		*10*	*10*	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfEventsPerType		1	1	{00}
noOfFaultsPerType		1	1	{00}
activityStructureLength		2	2	{00 00}
noOfCardVehicleRecords		2	2	{00 00}
noOfCardPlaceRecords		1	1	{00}
EF Card_Certificate		*194*	*194*	
CardCertificate		194	194	{00..00}
EF CA_Certificate		*194*	*194*	
MemberStateCertificate		194	194	{00..00}
EF Identification		*143*	*143*	
CardIdentification		*65*	*65*	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
DriverCardHolderIdentification		*78*	*78*	
cardHolderName		*72*	*72*	
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00, 20..20}
cardHolderBirthDate		4	4	{00..00}
cardHolderPreferredLanguage		2	2	{20 20}
EF Card_Download		*4*	*4*	
LastCardDownload		4	4	
EF Driving_Licence_Info		*53*	*53*	
CardDrivingLicenceInformation		*53*	*53*	
drivingLicenceIssuingAuthority		36	36	{00, 20..20}
drivingLicenceIssuingNation		1	1	{00}
drivingLicenceNumber		16	16	{20..20}
EF Events_Data		*864*	*1728*	
CardEventData		*864*	*1728*	
cardEventRecords	6	*144*	*288*	
CardEventRecord	n_1	*24*	*24*	
eventType		1	1	{00}
eventBeginTime		4	4	{00..00}
eventEndTime		4	4	{00..00}
eventVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Faults_Data		*576*	*1152*	
CardFaultData		*576*	*1152*	
cardFaultRecords	2	*288*	*576*	
CardFaultRecord	n_2	*24*	*24*	
faultType		1	1	{00}
faultBeginTime		4	4	{00..00}
faultEndTime		4	4	{00..00}
faultVehicleRegistration				

├─vehicleRegistrationNation		1	1	{00}
└─vehicleRegistrationNumber		14	14	{00, 20..20}
EF Driver_Activity_Data		*5548*	*13780*	
└CardDriverActivity		*5548*	*13780*	
├─activityPointerOldestDayRecord		2	2	{00 00}
├─activityPointerNewestRecord		2	2	{00 00}
└─activityDailyRecords	n_6	5544	13776	{00..00}
EF Vehicles_Used		*2606*	*6202*	
└CardVehiclesUsed		*2606*	*6202*	
├─vehiclePointerNewestRecord		2	2	{00 00}
└─cardVehicleRecords		*2604*	*6200*	
└─CardVehicleRecord	n_3	*31*	*31*	
├─vehicleOdometerBegin		3	3	{00..00}
├─vehicleOdometerEnd		3	3	{00..00}
├─vehicleFirstUse		4	4	{00..00}
├─vehicleLastUse		4	4	{00..00}
├─vehicleRegistration				
├─vehicleRegistrationNation		1	1	{00}
└─vehicleRegistrationNumber		14	14	{00, 20..20}
└─vuDataBlockCounter		2	2	{00 00}
EF Places		*841*	*1121*	
└CardPlaceDailyWorkPeriod		*841*	*1121*	
├─placePointerNewestRecord		1	1	{00}
└─placeRecords		*840*	*1120*	
└─PlaceRecord	n_4	*10*	*10*	
├─entryTime		4	4	{00..00}
├─entryTypeDailyWorkPeriod		1	1	{00}
├─dailyWorkPeriodCountry		1	1	{00}
├─dailyWorkPeriodRegion		1	1	{00}
└─vehicleOdometerValue		3	3	{00..00}
EF Current_Usage		*19*	*19*	
└CardCurrentUse		*19*	*19*	
├─sessionOpenTime		4	4	{00..00}
└─sessionOpenVehicle				
├─vehicleRegistrationNation		1	1	{00}
└─vehicleRegistrationNumber		14	14	{00, 20..20}
EF Control_Activity_Data		*46*	*46*	
└CardControlActivityDataRecord		*46*	*46*	
├─controlType		1	1	{00}
├─controlTime		4	4	{00..00}
├─controlCardNumber				
├─cardType		1	1	{00}
├─cardIssuingMemberState		1	1	{00}
└─cardNumber		16	16	{20..20}
├─controlVehicleRegistration				
├─vehicleRegistrationNation		1	1	{00}
└─vehicleRegistrationNumber		14	14	{00, 20..20}
├─controlDownloadPeriodBegin		4	4	{00..00}
└─controlDownloadPeriodEnd		4	4	{00..00}
EF Specific_Conditions		*280*	*280*	
└SpecificConditionRecord	56	*5*	*5*	
├─entryTime		4	4	{00..00}
└─SpecificConditionType		1	1	{00}

TCS_151 Následující hodnoty používané pro označení velikostí ve výše uvedené tabulce jsou hodnoty minimálního a maximálního počtu záznamů, které musí struktura dat karty řidiče používat pro aplikaci 1. generace:

		Min	**Max**
n_1	NoOfEventsPerType	6	12
n_2	NoOfFaultsPerType	12	24
n_3	NoOfCardVehicleRecords	84	200
n_4	NoOfCardPlaceRecords	84	112
n_6	CardActivityLengthRange	5 544 bajtů (28 dnů * 93 změn činnosti)	13 776 bajtů (28 dnů * 240 změn činnosti)

4.2.2 *Aplikace karty řidiče 2. generace*

TCS_152 Po personalizaci má aplikace karty řidiče 2. generace následující trvalou strukturu souborů a pravidla přístupu k souborům:

Poznámka: Krátký identifikátor EF SFID je uváděn jako číslo v desítkové soustavě, tj. hodnota 30 odpovídá binární hodnotě 11110.

			Pravidla přístupu	
Soubor	**ID souboru**	**SFID**	**Čtení / výběr**	**Aktualizace**
└─DF Tachograph_G2			SC1	
├─EF Application_Identification	'0501h'	1	SC1	NEV
├─EF CardMA_Certificate	'C100h'	2	SC1	NEV
├─EF CardSignCertificate	'C101h'	3	SC1	NEV
├─EF CA_Certificate	'C108h'	4	SC1	NEV
├─EF Link_Certificate	'C109h'	5	SC1	NEV
├─EF Identification	'0520h'	6	SC1	NEV
├─EF Card_Download	'050Eh'	7	SC1	SC1
├─EF Driving_Licence_Info	'0521h'	10	SC1	NEV
├─EF Events_Data	'0502h'	12	SC1	SM-MAC-G2
├─EF Faults_Data	'0503h'	13	SC1	SM-MAC-G2
├─EF Driver_Activity_Data	'0504h'	14	SC1	SM-MAC-G2
├─EF Vehicles_Used	'0505h'	15	SC1	SM-MAC-G2
├─EF Places	'0506h'	16	SC1	SM-MAC-G2
├─EF Current_Usage	'0507h'	17	SC1	SM-MAC-G2
├─EF Control_Activity_Data	'0508h'	18	SC1	SM-MAC-G2
├─EF Specific_Conditions	'0522h'	19	SC1	SM-MAC-G2
├─EF VehicleUnits_Used	'0523h'	20	SC1	SM-MAC-G2
└─EF GNSS_Places	'0524h'	21	SC1	SM-MAC-G2

V této tabulce je použita tato zkratka pro bezpečnostní podmínku:

SC1 ALW OR SM-MAC-G2

TCS_153 Všechny struktury EF jsou transparentní.

TCS_154 Aplikace karty řidiče 2. generace musí mít tuto strukturu dat:

Soubor / datový prvek	Počet záznamů	Velikost (bajty) Min	Velikost (bajty) Max	Výchozí hodnoty
DF Tachograph_G2		*19510*	*39306*	
EF Application_Identification		*15*	*15*	
DriverCardApplicationIdentification		*15*	*15*	
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}
noOfGNSSCDRecords		2	2	{00 00}
noOfSpecificConditionRecords		2	2	{00}
EF CardMA_Certificate		*204*	*341*	
CardMACertificate		204	341	{00..00}
EF CardSignCertificate		*204*	*341*	
CardSignCertificate		204	341	{00..00}
EF CA_Certificate		*204*	*341*	
MemberStateCertificate		204	341	{00..00}
EF Link_Certificate		*204*	*341*	
LinkCertificate		204	341	{00..00}
EF Identification		*143*	*143*	
CardIdentification		*65*	*65*	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
DriverCardHolderIdentification		*78*	*78*	
cardHolderName		*72*	*72*	
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00, 20..20}
cardHolderBirthDate		4	4	{00..00}
cardHolderPreferredLanguage		2	2	{20 20}
EF Card_Download		*4*	*4*	
LastCardDownload		4	4	
EF Driving_Licence_Info		*53*	*53*	
CardDrivingLicenceInformation		*53*	*53*	
drivingLicenceIssuingAuthority		36	36	{00, 20..20}
drivingLicenceIssuingNation		1	1	{00}
drivingLicenceNumber		16	16	{20..20}
EF Events_Data		*1584*	*3168*	
CardEventData		*1584*	*3168*	
cardEventRecords	11	*144*	*288*	
CardEventRecord	n_1	*24*	*24*	
eventType		1	1	{00}
eventBeginTime		4	4	{00..00}
eventEndTime		4	4	{00..00}
eventVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Faults_Data		*576*	*1152*	
CardFaultData		*576*	*1152*	
cardFaultRecords	2	*288*	*576*	
CardFaultRecord	n_2	*24*	*24*	

faultType		1	1	{00}
faultBeginTime		4	4	{00..00}
faultEndTime		4	4	{00..00}
faultVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Driver_Activity_Data		*5548*	*13780*	
CardDriverActivity		*5548*	*13780*	
activityPointerOldestDayRecord		2	2	{00 00}
activityPointerNewestRecord		2	2	{00 00}
activityDailyRecords	n_6	5544	13776	{00..00}
EF Vehicles_Used		*4034*	*9602*	
CardVehiclesUsed		*4034*	*9602*	
vehiclePointerNewestRecord		2	2	{00 00}
cardVehicleRecords		*4032*	*9600*	
CardVehicleRecord	n_3	*48*	*48*	
vehicleOdometerBegin		3	3	{00..00}
vehicleOdometerEnd		3	3	{00..00}
vehicleFirstUse		4	4	{00..00}
vehicleLastUse		4	4	{00..00}
vehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
vuDataBlockCounter		2	2	{00 00}
vehicleIdentificationNumber		17	17	{20..20}
EF Places		*1766*	*2354*	
CardPlaceDailyWorkPeriod		*1766*	*2354*	
placePointerNewestRecord		2	2	{00 00}
placeRecords		*1764*	*2352*	
PlaceRecord	n_4	*21*	*21*	
entryTime		4	4	{00..00}
entryTypeDailyWorkPeriod		1	1	{00}
dailyWorkPeriodCountry		1	1	{00}
dailyWorkPeriodRegion		1	1	{00}
vehicleOdometerValue		3	3	{00..00}
entryGNSSPlaceRecord		11	11	
timeStamp		4	4	{00..00}
gnssAccuracy		1	1	{00}
geoCoordinates		6	6	{00..00}
EF Current_Usage		*19*	*19*	
CardCurrentUse		*19*	*19*	
sessionOpenTime		4	4	{00..00}
sessionOpenVehicle				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Control_Activity_Data		*46*	*46*	
CardControlActivityDataRecord		*46*	*46*	
controlType		1	1	{00}
controlTime		4	4	{00..00}
controlCardNumber				
cardType		1	1	{00}
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
controlVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
controlDownloadPeriodBegin		4	4	{00..00}
controlDownloadPeriodEnd		4	4	{00..00}

EF Specific_Conditions		*282*	*562*	
SpecificConditions		*282*	*562*	
conditionPointerNewestRecord		2	2	{00 00}
specificConditionRecords		*280*	*560*	
SpecificConditionRecord	n_9	*5*	*5*	
entryTime		4	4	{00..00}
specificConditionType		1	1	{00}
EF VehicleUnits_Used		*842*	*2002*	
CardVehicleUnitsUsed		*842*	*2002*	
vehicleUnitPointerNewestRecord		2	2	{00 00}
cardVehicleUnitRecords		*840*	*2000*	
CardVehicleUnitRecord	n_7	*10*	*10*	
timeStamp		4	4	{00..00}
manufacturerCode		1	1	{00}
deviceID		1	1	{00}
vuSoftwareVersion		4	4	{00..00}
EF GNSS_Places		*3782*	*5042*	
GNSSContinuousDriving		*3782*	*5042*	
gnssCDPointerNewestRecord		2	2	{00 00}
gnssContinuousDrivingRecords		3780	5040	{00}
GNSSContinuousDrivingRecord	n_8	*15*	*15*	
timeStamp		4	4	{00..00}
gnssPlaceRecord		11	11	
timeStamp		4	4	{00..00}
gnssAccuracy		1	1	{00}
geoCoordinates		6	6	{00..00}

TCS_155 Následující hodnoty používané pro označení velikostí ve výše uvedené tabulce jsou hodnoty minimálního a maximálního počtu záznamů, které musí struktura dat karty řidiče používat pro aplikaci 2. generace:

		Min	**Max**
n_1	NoOfEventsPerType	6	12
n_2	NoOfFaultsPerType	12	24
n_3	NoOfCardVehicleRecords	84	200
n_4	NoOfCardPlaceRecords	84	112
n_6	CardActivityLengthRange	5 544 bajtů (28 dnů * 93 změn činnosti)	13 776 bajtů (28 dnů * 240 změn činnosti)
n_7	NoOfCardVehicleUnitRecords	84	200
n_8	NoOfGNSSCDRecords	252	336
n_9	NoOfSpecificConditionRecords	56	112

4.3 Aplikace karty dílny

4.3.1 *Aplikace karty dílny 1. generace*

TCS_156 Po personalizaci musí mít aplikace karty dílny 1. generace následující trvalou strukturu souborů a pravidla přístupu k souborům:

		Pravidla přístupu		
Soubor	**ID souboru**	**Čtení**	**Výběr**	**Aktualizace**
└─DF Tachograph	'0500h'		SC1	
├─EF Application_Identification	'0501h'	SC2	SC1	NEV
├─EF Card_Certificate	'C100h'	SC2	SC1	NEV
├─EF CA_Certificate	'C108h'	SC2	SC1	NEV
├─EF Identification	'0520h'	SC2	SC1	NEV
├─EF Card_Download	'0509h'	SC2	SC1	**SC1**
├─EF Calibration	'050Ah'	SC2	SC1	SC3
├─EF Sensor_Installation_Data	'050Bh'	**SC4**	SC1	NEV
├─EF Events_Data	'0502h'	SC2	SC1	SC3
├─EF Faults_Data	'0503h'	SC2	SC1	SC3
├─EF Driver_Activity_Data	'0504h'	SC2	SC1	SC3
├─EF Vehicles_Used	'0505h'	SC2	SC1	SC3
├─EF Places	'0506h'	SC2	SC1	SC3
├─EF Current_Usage	'0507h'	SC2	SC1	SC3
├─EF Control_Activity_Data	'0508h'	SC2	SC1	SC3
└─EF Specific_Conditions	'0522h'	SC2	SC1	SC3

V této tabulce jsou použity tyto zkratky pro bezpečnostní podmínky:

SC1 ALW OR SM-MAC-G2

SC2 ALW OR SM-MAC-G1 OR SM-MAC-G2

SC3 SM-MAC-G1 OR SM-MAC-G2

SC4 Pro příkaz READ BINARY se sudým bajtem INS:

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

TCS_157 Všechny struktury EF jsou transparentní.

TCS_158 Aplikace karty dílny 1. generace musí mít tuto strukturu dat:

Soubor / datový prvek	Počet záznamů	Velikost (bajty) Min	Max	Výchozí hodnoty
DF Tachograph		*11055*	*29028*	
EF Application_Identification		*11*	*11*	
WorkshopCardApplicationIdentification		*11*	*11*	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfEventsPerType		1	1	{00}
noOfFaultsPerType		1	1	{00}
activityStructureLength		2	2	{00 00}
noOfCardVehicleRecords		2	2	{00 00}
noOfCardPlaceRecords		1	1	{00}
noOfCalibrationRecords		1	1	{00}
EF Card_Certificate		*194*	*194*	
CardCertificate		194	194	{00..00}
EF CA_Certificate		*194*	*194*	
MemberStateCertificate		194	194	{00..00}
EF Identification		*211*	*211*	
CardIdentification		65	65	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{00, 20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
WorkshopCardHolderIdentification		*146*	*146*	
workshopName		36	36	{00, 20..20}
workshopAddress		36	36	{00, 20..20}
cardHolderName				
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00, 20..20}
cardHolderPreferredLanguage		2	2	{20 20}
EF Card_Download		*2*	*2*	
NoOfCalibrationsSinceDownload		2	2	{00 00}
EF Calibration		*9243*	*26778*	
WorkshopCardCalibrationData		*9243*	*26778*	
calibrationTotalNumber		2	2	{00 00}
calibrationPointerNewestRecord		1	1	{00}
calibrationRecords		*9240*	*26775*	
WorkshopCardCalibrationRecord	n_5	*105*	*105*	
calibrationPurpose		1	1	{00}
vehicleIdentificationNumber		17	17	{20..20}
vehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
wVehicleCharacteristicConstant		2	2	{00 00}
kConstantOfRecordingEquipment		2	2	{00 00}
lTyreCircumference		2	2	{00 00}
tyreSize		15	15	{20..20}
authorisedSpeed		1	1	{00}
oldOdometerValue		3	3	{00..00}
newOdometerValue		3	3	{00..00}
oldTimeValue		4	4	{00..00}
newTimeValue		4	4	{00..00}
nextCalibrationDate		4	4	{00..00}
vuPartNumber		16	16	{20..20}
vuSerialNumber		8	8	{00..00}
sensorSerialNumber		8	8	{00..00}

EF Sensor_Installation_Data		*16*	*16*	
SensorInstallationSecData		16	16	{00..00}
EF Events_Data		*432*	*432*	
CardEventData		*432*	*432*	
cardEventRecords	6	*72*	*72*	
CardEventRecord	n_1	*24*	*24*	
eventType		1	1	{00}
eventBeginTime		4	4	{00..00}
eventEndTime		4	4	{00..00}
eventVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Faults_Data		*288*	*288*	
CardFaultData		*288*	*288*	
cardFaultRecords	2	*144*	*144*	
CardFaultRecord	n_2	*24*	*24*	
faultType		1	1	{00}
faultBeginTime		4	4	{00..00}
faultEndTime		4	4	{00..00}
faultVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Driver_Activity_Data		*202*	*496*	
CardDriverActivity		*202*	*496*	
activityPointerOldestDayRecord		2	2	{00 00}
activityPointerNewestRecord		2	2	{00 00}
activityDailyRecords	n_6	198	492	{00..00}
EF Vehicles_Used		*126*	*250*	
CardVehiclesUsed		*126*	*250*	
vehiclePointerNewestRecord		2	2	{00 00}
cardVehicleRecords		*124*	*248*	
CardVehicleRecord	n_3	*31*	*31*	
vehicleOdometerBegin		3	3	{00..00}
vehicleOdometerEnd		3	3	{00..00}
vehicleFirstUse		4	4	{00..00}
vehicleLastUse		4	4	{00..00}
vehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
vuDataBlockCounter		2	2	{00 00}
EF Places		*61*	*81*	
CardPlaceDailyWorkPeriod		*61*	*81*	
placePointerNewestRecord		1	1	{00}
placeRecords		*60*	*80*	
PlaceRecord	n_4	*10*	*10*	
entryTime		4	4	{00..00}
entryTypeDailyWorkPeriod		1	1	{00}
dailyWorkPeriodCountry		1	1	{00}
dailyWorkPeriodRegion		1	1	{00}
vehicleOdometerValue		3	3	{00..00}
EF Current_Usage		*19*	*19*	
CardCurrentUse		*19*	*19*	
sessionOpenTime		4	4	{00..00}
sessionOpenVehicle				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}

EF Control_Activity_Data		*46*	*46*	
CardControlActivityDataRecord		*46*	*46*	
controlType		1	1	{00}
controlTime		4	4	{00..00}
controlCardNumber				
cardType		1	1	{00}
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
controlVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
controlDownloadPeriodBegin		4	4	{00..00}
controlDownloadPeriodEnd		4	4	{00..00}
EF Specific_Conditions		*10*	*10*	
SpecificConditionRecord	2	*5*	*5*	
entryTime		4	4	{00..00}
SpecificConditionType		1	1	{00}

TCS_159 Následující hodnoty používané pro označení velikostí ve výše uvedené tabulce jsou hodnoty minimálního a maximálního počtu záznamů, které musí struktura dat karty dílny používat pro aplikaci 1. generace:

		Min	**Max**
n_1	NoOfEventsPerType	3	3
n_2	NoOfFaultsPerType	6	6
n_3	NoOfCardVehicleRecords	4	8
n_4	NoOfCardPlaceRecords	6	8
n_5	NoOfCalibrationRecords	88	255
n_6	CardActivityLengthRange	198 bajtů (1 den * 93 změn činnosti)	492 bajtů (1 den * 240 změn činnosti)

4.3.2 *Aplikace karty dílny 2. generace*

TCS_160 Po personalizaci musí mít aplikace karty dílny 2. generace následující trvalou strukturu souborů a pravidla přístupu k souborům:

Poznámka: Krátký identifikátor EF SFID je uváděn jako číslo v desítkové soustavě, tj. hodnota 30 odpovídá binární hodnotě 11110.

			Pravidla přístupu		
Soubor	**ID souboru**	**SFID**	**Čtení**	**Výběr**	**Aktualizace**
└─DF Tachograph_G2			SC1	SC1	
├─EF Application_Identification	'0501h'	1	SC1	SC1	NEV
├─EF CardMA_Certificate	'C100h'	2	SC1	SC1	NEV
├─EF CardSignCertificate	'C101h'	3	SC1	SC1	NEV
├─EF CA_Certificate	'C108h'	4	SC1	SC1	NEV
├─EF Link_Certificate	'C109h'	5	SC1	SC1	NEV
├─EF Identification	'0520h'	6	SC1	SC1	NEV
├─EF Card_Download	'0509h'	7	SC1	SC1	SC1
├─EF Calibration	'050Ah'	10	SC1	SC1	SM-MAC-G2
├─EF Sensor_Installation_Data	'050Bh'	11	**SC5**	SM-MAC-G2	NEV
├─EF Events_Data	'0502h'	12	SC1	SC1	SM-MAC-G2
├─EF Faults_Data	'0503h'	13	SC1	SC1	SM-MAC-G2
├─EF Driver_Activity_Data	'0504h'	14	SC1	SC1	SM-MAC-G2
├─EF Vehicles_Used	'0505h'	15	SC1	SC1	SM-MAC-G2
├─EF Places	'0506h'	16	SC1	SC1	SM-MAC-G2
├─EF Current_Usage	'0507h'	17	SC1	SC1	SM-MAC-G2
├─EF Control_Activity_Data	'0508h'	18	SC1	SC1	SM-MAC-G2
├─EF Specific_Conditions	'0522h'	19	SC1	SC1	SM-MAC-G2
├─EF VehicleUnits_Used	'0523h'	20	SC1	SC1	SM-MAC-G2
└─EF GNSS_Places	'0524h'	21	SC1	SC1	SM-MAC-G2

V této tabulce jsou použity tyto zkratky pro bezpečnostní podmínky:

SC1 ALW OR SM-MAC-G2

SC5 Pro příkaz READ BINARY se sudým bajtem INS: SM-C-MAC-G2 AND SM-R-ENC-MAC-G2

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

TCS_161 Všechny struktury EF jsou transparentní.

TCS_162 Aplikace karty dílny 2. generace musí mít tuto strukturu dat:

Soubor / datový prvek	Počet záznamů	Velikost (bajty) Min	Max	Výchozí hodnoty
DF Tachograph_G2		*17837*	*47163*	
EF Application_Identification		*17*	*17*	
WorkshopCardApplicationIdentification		*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}
noOfCalibrationRecords		2	2	{00}
noOfGNSSCDRecords		2	2	{00..00}
noOfSpecificConditionRecords		2	2	{00..00}
EF CardMA_Certificate		*204*	*341*	
CardMACertificate		204	341	{00..00}
EF CardSignCertificate		*204*	*341*	
CardSignCertificate		204	341	{00..00}
EF CA_Certificate		*204*	*341*	
MemberStateCertificate		204	341	{00..00}
EF Link_Certificate		*204*	*341*	
LinkCertificate		204	341	{00..00}
EF Identification		*211*	*211*	
CardIdentification		*65*	*65*	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{00, 20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
WorkshopCardHolderIdentification		*146*	*146*	
workshopName		36	36	{00, 20..20}
workshopAddress		36	36	{00, 20..20}
cardHolderName				
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00, 20..20}
cardHolderPreferredLanguage		2	2	{20 20}
EF Card_Download		*2*	*2*	
NoOfCalibrationsSinceDownload		2	2	{00 00}
EF Calibration		*14788*	*42844*	
WorkshopCardCalibrationData		*14788*	*42844*	
calibrationTotalNumber		2	2	{00 00}
calibrationPointerNewestRecord		2	2	{00}
calibrationRecords		*14784*	*42840*	
WorkshopCardCalibrationRecord	n_5	*168*	*168*	
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		46	46	
noOfSealRecords		1	1	{00}
SealRecords		45	45	
SealRecord	5	9	9	
equipmentType		1	1	{00}
extendedSealIdentifier		8	8	{00..00}
EF Sensor_Installation_Data		*18*	*102*	
SensorInstallationSecData		18	102	{00..00}
EF Events_Data		*792*	*792*	
CardEventData		*792*	*792*	
cardEventRecords	11	*72*	*72*	
CardEventRecord	n_1	*24*	*24*	
eventType		1	1	{00}
eventBeginTime		4	4	{00..00}
eventEndTime		4	4	{00..00}
eventVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Faults_Data		*288*	*288*	
CardFaultData		*288*	*288*	
cardFaultRecords	2	*144*	*144*	
CardFaultRecord	n_2	*24*	*24*	
faultType		1	1	{00}
faultBeginTime		4	4	{00..00}
faultEndTime		4	4	{00..00}
faultVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Driver_Activity_Data		*202*	*496*	
CardDriverActivity		*202*	*496*	
activityPointerOldestDayRecord		2	2	{00 00}
activityPointerNewestRecord		2	2	{00 00}
activityDailyRecords	n_6	198	492	{00..00}
EF Vehicles_Used		*194*	*386*	
CardVehiclesUsed		*194*	*386*	
vehiclePointerNewestRecord		2	2	{00 00}
cardVehicleRecords		*192*	*384*	
CardVehicleRecord	n_3	*48*	*48*	
vehicleOdometerBegin		3	3	{00..00}
vehicleOdometerEnd		3	3	{00..00}
vehicleFirstUse		4	4	{00..00}
vehicleLastUse		4	4	{00..00}
vehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
vuDataBlockCounter		2	2	{00 00}
vehicleIdentificationNumber		*17*	17	{20..20}
EF Places		*128*	*170*	

└CardPlaceDailyWorkPeriod		*128*	*170*	
├placePointerNewestRecord		2	2	{00 00}
└placeRecords		*126*	*168*	
└PlaceRecord	n_4	*21*	*21*	
├entryTime		4	4	{00..00}
├entryTypeDailyWorkPeriod		1	1	{00}
├dailyWorkPeriodCountry		1	1	{00}
├dailyWorkPeriodRegion		1	1	{00}
├vehicleOdometerValue		3	3	{00..00}
└entryGNSSPlaceRecord		11	11	{00..00}
├timeStamp		4	4	{00..00}
├gnssAccuracy		1	1	{00}
└geoCoordinates		6	6	{00..00}
EF Current_Usage		*19*	*19*	
└CardCurrentUse		*19*	*19*	
├sessionOpenTime		4	4	{00..00}
└sessionOpenVehicle				
├vehicleRegistrationNation		1	1	{00}
└vehicleRegistrationNumber		14	14	{00, 20..20}
EF Control_Activity_Data		*46*	*46*	
└CardControlActivityDataRecord		*46*	*46*	
├controlType		1	1	{00}
├controlTime		4	4	{00..00}
├controlCardNumber				
├cardType		1	1	{00}
├cardIssuingMemberState		1	1	{00}
└cardNumber		16	16	{20..20}
├controlVehicleRegistration				
├vehicleRegistrationNation		1	1	{00}
└vehicleRegistrationNumber		14	14	{00, 20..20}
├controlDownloadPeriodBegin		4	4	{00..00}
└controlDownloadPeriodEnd		4	4	{00..00}
EF VehicleUnits_Used		*42*	*42*	
└CardVehicleUnitsUsed		*42*	*82*	
├vehicleUnitPointerNewestRecord		2	2	{00 00}
└cardVehicleUnitRecords		*40*	*80*	
└CardVehicleUnitRecord	n_7	*10*	*10*	
├timeStamp		4	4	{00..00}
├manufacturerCode		1	1	{00..00}
├deviceID		1	1	{00..00}
└vuSoftwareVersion		4	4	{00..00}
EF GNSS_Places		*262*	*362*	
└GNSSContinuousDriving		*262*	*362*	
├gnssCDPointerNewestRecord		2	2	{00 00}
└gnssContinuousDrivingRecords		*260*	*360*	
└GNSSContinuousDrivingRecord	n_8	*15*	*15*	
├timeStamp		4	4	{00..00}
└gnssPlaceRecord		11	11	
├timeStamp		4	4	{00..00}
├gnssAccuracy		1	1	{00}
└geoCoordinates		6	6	{00..00}
EF Specific_Conditions		*12*	*22*	
└SpecificConditions		*12*	*22*	
├conditionPointerNewestRecord		2	2	{00 00}
└specificConditionRecords		10	20	
└SpecificConditionRecord	n_9	*5*	*5*	
├entryTime		4	4	{00..00}
└specificConditionType		1	1	{00}

TCS_163 Následující hodnoty používané pro označení velikostí ve výše uvedené tabulce jsou hodnoty minimálního a maximálního počtu záznamů, které musí struktura dat karty dílny používat pro aplikaci 2. generace:

		Min	Max
n_1	NoOfEventsPerType	3	3
n_2	NoOfFaultsPerType	6	6
n_3	NoOfCardVehicleRecords	4	8
n_4	NoOfCardPlaceRecords	6	8
n_5	NoOfCalibrationRecords	88	255
n_6	CardActivityLengthRange	198 bajtů (1 den * 93 změn činnosti)	492 bajtů (1 den * 240 změn činnosti)
n_7	NoOfCardVehicleUnitRecords	4	8
n_8	NoOfGNSSCDRecords	18	24
n_9	NoOfSpecificConditionRecords	2	4

4.4 Aplikace kontrolní karty

4.4.1 *Aplikace kontrolní karty 1. generace*

TCS_164 Po personalizaci musí mít aplikace kontrolní karty 1. generace následující trvalou strukturu souborů a pravidla přístupu k souborům:

		Pravidla přístupu		
Soubor	**ID souboru**	**Čtení**	**Výběr**	**Aktualizace**
└─DF Tachograph	'0500h'			
├─EF Application_Identification	'0501h'	SC2	SC1	NEV
├─EF Card_Certificate	'C100h'	SC2	SC1	NEV
├─EF CA_Certificate	'C108h'	SC2	SC1	NEV
├─EF Identification	'0520h'	**SC6**	SC1	NEV
└─EF Controller_Activity_Data	'050Ch'	SC2	SC1	SC3

V této tabulce jsou použity tyto zkratky pro bezpečnostní podmínky:

SC1 ALW OR SM-MAC-G2

SC2 ALW OR SM-MAC-G1 OR SM-MAC-G2

SC3 SM-MAC-G1 OR SM-MAC-G2

SC6 EXT-AUT-G1 OR SM-MAC-G1 OR SM-MAC-G2

TCS_165 Všechny struktury EF jsou transparentní.

TCS_166 Aplikace kontrolní karty 1. generace musí mít tuto strukturu dat:

Soubor / datový prvek	Počet záznamů	Velikost (bajty) Min	Max	
DF Tachograph		*11186*	*24526*	
EF Application_Identification		*5*	*5*	
ControlCardApplicationIdentification		*5*	*5*	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfControlActivityRecords		2	2	{00 00}
EF Card_Certificate		*194*	*194*	
CardCertificate		194	194	{00..00}
EF CA_Certificate		*194*	*194*	
MemberStateCertificate		194	194	{00..00}
EF Identification		*211*	*211*	
CardIdentification		*65*	*65*	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{00, 20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
ControlCardHolderIdentification		*146*	*146*	
controlBodyName		36	36	{00, 20..20}
controlBodyAddress		36	36	{00, 20..20}
cardHolderName				
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00, 20..20}
cardHolderPreferredLanguage		2	2	{20 20}
EF Controller_Activity_Data		*10582*	*23922*	
ControlCardControlActivityData		*10582*	*23922*	
controlPointerNewestRecord		2	2	{00 00}
controlActivityRecords		*10580*	*23920*	
controlActivityRecord	n_7	*46*	*46*	
controlType		1	1	{00}
controlTime		4	4	{00..00}
controlledCardNumber				
cardType		1	1	{00}
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
controlledVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
controlDownloadPeriodBegin		4	4	{00..00}
controlDownloadPeriodEnd		4	4	{00..00}

TCS_167 Následující hodnoty používané pro označení velikostí ve výše uvedené tabulce jsou hodnoty minimálního a maximálního počtu záznamů, které musí struktura dat kontrolní karty používat pro aplikaci 1. generace:

		Min	Max
n_7	NoOfControlActivityRecords	230	520

4.4.2 *Aplikace kontrolní karty 2. generace*

TCS_168 Po personalizaci musí mít aplikace kontrolní karty 2. generace následující trvalou strukturu souborů a pravidla přístupu k souborům:

Poznámka: Krátký identifikátor EF SFID je uváděn jako číslo v desítkové soustavě, tj. hodnota 30 odpovídá binární hodnotě 11110.

			Pravidla přístupu	
Soubor	**ID souboru**	**SFID**	**Čtení / výběr**	**Aktualizace**
└─DF Tachograph_G2			SC1	
├─EF Application_Identification	'0501h'	1	SC1	NEV
├─EF CardMA_Certificate	'C100h'	2	SC1	NEV
├─EF CA_Certificate	'C108h'	4	SC1	NEV
├─EF Link_Certificate	'C109h'	5	SC1	NEV
├─EF Identification	'0520h'	6	SC1	NEV
└─EF Controller_Activity_Data	'050Ch'	14	SC1	SM-MAC-G2

V této tabulce je použita tato zkratka pro bezpečnostní podmínku:

SC1 ALW OR SM-MAC-G2

TCS_169 Všechny struktury EF jsou transparentní.

TCS_170 Aplikace kontrolní karty 2. generace musí mít tuto strukturu dat:

Soubor / datový prvek	Počet záznamů	Velikost (bajty) Min	Max	
DF Tachograph_G2		*11410*	*25161*	
EF Application_Identification		*5*	*5*	
ControlCardApplicationIdentification		*5*	*5*	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfControlActivityRecords		2	2	{00 00}
EF CardMA_Certificate		*204*	*341*	
CardMACertificate		204	341	{00..00}
EF CA_Certificate		*204*	*341*	
MemberStateCertificate		204	341	{00..00}
EF Link_Certificate		*204*	*341*	
LinkCertificate		204	341	{00..00}
EF Identification		*211*	*211*	
CardIdentification		*65*	*65*	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{00, 20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
ControlCardHolderIdentification		*146*	*146*	
controlBodyName		36	36	{00, 20..20}
controlBodyAddress		36	36	{00, 20..20}
cardHolderName				
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00, 20..20}
cardHolderPreferredLanguage		2	2	{20 20}
EF Controller_Activity_Data		*10582*	*23922*	
ControlCardControlActivityData		*10582*	*23922*	
controlPointerNewestRecord		2	2	{00 00}
controlActivityRecords		*10580*	*23920*	
controlActivityRecord	n_7	*46*	*46*	
controlType		1	1	{00}
controlTime		4	4	{00..00}
controlledCardNumber				
cardType		1	1	{00}
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
controlledVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
controlDownloadPeriodBegin		4	4	{00..00}
controlDownloadPeriodEnd		4	4	{00..00}

TCS_171 Následující hodnoty používané pro označení velikostí ve výše uvedené tabulce jsou hodnoty minimálního a maximálního počtu záznamů, které musí struktura dat kontrolní karty používat pro aplikaci 2. generace:

		Min	Max
n_7	NoOfControlActivityRecords	230	520

4.5 Aplikace karty podniku

4.5.1 *Aplikace karty podniku 1. generace*

TCS_172 Po personalizaci musí mít aplikace karty podniku 1. generace následující trvalou strukturu souborů a pravidla přístupu k souborům:

		Pravidla přístupu		
Soubor	**ID souboru**	**Čtení**	**Výběr**	**Aktualizace**
DF Tachograph	'0500h'		SC1	
EF Application_Identification	'0501h'	SC2	SC1	NEV
EF Card_Certificate	'C100h'	SC2	SC1	NEV
EF CA_Certificate	'C108h'	SC2	SC1	NEV
EF Identification	'0520h'	**SC6**	SC1	NEV
EF Company_Activity_Data	'050Dh'	SC2	SC1	SC3

V této tabulce jsou použity tyto zkratky pro bezpečnostní podmínky:

SC1 ALW OR SM-MAC-G2

SC2 ALW OR SM-MAC-G1 OR SM-MAC-G2

SC3 SM-MAC-G1 OR SM-MAC-G2

SC6 EXT-AUT-G1 OR SM-MAC-G1 OR SM-MAC-G2

TCS_173 Všechny struktury EF jsou transparentní.

TCS_174 Aplikace karty podniku 1. generace musí mít tuto strukturu dat:

Soubor / datový prvek	**Počet záznamů**	**Velikost (bajty) Min**	**Max**	**Výchozí hodnoty**
DF Tachograph		*11114*	*24454*	
EF Application_Identification		*5*	*5*	
CompanyCardApplicationIdentification		*5*	*5*	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfCompanyActivityRecords		2	2	{00 00}
EF Card_Certificate		*194*	*194*	
CardCertificate		194	194	{00..00}
EF CA_Certificate		*194*	*194*	
MemberStateCertificate		194	194	{00..00}
EF Identification		*139*	*139*	
CardIdentification		*65*	*65*	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{00, 20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
CompanyCardHolderIdentification		*74*	*74*	
companyName		36	36	{00, 20..20}
companyAddress		36	36	{00, 20..20}
cardHolderPreferredLanguage		2	2	{20 20}
EF Company_Activity_Data		*10582*	*23922*	
CompanyActivityData		*10582*	*23922*	
companyPointerNewestRecord		2	2	{00 00}
companyActivityRecords		*10580*	*23920*	
companyActivityRecord	n_8	*46*	*46*	
companyActivityType		1	1	{00}
companyActivityTime		4	4	{00..00}
cardNumberInformation				
cardType		1	1	{00}
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
vehicleRegistrationInformation				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
downloadPeriodBegin		4	4	{00..00}
downloadPeriodEnd		4	4	{00..00}

TCS_175 Následující hodnoty používané pro označení velikostí ve výše uvedené tabulce jsou hodnoty minimálního a maximálního počtu záznamů, které musí struktura dat karty podniku používat pro aplikaci 1. generace

		Min	Max
n_8	NoOfCompanyActivityRecords	230	520

4.5.2 *Aplikace karty podniku 2. generace*

TCS_176 Po personalizaci musí mít aplikace karty podniku 2. generace následující trvalou strukturu souborů a pravidla přístupu k souborům:

Poznámka: Krátký identifikátor EF SFID je uváděn jako číslo v desítkové soustavě, tj. hodnota 30 odpovídá binární hodnotě 11110.

			Pravidla přístupu	
Soubor	**ID souboru**	**SFID**	**Čtení / výběr**	**Aktualizace**
└─DF Tachograph_G2			SC1	
├─EF Application_Identification	'0501h'	1	SC1	NEV
├─EF CardMA_Certificate	'C100h'	2	SC1	NEV
├─EF CA_Certificate	'C108h'	4	SC1	NEV
├─EF Link_Certificate	'C109h'	5	SC1	NEV
├─EF Identification	'0520h'	6	SC1	NEV
└─EF Company_Activity_Data	'050Dh'	14	SC1	SM-MAC-G2

V této tabulce je použita tato zkratka pro bezpečnostní podmínku:

SC1 ALW OR SM-MAC-G2

TCS_177 Všechny struktury EF jsou transparentní.

TCS_178 Aplikace karty podniku 2. generace musí mít tuto strukturu dat:

Soubor / datový prvek	Počet záznamů	Velikost (bajty) Min	Max	Výchozí hodnoty
DF Tachograph_G2		*11338*	*25089*	
EF Application_Identification		*5*	*5*	
CompanyCardApplicationIdentification		*5*	*5*	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfCompanyActivityRecords		2	2	{00 00}
EF CardMA_Certificate		*204*	*341*	
CardMACertificate		204	341	{00..00}
EF CA_Certificate		*204*	*341*	
MemberStateCertificate		204	341	{00..00}
EF Link_Certificate		*204*	*341*	
LinkCertificate		204	341	{00..00}
EF Identification		*139*	*139*	
CardIdentification		*65*	*65*	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{00, 20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
CompanyCardHolderIdentification		*74*	*74*	
companyName		36	36	{00, 20..20}
companyAddress		36	36	{00, 20..20}
cardHolderPreferredLanguage		2	2	{20 20}
EF Company_Activity_Data		*10582*	*23922*	
CompanyActivityData		*10582*	*23922*	
companyPointerNewestRecord		2	2	{00 00}
companyActivityRecords		*10580*	*23920*	
companyActivityRecord	n_8	*46*	*46*	
companyActivityType		1	1	{00}
companyActivityTime		4	4	{00..00}
cardNumberInformation				
cardType		1	1	{00}
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
vehicleRegistrationInformation				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
downloadPeriodBegin		4	4	{00..00}
downloadPeriodEnd		4	4	{00..00}

TCS_179 Následující hodnoty používané pro označení velikostí ve výše uvedené tabulce jsou hodnoty minimálního a maximálního počtu záznamů, které musí struktura dat karty podniku používat pro aplikaci 2. generace

		Min	Max
n_8	NoOfCompanyActivityRecords	230	520

Dodatek 3

PIKTOGRAMY

PIC_001 Tachograf může volitelně používat tyto piktogramy a jejich kombinace (nebo piktogramy a jejich kombinace dostatečně podobné, aby je bylo možno jednoznačně ztotožnit s těmito):

1. ZÁKLADNÍ PIKTOGRAMY

	Osoby	**Akce**	**Provozní režimy**
	podnik		podnikový režim
	kontrolor	kontrola	kontrolní režim
	řidič	řízení	provozní režim
	dílna/zkušebna	kontrola/kalibrace	kalibrační režim
	výrobce		
	Činnosti	**Doba trvání**	
	pohotovost	stávající doba pohotovosti	
	řízení	nepřetržitá doba řízení	
	odpočinek	stávající doba odpočinku	
	jiná práce	stávající pracovní doba	
	přestávka	souhrnná doba přestávek	
	neznámá		
	Zařízení	**Funkce**	
	otvor pro kartu řidiče		
	otvor pro kartu druhého řidiče		
	karta		
	hodiny		
	displej	zobrazení	
	externí paměťové médium	stahování	
	napájení		
	tiskárna/výtisk	tisk	
	snímač		
	rozměr pneumatik		
	vozidlo / celek ve vozidle		
	zařízení GNSS		
	zařízení pro dálkové odhalování		
	rozhraní ITS		
	Zvláštní podmínky		
	mimo působnost		
	převoz lodí / převoz vlakem		

Různé

!	události	⤫	závady
⏵	začátek denní pracovní doby	⏹	konec denní pracovní doby
●	místo		
M	ruční zadání činností řidiče		
🔒	zabezpečení		
>	rychlost		
◷	čas		
Σ	celkem/souhrn		

Kvalifikátory

24h	denní
|	týdenní
||	dvoutýdenní
+	od nebo do

2. KOMBINACE PIKTOGRAMŮ

Různé

▯●	místo kontroly		
●⏵	místo začátku denní pracovní doby	⏹●	místo konce denní pracovní doby
◷+	čas začátku	+◷	čas konce
🚚+	z vozidla		
OUT+	mimo působnost – začátek	+OUT	mimo působnost – konec

Karty

⊙▮	karta řidiče
🏠▮	karta podniku
▯▮	kontrolní karta
T▮	karta dílny
▮– – –	žádná karta

Řízení

⊙⊙	řízení posádkou
⊙ |	doba řízení během jednoho týdne
⊙ ||	doba řízení během dvou týdnů

Výtisky

24h ▮▼	denní výtisk činností řidiče z karty
24h 🚚▼	denní výtisk činností řidiče z celku ve vozidle
! ⤫▮▼	výtisk událostí a závad z karty
! ⤫🚚▼	výtisk událostí a závad z celku ve vozidle
T◷▼	výtisk technických dat
>>▼	výtisk překročení povolené rychlosti

Události

	vložení neplatné karty
	konflikt karet
	časový přesah
	řízení bez příslušné karty
	vložení karty během řízení
	nesprávné ukončení poslední relace karty
	překročení povolené rychlosti
	přerušení napájení
	chyba údajů o pohybu vozidla
	nesoulad údajů o pohybu vozidla
	narušení zabezpečení
	nastavení času (dílnou)
	kontrola překročení povolené rychlosti

Závady

	závada karty (otvor pro kartu řidiče)
	závada karty (otvor pro kartu druhého řidiče)
	závada displeje
	závada stahování
	závada tiskárny
	závada snímače
	interní závada celku ve vozidle
	závada GNSS
	závada dálkového odhalování

Proces ručního zadávání

	nadále tatáž denní pracovní doba?
	konec předešlé pracovní doby?
	potvrzení nebo zadání místa konce pracovní doby
	zadání času začátku
	zadání místa začátku pracovní doby

Poznámka: Další kombinace piktogramů k vytvoření bloků ve výtiscích nebo identifikátorů záznamů jsou definovány v dodatku 4.

Dodatek 4

VÝTISKY

OBSAH

1. VŠEOBECNÉ

Každý výtisk je tvořen zřetězením různých datových bloků, které mohou být identifikovány identifikátorem bloku.

Datový blok obsahuje jeden nebo více záznamů, které mohou být identifikovány identifikátorem záznamu.

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

PRT_002 Není-li některá datová položka známa nebo nesmí být vytištěna z důvodu přístupových práv k údajům, vytisknou se místo ní mezery.

PRT_003 Není-li znám obsah celé řádky nebo není třeba jej tisknout, vynechá se celá řádka.

PRT_004 Číselná datová pole se tisknou zarovnaná doprava, s mezerou jako oddělovačem tisíců a milionů a bez nul na začátku.

PRT_005 Řetězcová datová pole se tisknou zarovnaná doleva a doplněná mezerami na délku datové položky, nebo v případě potřeby zkrácená na délku datové položky (jména či názvy a adresy).

PRT_006 V případě zalomení řádky z důvodu dlouhého textu se jako první znak na nové řádce vytiskne zvláštní znak (tečka uprostřed výšky řádky – „•“).

2. SPECIFIKACE DATOVÝCH BLOKŮ

V této kapitole je použita následující konvence, pokud jde o formát:

— znaky vytištěné **tučně** označují prostý text k vytištění (tiskne se normálními znaky),

— normální znaky označují proměnné (piktogramy nebo data), které se při tisku nahradí svými hodnotami,

— názvy proměnných jsou doplněny podtržítky, aby se znázornila délka datové položky, která je pro proměnnou k dispozici,

— datum se uvádí ve formátu „dd/mm/yyyy“ (den/měsíc/rok). Smí se použít i formát „dd.mm.yyyy“,

— termín „identifikace karty“ označuje posloupnost: typu karty znázorněného kombinací piktogramů karty, kódu členského státu vydávajícího kartu, znaku lomítka a čísla karty s indexem náhrady a indexem obnovy oddělenými mezerami:

P	■	x	x	x	/	x	x	x	x	x	x	x	x	x	x	x	x	x		x		x
Kombinace piktogramů karty		Kód vydávajícího členského státu				Prvních 14 znaků čísla karty (případně s pořadovým indexem)														Index náhrady		Index obnovy

PRT_007 Ve výtiscích se používají následující datové bloky a/nebo datové záznamy v souladu s následujícími významy a formáty:

Číslo bloku nebo záznamu Význam	Data Format
1 ***Datum a čas vytištění dokumentu***	▼ dd/mm/yyyy hh:mm **(UTC)**
2 ***Typ výtisku*** Identifikátor bloku Kombinace piktogramů výtisku (viz dodatek 3), nastavení omezovače rychlosti (pouze výtisk překročení povolené rychlosti)	----------▼---------- Picto xxx **km/h**
3 ***Identifikace držitele karty*** Identifikátor bloku. P = piktogram osoby Příjmení držitele karty Jméno (jména) držitele karty (pokud existují) Identifikace karty Datum konce platnosti karty (pokud existuje) a číslo generace karty (GEN 1 nebo GEN 2) (*)	----------P---------- P Last_Name_____ First_Name_____ Card_Identification_____ dd/mm/yyyy - GEN 2

V případě, že se jedná o neosobní kartu, na které není uvedeno žádné příjmení držitele, vytiskne se namísto něj název podniku, dílny nebo kontrolního subjektu.

(*) Číslo generace karty může vytisknout pouze inteligentní tachograf.

4 ***Identifikace vozidla*** Identifikátor bloku VIN Členský stát registrace a registrační značka vozidla (VRN)	----------🚘---------- 🚘 VIN_____ Nat/VRN_____
5 ***Identifikace celku ve vozidle (VU)*** Identifikátor bloku Název výrobce VU Číslo dílu VU Číslo generace VU (*)	----------⊟---------- ⊟ VU_Manufacturer_____ VU_Part_Number__ GEN 2

(*) Číslo generace karty může vytisknout pouze inteligentní tachograf.

6 ***Poslední kalibrace tachografu*** Identifikátor bloku Název dílny Identifikace karty dílny Datum kalibrace	----------🔧---------- 🔧 Last_Name_____ Card_Identification_____ 🔧 dd/mm/yyyy

7 ***Poslední kontrola (kontrolorem)***

Identifikátor bloku
Identifikace karty kontrolora
Datum, čas a typ kontroly

```
----------▯----------
Card_Identification_____
▯ dd/mm/yyyy hh:mm ppppp
```

Typ kontroly: až pět piktogramů. Možné typy kontroly jsou následující (včetně jejich kombinací):
▮: stahování dat z karty, ▼: stahování dat z celku ve vozidle, ▛: tisk, □: zobrazení, ▔: silniční kontrola kalibrace

8 ***Činnosti řidiče uložené na kartě v pořadí, v jakém k nim došlo***

Identifikátor bloku
Datum dotazu (kalendářní den, kterého se výtisk týká) + stav počitadla dnů přítomnosti karty

```
----------⊙----------
    dd/mm/yyyy  xxx
```

8a *Podmínka „mimo působnost" na začátku tohoto dne* (ponechá se prázdné, pokud není otevřen záznam podmínky „mimo působnost")

```
----------OUT----------
```

8.1 *Doba, během které nebyla karta vložena*
8.1a Identifikátor záznamu (začátek doby)
8.1b *Neznámá doba*. Čas začátku, doba trvání
8.1c *Ručně zadaná činnost*.
Piktogram činnosti, čas začátku, doba trvání

```
  --------------------
?       hh:mm hhhmm
A       hh:mm hhhmm
```

8.2 *Vložení karty do otvoru pro kartu S*
Identifikátor záznamu; S = piktogram otvoru
Členský stát registrace vozidla a VRN
Stav počitadla ujetých kilometrů při vložení karty

```
  ---------S---------
🚘 Nat/VRN__________
  x xxx xxx km
```

8.3 *Činnost (při vložené kartě)*
Piktogram činnosti, čas začátku, doba trvání, stav posádky (piktogram posádky, pokud je stav POSÁDKA, prázdná místa, pokud je stav SAMOTNÝ ŘIDIČ).

```
A       hh:mm hhhmm ⊙⊙
```

8.3a *Zvláštní podmínka*. Čas zadání, piktogram zvláštní podmínky (nebo kombinace piktogramů).

```
        hh:mm ---pppp---
```

8.4 *Vyjmutí karty*
Stav počitadla ujetých kilometrů a vzdálenost ujetá od posledního vložení, u kterého je známý stav počitadla ujetých kilometrů

```
  x xxx xxx km; x xxx km
```

9 ***Činnosti řidiče zaznamenané v celku ve vozidle u jednotlivých otvorů pro kartu v chronologickém pořadí***

Identifikátor bloku
Datum dotazu (kalendářní den, kterého se výtisk týká)
Stav počitadla ujetých kilometrů v 00:00 hod. a ve 24:00 hod.

```
----------⊙----------
       dd/mm/yyyy
x xxx xxx - x xxx xxx km
```

10 ***Činnosti provedené v otvoru pro kartu S***

Identifikátor bloku

```
----------S----------
```

10a *Podmínka „mimo působnost" na začátku tohoto dne* (ponechá se prázdné, pokud není otevřen záznam podmínky „mimo působnost")

```
----------OUT----------
```

10.1 *Doba, během které nebyla v otvoru S vložena žádná karta*
Identifikátor záznamu
Není vložena žádná karta
Stav počitadla ujetých kilometrů na začátku doby

```
  --------------------
⊙▮---
  x xxx xxx km
```

10.2 *Vložení karty*
Identifikátor záznamu o vložení karty
Příjmení řidiče

```
  --------------------
⊙ Last_Name_____________
```

	Jméno řidiče	First_Name_____
	Identifikace karty řidiče	Card_Identification_____
	Datum konce platnosti karty (pokud existuje) a číslo generace karty (GEN 1 nebo GEN 2) (*)	dd/mm/yyyy - GEN 2
	Členský stát registrace a VRN předchozího použitého vozidla	+Nat/VRN_____
	Datum a čas vyjmutí karty z předchozího vozidla	dd/mm/yyyy hh:mm
	Prázdná řádka	
	Stav počitadla ujetých kilometrů při vložení karty, příznak ručního zadání činností řidiče (M, pokud ano, prázdné místo, pokud ne).	x xxx xxx **km** M
	Pokud v den, za který se provádí výtisk, nedošlo k žádnému vložení karty řidiče, použije se v bloku 10.2 stav počitadla ujetých kilometrů při posledním dostupném vložení karty před tímto dnem.	
10.3	*Činnost*	
	Piktogram činnosti, čas začátku, doba trvání, stav posádky (piktogram posádky, pokud je stav POSÁDKA, prázdné místo, pokud je stav SAMOTNÝ ŘIDIČ).	A hh:mm hh**h**mm
10.3a	*Zvláštní podmínka.* Čas zadání, piktogram zvláštní podmínky (nebo kombinace piktogramů).	hh:mm ---pppp---
10.4	*Vyjmutí karty nebo konec doby bez vložené karty*	
	Stav počitadla ujetých kilometrů vozidla při vyjmutí karty nebo na konci doby bez vložené karty a vzdálenost ujetá od vložení karty nebo od začátku doby bez vložené karty.	x xxx xxx **km**; x xxx **km**

(*) Číslo generace karty může vytisknout pouze inteligentní tachograf.

11	***Denní souhrn***	
	Identifikátor bloku	----------Σ----------
11.1	***VU – souhrn dob bez karty v otvoru pro kartu řidiče***	
	Identifikátor bloku	1----
11.2	***VU – souhrn dob bez karty v otvoru pro kartu druhého řidiče***	
	Identifikátor bloku	2----
11.3	***VU – denní souhrn pro jednotlivé řidiče***	
	Identifikátor záznamu	----------
	Příjmení řidiče	Last_Name_____
	Jméno (jména) řidiče	First_Name_____
	Identifikace karty řidiče	Card_Identification_____
11.4	*Zadání místa začátku a/nebo konce denní pracovní doby*	
	pi=piktogram místa začátku/konce, čas, země, region,	pihh:mm Cou Reg
	stav počitadla ujetých kilometrů	x xxx xxx **km**
11.5	*Zadání místa začátku a/nebo konce denní pracovní doby*	
	a po 3 hodinách nepřetržité doby řízení	hh:mm
	Stav počitadla ujetých kilometrů	x xxx xxx **km**
11.6	*Celkové doby trvání činností (z karty)*	
	Celková doba řízení, ujetá vzdálenost	hh**h**mm x xxx **km**
	Celková doba práce a pracovní pohotovosti	hh**h**mm hh**h**mm
	Celková doba odpočinku a neznámé činnosti	hh**h**mm hh**h**mm
	Celková doba činností posádky	hh**h**mm
11.7	*Celkové doby trvání činností (v době bez karty v otvoru pro kartu řidiče)*	
	Celková doba řízení, ujetá vzdálenost	hh**h**mm x xxx **km**
	Celková doba práce a pracovní pohotovosti	hh**h**mm hh**h**mm
	Celková doba odpočinku	hh**h**mm

11.8	*Celkové doby trvání činností (v době bez karty v otvoru pro kartu druhého řidiče)*	
	Celková doba práce a pracovní pohotovosti	⚒ hh**h**mm ⧈ hh**h**mm
	Celková doba odpočinku	⊢ hh**h**mm
11.9	*Celkové doby trvání činností (pro jednotlivé řidiče, zahrnou se oba otvory pro kartu)*	
	Celková doba řízení, ujetá vzdálenost	⊙ hh**h**mm x xxx **km**
	Celková doba práce a pracovní pohotovosti	⚒ hh**h**mm ⧈ hh**h**mm
	Celková doba odpočinku	⊢ hh**h**mm
	Celková doba činností posádky	⊙⊙ hh**h**mm

Pokud je požadován denní výtisk za aktuální den, vypočtou se denní souhrnné informace z údajů, které jsou k dispozici v okamžiku tisku.

12	***Události a/nebo chyby uložené na kartě***	
12.1	Identifikátor bloku posledních pěti událostí a závad z karty	----------!×▬----------
12.2	Identifikátor bloku všech událostí zaznamenaných na kartě	----------!▬----------
12.3	Identifikátor bloku všech závad zaznamenaných na kartě	----------×▬----------
12.4	*Záznam události a/nebo závady*	
	Identifikátor záznamu Piktogram události/závady, účel záznamu, datum a čas začátku, dodatečný kód události/závady (pokud existuje), doba trvání Členský stát registrace a registrační značka (VRN) vozidla, ve kterém k události nebo závadě došlo	---------- Pic (p) dd/mm/yyyy hh:mm !xx hh**h**mm 🚘 Nat/VRN_____

13	***Události a/nebo závady uložené nebo probíhající ve VU***	
13.1	Identifikátor bloku posledních pěti událostí a závad z VU	----------!×🚘----------
13.2	Identifikátor bloku všech zaznamenaných nebo probíhajících událostí ve VU	----------!🚘----------
13.3	Identifikátor bloku všech zaznamenaných nebo probíhajících závad ve VU	----------×🚘----------
13.4	*Záznam události a/nebo závady*	
	Identifikátor záznamu Piktogram události/závady, účel záznamu, datum a čas začátku, dodatečný kód události nebo závady (pokud existuje), počet podobných událostí v tomtéž dni, doba trvání Identifikace karet vložených na začátku nebo na konci události nebo závady (až 4 řádky, bez opakování stejných čísel karty) Případ, kdy nebyla vložena žádná karta Údaje specifické pro výrobce	---------- Pic (p) dd/mm/yyyy hh:mm !xx (xxx) hh**h**mm Card_Identification_____ Card_Identification_____ Card_Identification_____ Card_Identification_____ ▬--- **< Literal><ErrorCode>**

Účel záznamu (p) je číselný kód vysvětlující, proč byla událost nebo závada zaznamenána, a kódovaný v souladu s datovým prvkem `EventFaultRecordPurpose`.

`Literal` je literál specifický pro výrobce tachografu s délkou maximálně 12 znaků.

`ErrorCode` je kód chyby specifický pro výrobce tachografu s délkou maximálně 12 znaků.

14 ***Identifikace VU***

Identifikátor bloku	----------B----------
Název výrobce VU	B Name_____
Adresa výrobce VU	Address_____
Číslo dílu VU	PartNumber_____
Číslo schválení VU	Apprv_____
Výrobní číslo VU	S/N_____
Rok výroby VU	yyyy
Verze softwaru a datum instalace VU	V xxxx dd/mm/yyyy

15 ***Identifikace snímače***

Identifikátor bloku	----------Л----------

15.1 *Záznam o párování*

Výrobní číslo snímače	Л S/N_____
Číslo schválení snímače	Apprv_____
Datum párování snímače	dd/mm/yyyy hh:mm

16 ***Identifikace GNSS***

Identifikátor bloku	----------▚----------

16.1 *Záznam o vazbě*

Výrobní číslo vnějšího zařízení GNSS	▚ S/N_____
Číslo schválení vnějšího zařízení GNSS	Apprv_____
Datum vazby s vnějším zařízením GNSS	dd/mm/yyyy hh:mm

17 ***Kalibrační údaje***

Identifikátor bloku	----------T----------

17.1 *Záznam o kalibraci*

Identifikátor záznamu	----------
Dílna, která kalibraci provedla	T Workshop_name_____
Adresa dílny	Workshop_address_____
Identifikace karty dílny	Card_Identification_____
Datum konce platnosti karty dílny	dd/mm/yyyy
Prázdná řádka	
Datum kalibrace + účel kalibrace	T dd/mm/yyyy (p)
VIN	A VIN_____
Členský stát registrace a VRN	Nat/VRN_____
Charakteristický koeficient vozidla	w xx xxx Imp/km
Konstanta záznamového zařízení	k xx xxx Imp/km
Effective circumference of wheel tyres	l xx xxx mm
Rozměr namontovaných pneumatik	● TyreSize_____
Nastavení omezovače rychlosti	> xxx km/h
Stará a nová hodnota počitadla ujetých kilometrů	x xxx xxx – x xxx xxx km

Účel kalibrace (p) je číselný kód vysvětlující, proč byly tyto kalibrační parametry zaznamenány, a kódovaný v souladu s datovým prvkem `CalibrationPurpose`.

18 ***Nastavení času***

Identifikátor bloku

```
----------◷----------
```

18.1 *Záznam o nastavení času*

Identifikátor záznamu
Staré datum a čas
Nové datum a čas
Dílna, která nastavení času provedla
Adresa dílny
Identifikace karty dílny
Datum konce platnosti karty dílny

```
  --------------------
!◷ dd/mm/yyyy  hh:mm
 ◷ dd/mm/yyyy  hh:mm
T Workshop_name_________
  Workshop_address______
Card_Identification_____
  dd/mm/yyyy
```

19 ***Nejnovější událost a závada zaznamenané ve VU***

Identifikátor bloku
Datum a čas nejnovější události
Datum a čas nejnovější závady

```
----------!×🚶----------
! dd/mm/yyyy  hh:mm
× dd/mm/yyyy  hh:mm
```

20 ***Informace o kontrole překročení povolené rychlosti***

Identifikátor bloku
Datum a čas poslední KONTROLY PŘEKROČENÍ POVOLENÉ RYCHLOSTI
Datum/čas prvního překročení povolené rychlosti a počet událostí překročení povolené rychlosti od té doby

```
----------►►----------
►▯dd/mm/yyyy hh:mm

►►dd/mm/yyyy hh:mm (nnn)
```

21 ***Záznam o překročení povolené rychlosti***

21.1 Identifikátor bloku „první překročení povolené rychlosti po poslední kalibraci“

```
--------►►T---------
```

21.2 Identifikátor bloku „pět nejzávažnějších během posledních 365 dní“

```
-------►►(365)------
```

21.3 Identifikátor bloku „nejzávažnější v každém z posledních 10 dnů výskytu“

```
-------►►(10)-------
```

21.4 Identifikátor záznamu
Datum, čas a doba trvání
Maximální a průměrná rychlost, počet podobných událostí v tomtéž dni
Příjmení řidiče
Jméno (jména) řidiče
Identifikace karty řidiče

```
  --------------------
►►dd/mm/yyyy hh:mm hhhmm
  xxx km/h xxx km/h(xxx)

◙ Last_Name____________
  First_Name___________
Card_Identification_____
```

21.5 Pokud v bloku neexistuje záznam o překročení povolené rychlosti

```
►►---
```

22 ***Ručně zapisované informace***

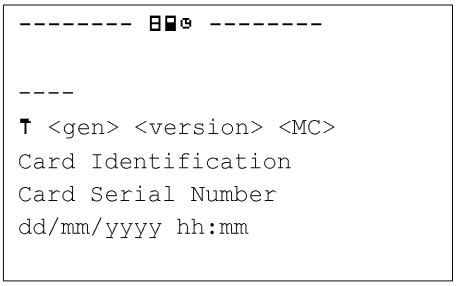
Identifikátor bloku

```
------------------------
▯• ..................
▯  ..................
◷+ ..................
+◷ ..................
◙  ..................
```

22.1 Místo kontroly
22.2 Podpis kontrolora
22.3 Čas začátku
22.4 Čas konce
22.5 Podpis řidiče

„Ručně zapisované informace“: před ručně zapisovaný údaj vložte dostatečný počet prázdných řádek, aby bylo skutečně možno zapsat požadované informace nebo se podepsat.

23 ***Karty naposledy vložené do VU***
Identifikátor bloku
23.1 Vložená karta
Identifikátor záznamu
Typ karty, generace, verze, výrobce (*)
Identifikace karty
Výrobní číslo karty
Datum a čas posledního vložení karty



(*) (vše na jedné řádce)
přičemž
typ karty: piktogram, jeden znak + mezera
gen: GEN1 nebo GEN2, 4 znaky + mezera
verze: až 10 znaků
MC: kód výrobce, 3 znaky

3. SPECIFIKACE VÝTISKŮ

V této kapitole je použita následující konvence:

N	Tisk bloku nebo záznamu s číslem N
N	Tisk bloku nebo záznamu s číslem N tolikrát, kolikrát je třeba
X/Y	Tisk bloků nebo záznamů X a/nebo Y dle potřeby a tolikrát, kolikrát je třeba

3.1 Denní výtisk činností řidiče z karty

PRT_008 Denní výtisk činností řidiče z karty musí mít následující formát:

1	Datum a čas vytištění dokumentu
2	Typ výtisku
3	Identifikace kontrolora (pokud je do VU vložena kontrolní karta)
3	Identifikace řidiče (z karty, pro kterou se výtisk pořizuje, + 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, které byl kontrolovaný řidič podroben
8	Oddělovač činností řidiče
8a	Na začátku tohoto dne platila podmínka „mimo působnost“
8.1a / 8.1b / 8.1c / 8.2 / 8.3 / 8.3a / 8.4	Činnosti řidiče v pořadí, v jakém k nim došlo
11	Oddělovač denního souhrnu

11.4	Zadaná místa v chronologickém pořadí
11.5	Údaje GNSS
11.6	Celkové doby trvání činností
12.1	Oddělovač událostí nebo závad z karty
12.4	Záznamy událostí/závad (posledních 5 událostí nebo závad uložených na kartě)
13.1	Oddělovač událostí nebo závad z VU
13.4	Záznamy událostí/závad (posledních 5 událostí nebo závad uložených nebo probíhajících ve VU)
22.1	Místo kontroly
22.2	Podpis kontrolora
22.5	Podpis řidiče

3.2 **Denní výtisk činností řidiče z VU**

PRT_009 Denní výtisk činností řidiče z VU musí mít následující formát:

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	Údaje GNSS
11.6	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	Údaje GNSS

11.7	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	Údaje GNSS
11.8	Celkové doby trvání činností tohoto řidiče
13.1	Oddělovač událostí a závad
12.4	Záznamy událostí/závad (posledních 5 událostí nebo závad uložených nebo probíhajících ve VU)
13.1	Místo kontroly
22.2	Podpis kontrolora
22.3	Čas začátku (místo, kde může řidič bez karty uvést, která období se ho týkají)
22.4	Čas konce
22.5	Podpis řidiče

3.3 **Výtisk událostí a závad z karty**

PRT_010 Výtisk událostí a závad z karty musí mít následující formát:

1	Datum a čas vytištění dokumentu
2	Typ výtisku
3	Identifikace kontrolora (pokud je do VU vložena kontrolní karta, + GEN)
3	Identifikace řidiče (z karty, které se výtisk týká)
4	Identifikace vozidla (z nějž se výtisk pořizuje)
12.2	Oddělovač událostí
12.4	Záznamy událostí (všechny události uložené na kartě)
12.3	Oddělovač závad
12.4	Záznamy závad (všechny závady uložené na kartě)
22.1	Místo kontroly
22.2	Podpis kontrolora
22.5	Podpis řidiče

3.4 **Výtisk událostí a závad z VU**

PRT_011 Výtisk událostí a závad z VU musí mít následující formát:

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)

13.2	Oddělovač událostí
13.4	Záznamy událostí (všechny události uložené nebo probíhající ve VU)
13.3	Oddělovač závad
13.4	Záznamy závad (všechny závady uložené nebo probíhající ve VU)
22.1	Místo kontroly
22.2	Podpis kontrolora
22.5	Podpis řidiče

3.5 **Výtisk technických dat**

PRT_012 Výpis technických dat musí mít následující formát:

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)
14	Identifikace VU
15	Identifikace snímače
15.1	Údaje o párování snímačů (všechny dostupné údaje v chronologickém pořadí)
16	Identifikace GNSS
16.1	Údaje o vazbě s vnějším zařízením GNSS (všechny dostupné údaje v chronologickém pořadí)
17	Oddělovač kalibračních údajů
17.1	Záznamy o kalibraci (všechny dostupné záznamy v chronologickém pořadí)
18	Oddělovač nastavení času
18.1	Záznamy o nastavení času (všechny dostupné záznamy z nastavení času a ze záznamů kalibračních údajů)
19	Nejnovější událost a závada zaznamenané ve VU

3.6 **Výtisk překročení povolené rychlosti**

PRT_013 Výtisk překročení povolené rychlosti musí mít následující formát:

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)
20	Informace o kontrole překročení povolené rychlosti
21.1	Identifikátor údajů o překročení povolené rychlosti
21.4 / 21.5	První překročení povolené rychlosti po poslední kalibraci

21.2	Identifikátor údajů o překročení povolené rychlosti
21.4 / 21.5	5 nejzávažnějších překročení povolené rychlosti za posledních 365 dnů
21.3	Identifikátor údajů o překročení povolené rychlosti
21.4 / 21.5	Nejzávažnější překročení povolené rychlosti v každém z posledních 10 dnů výskytu
22.1	Místo kontroly
22.2	Podpis kontrolora
22.5	Podpis řidiče

3.7 **Historie vložených karet**

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

Dodatek 5

ZOBRAZENÍ

V tomto dodatku je použita tato konvence, pokud jde o formát:

— znaky vytištěné **tučně** znamenají prostý text, který se má zobrazit (zobrazí se normálními znaky),

— normální znaky označují proměnné (piktogramy nebo údaje), které se při zobrazení nahradí svými hodnotami,

— dd mm yyyy: den, měsíc, rok,

— hh: hodiny,

— mm: minuty,

— D: piktogram doby trvání,

— EF: kombinace piktogramů události nebo závady,

— O: piktogram provozního režimu.

DIS_001 Tachograf zobrazuje data na displeji v následujících formátech:

Údaje	Formát
Výchozí zobrazení	
Místní čas	hh:mm
Provozní režim	O
Informace o řidiči	1Dhh**h**mm ▮▮hh**h**mm
Informace o druhém řidiči	2Dhh**h**mm
Otevřená podmínka „mimo působnost“	OUT
Varovné zobrazení	
Překročení nepřetržité doby řízení	1⊙hh**h**mm ▮▮hh**h**mm
Událost nebo závada	EF
Další zobrazení	
Datum v UTC čas	UTC⊙dd/mm/yyyy nebo UTC⊙dd.mm.yyyy hh:mm
Nepřetržitá doba řízení a souhrnná doba přestávek – řidič	1⊙hh**h**mm ▮▮hh**h**mm
Nepřetržitá doba řízení a souhrnná doba přestávek – druhý řidič	2⊙hh**h**mm ▮▮hh**h**mm
Souhrnná doba řízení za předchozí a aktuální týden – řidič	1⊙▮▮ hhh**h**mm
Souhrnná doba řízení za předchozí a aktuální týden – druhý řidič	2⊙▮▮ hhh**h**mm

Dodatek 6

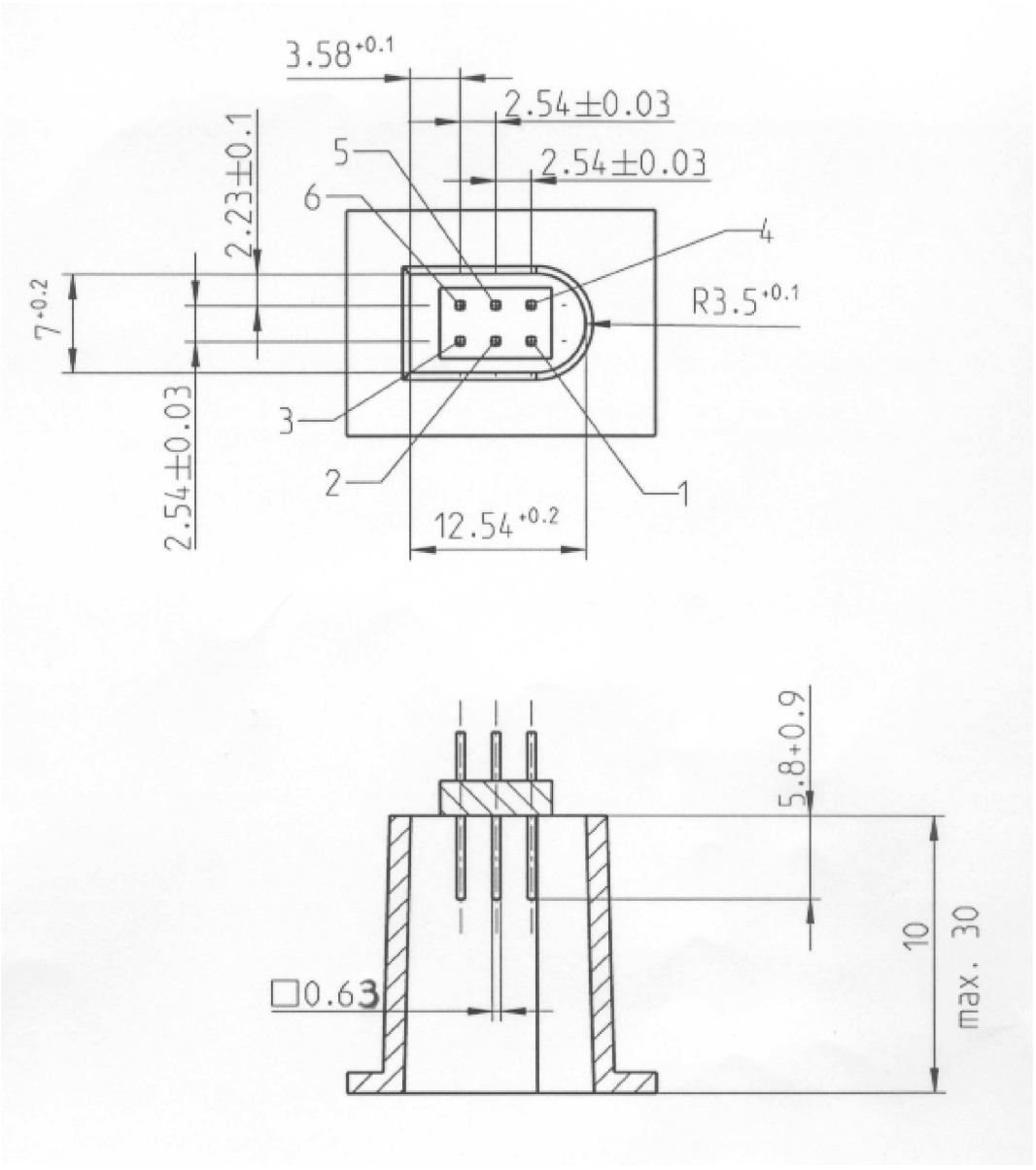
PŘEDNÍ KONEKTOR PRO KALIBRACI A STAHOVÁNÍ

OBSAH

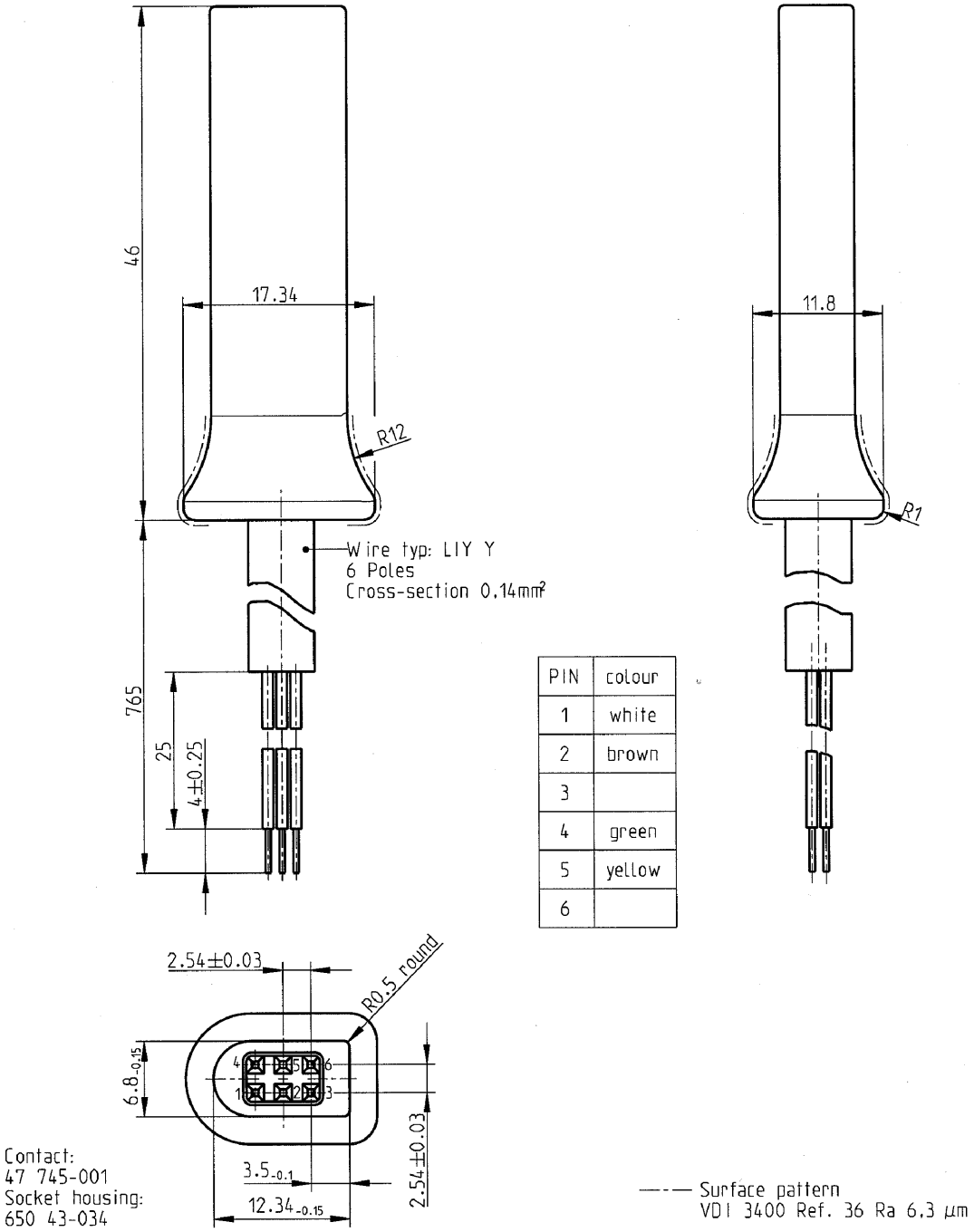
1. TECHNICKÉ VYBAVENÍ

1.1 **Konektor**

INT_001 Konektor pro stahování/kalibraci je šestikolíkový, je přístupný na předním panelu bez nutnosti odpojení jakékoli části tachografu a odpovídá následujícímu výkresu (všechny rozměry jsou v milimetrech):



Následující výkres znázorňuje typický šestikolíkový protikus:



1.2 **Zapojení kontaktů**

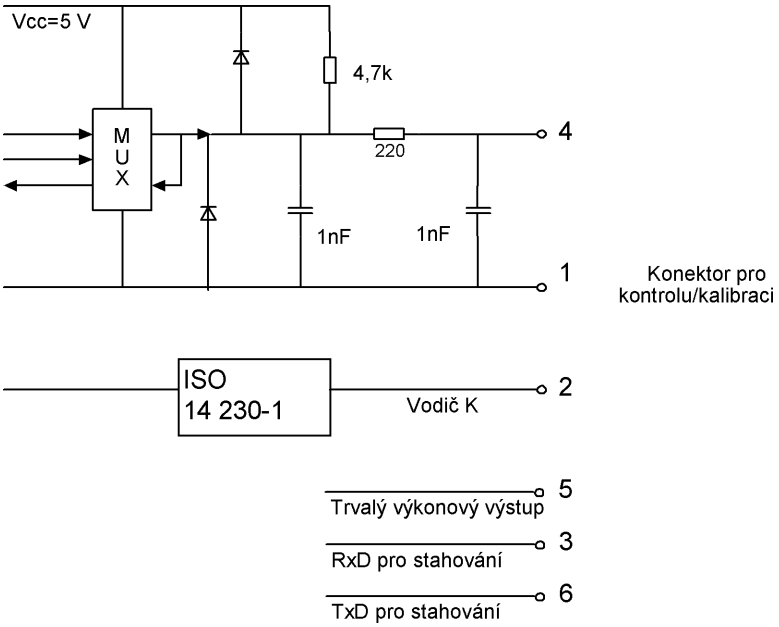
INT_002 Kontakty jsou zapojeny podle následující tabulky:

Kolík	Popis	Poznámka
1	Záporný pól baterie	Připojen k zápornému pólu baterie vozidla
2	Datová komunikace	Vodič K (ISO 14230-1)

Kolík	Popis	Poznámka
3	RxD pro stahování	Vstup dat do tachografu
4	Vstupní/výstupní signál	Kalibrace
5	Trvalý výkonový výstup	Napěťový rozsah je specifikován jako napěťový rozsah elektroinstalace vozidla minus 3 V pro zohlednění poklesu napětí na ochranných obvodech Výstup 40 mA
6	TxD pro stahování	Výstup dat z tachografu

1.3 **Blokové schéma**

INT_003 Blokové schéma musí odpovídat tomuto:



2. ROZHRANÍ PRO STAHOVÁNÍ

INT_004 Rozhraní pro stahování musí splňovat specifikace RS232.

INT_005 Rozhraní pro stahování používá jeden start bit, 8 datových bitů, z nichž první je nejméně významný (LSB), jeden bit sudé parity a 1 stop bit.

Uspořádání datového bajtu

Start bit: jeden bit s logickou úrovní 0

Datové bity: přenášené s nejméně významným bitem jako prvním

Paritní bit: sudá parita

Stop bit: jeden bit s logickou úrovní 1

Při přenosu číselných dat tvořených více bajty se nejvýznamnější bajt se přenese jako první a nejméně významný bajt jako poslední.

INT_006 Rychlost přenosu dat musí být nastavitelná od 9 600 bit/s do 115 200 bit/s. Přenos se uskutečňuje při nejvyšší možné rychlosti, počáteční rychlost přenosu dat po zahájení komunikace se nastaví na 9 600 bit/s.

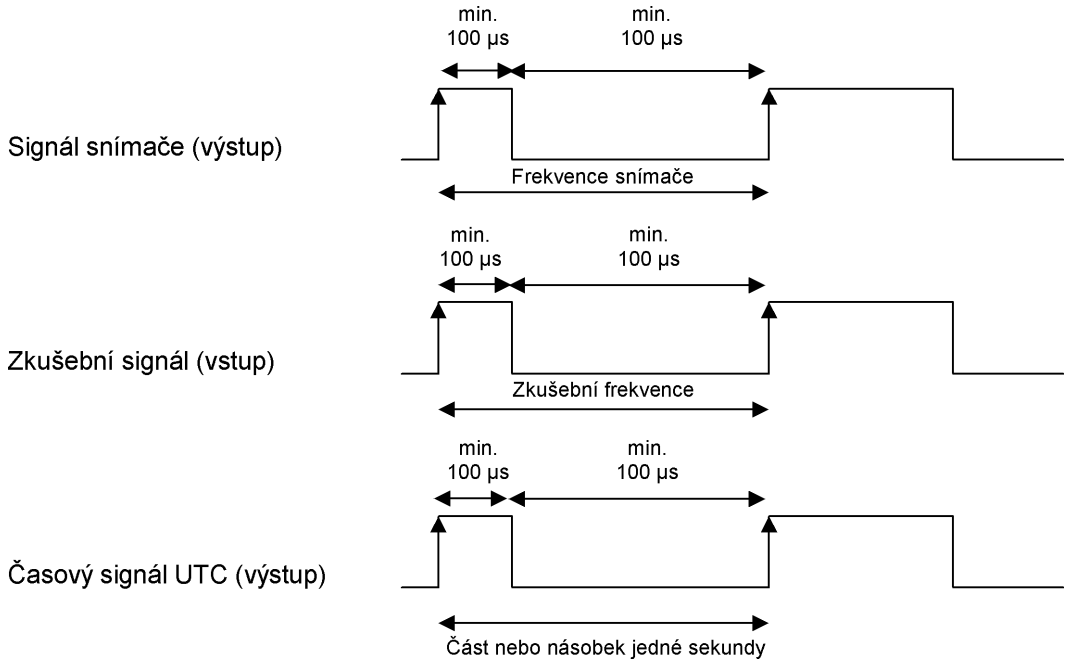
3. ROZHRANÍ PRO KALIBRACI

INT_007 Datová komunikace musí splňovat normu ISO 14230-1 *Road vehicles – Diagnostic systems – Keyword protocol 2000 – Part 1: Physical layer, First edition: 1999*.

INT_008 Vstupní/výstupní signál musí splňovat tyto elektrické specifikace:

Parametr	Minimum	Typická hodnota	Maximum	Poznámka
U_{low} (in)			1,0 V	I = 750 µA
U_{high} (in)	4 V			I = 200 µA
Frekvence			4 kHz	
U_{low} (out)			1,0 V	I = 1 mA
U_{high} (out)	4 V			I = 1 mA

INT_009 Vstupní/výstupní signál musí splňovat tyto časové diagramy:



Dodatek 7

PROTOKOLY PRO STAHOVÁNÍ DAT

OBSAH

1. ÚVOD

Tento dodatek určuje postupy pro stahování různých typů dat na externí paměťové médium a protokoly, které je nutno implementovat k zajištění správného přenosu dat a plné slučitelnosti formátu stažených dat, aby kterýkoli kontrolor mohl tato data prověřit a před jejich analýzou zkontrolovat jejich pravost a integritu.

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.

DDP_001 Data stažená během jedné relace stahování musí být uložena na externím paměťovém médiu v jednom souboru.

1.2 **Zkratky a notace**

V tomto dodatku jsou použity následující zkratky:

AID identifikátor aplikace (*Application Identifier*)

ATR odpověď na reset (*Answer To Reset*)

CS bajt kontrolního součtu (*Checksum byte*)

DF vyhrazený soubor (*Dedicated File*)

DS_ diagnostická relace (*Diagnostic Session*)

EF elementární soubor (*Elementary File*)

ESM externí paměťové médium (*External Storage Medium*)

FID identifikátor souboru (*File ID*)

FMT bajt formátu (první bajt hlavičky zprávy) (*Format Byte*)

ICC karta s integrovaným obvodem, čipová karta (*Integrated Circuit Card*)

IDE inteligentní vyhrazené zařízení (*Intelligent Dedicated Equipment*): zařízení používané pro stahování dat na ESM (např. osobní počítač)

IFD zařízení rozhraní (*Interface Device*)

KWP protokol KWP 2000 (*Keyword Protocol 2000*)

LEN bajt délky (poslední bajt hlavičky zprávy)

PPS volba parametrů protokolu (*Protocol Parameter Selection*)

PSO provedení bezpečnostní operace (*Perform Security Operation*)

SID identifikátor služby (*Service Identifier*)

SRC bajt zdroje (*Source byte*)

TGT bajt cíle (*Target byte*)

TLV tag, délka, hodnota (*Tag Length Value*)

TREP parametr odpovědi na požadavek na přenos (*Transfer Response Parameter*)

TRTP parametr požadavku na přenos (*Transfer Request Parameter*)

VU celek ve vozidle (*Vehicle Unit*)

2. STAHOVÁNÍ DAT Z CELKU VE VOZIDLE

2.1 **Postup stahování**

Ke stažení dat z VU musí operátor provést následující operace:

— vsunout svou kartu tachografu do otvoru pro kartu v celku ve vozidle (*),

— připojit IDE ke konektoru VU pro stahování,

— navázat spojení mezi IDE a VU,

— vybrat v IDE data, která se mají stáhnout, a odeslat požadavek do VU,

— uzavřít relaci stahování.

2.2 **Protokol pro stahování dat**

Protokol používá strukturu „master-slave“ s IDE jako nadřízeným zařízením a VU jako podřízeným zařízením.

Struktura, typy a tok zpráv jsou v zásadě založeny na protokolu KWP 2000 (ISO 14230-2 *Road vehicles – Diagnostic systems – Keyword protocol 2000 – Part 2: Data link layer*).

Aplikační vrstva je v zásadě založena na aktuálním návrhu ISO 14229-1 (*Road vehicles – Diagnostic systems – Part 1: Diagnostic services, version 6 of 22 February 2001*).

2.2.1 *Struktura zpráv*

DDP_002 Všechny zprávy vyměňované mezi IDE a VU mají formát struktury sestávající ze tří částí:

— hlavičky složené z bajtu formátu (FMT), bajtu cíle (TGT), bajtu zdroje (SRC) a v příslušných případech bajtu délky (LEN),

— datového pole složeného z bajtu identifikátoru služby (SID) a proměnného počtu datových bajtů, které mohou případně zahrnovat volitelný bajt diagnostické relace (DS_) nebo volitelný bajt parametru přenosu (TRTP nebo TREP),

— kontrolního součtu tvořeného bajtem kontrolního součtu (CS).

Hlavička				Datové pole					Kontrolní součet
FMT	TGT	SRC	LEN	SID	DATA	…	…	…	CS
4 bajty				Max. 255 bajtů					1 bajt

(*) Vložená karta aktivuje příslušná přístupová práva k funkci stahování a k datům. Musí být nicméně možné stáhnout data z karty řidiče vložené do jednoho z otvorů pro kartu ve VU, i když v druhém otvoru pro kartu není vložena žádná karta.

Bajty TGT a SRC představují fyzickou adresu příjemce a původce zprávy. Hodnoty jsou F0 hex pro IDE a EE hex pro VU.

Bajt LEN je délka datového pole.

Bajt kontrolního součtu je osmibitový součet modulo 256 všech bajtů zprávy vyjma samotného CS.

Bajty FMT, SID, DS_, TRTP a TREP jsou definovány dále v tomto dokumentu.

DDP_003 V případě, že data, která má zpráva nést, jsou delší než dostupný prostor v datovém poli, pošle se zpráva jako několik dílčích zpráv. Každá dílčí zpráva nese hlavičku, stejný bajt SID, bajt TREP a dvoubajtový čítač dílčích zpráv udávající pořadí dílčí zprávy v celkové zprávě. Aby byla možná kontrola chyb a přerušení přenosu, potvrzuje IDE každou dílčí zprávu. IDE může přijmout dílčí zprávu, požádat, aby byla přenesena znovu, požádat VU o opětovný start nebo přenos přerušit.

DDP_004 Jestliže poslední dílčí zpráva obsahuje v datovém poli přesně 255 bajtů, musí se připojit závěrečná dílčí zpráva s prázdným datovým polem (vyjma bajtů SID a TREP a čítače dílčích zpráv) jako indikátor konce zprávy.

Příklad:

Hlavička	SID	TREP	Zpráva	CS
4 bajty	Delší než 255 bajtů			

Přenese se jako:

Hlavička	SID	TREP	00	01	Dílčí zpráva 1	CS
4 bajty	255 bajtů					

Hlavička	SID	TREP	00	02	Dílčí zpráva 2	CS
4 bajty	255 bajtů					

…

Hlavička	SID	TREP	xx	yy	Dílčí zpráva n	CS
4 bajty	Méně než 255 bajtů					

nebo jako:

Hlavička	SID	TREP	00	01	Dílčí zpráva 1	CS
4 bajty	255 bajtů					

Hlavička	SID	TREP	00	02	Dílčí zpráva 2	CS
4 bajty	255 bajtů					

…

Hlavička	SID	TREP	xx	yy	Dílčí zpráva n	CS
4 bajty	255 bajtů					

Hlavička	SID	TREP	xx	yy + 1	CS
4 bajty	4 bajty				

2.2.2 *Typy zpráv*

Komunikační protokol mezi VU a IDE pro stahování dat vyžaduje výměnu osmi různých typů zpráv.

Následující tabulka uvádí přehled těchto zpráv.

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

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
Transfer Data Request								
Overview	80	EE	F0	02	36	01		97
Activities	80	EE	F0	06	36	02	Date	CS
Events & Faults	80	EE	F0	02	36	03		99
Detailed Speed	80	EE	F0	02	36	04		9A
Technical Data	80	EE	F0	02	36	05		9B
Card download	80	EE	F0	02	36	06	Slot	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

Poznámky:

— Sid Req = SID odpovídajícího požadavku.

— TREP = TRTP odpovídajícího požadavku.

— Tmavé buňky znamenají, že se nic nepřenáší.

— Termín „odeslání dat“ (*„upload“*, z pohledu IDE) se používá z důvodu slučitelnosti s ISO 14229. Znamená totéž jako stahování dat (*„download“*, z pohledu VU).

— Případné 2bajtové čítače dílčích zpráv nejsou v tabulce uvedeny.

— Slot je číslo otvoru pro kartu, buď „1“ (karta v otvoru pro kartu řidiče), nebo „2“ (karta v otvoru pro kartu druhého řidiče).

— Není-li otvor specifikován, VU vybere otvor č. 1, pokud je v něm vložena karta, a otvor č. 2 vybere jen v případě, že jej explicitně vybere uživatel.

2.2.2.1 Start Communication Request (SID 81)

DDP_005 Tuto zprávu vyšle zařízení IDE, aby navázalo spojení s VU. Počáteční komunikace vždy probíhá rychlostí 9 600 baudů (až do případné změny rychlosti přenosu dat příslušnými zprávami *Link Control Service*).

2.2.2.2 Positive Response Start Communication (SID C1)

DDP_006 Tuto zprávu vyšle VU jako kladnou odpověď na požadavek *Start Communication Request*. Zpráva obsahuje 2 klíčové bajty „EA“ „8F“ udávající, že VU podporuje protokol s hlavičkou zahrnující informace o zdroji, cíli a délce.

2.2.2.3 Start Diagnostic Session Request (SID 10)

DDP_007 Zprávu *Start Diagnostic Session Request* vyšle IDE jako žádost o novou diagnostickou relaci s VU. Podfunkce „*default session*“ (81 hex) udává, že se má otevřít standardní diagnostická relace.

2.2.2.4 Positive Response Start Diagnostic (SID 50)

DDP_008 Zprávu *Positive Response Start Diagnostic* posílá VU jako kladnou odpověď na požadavek *Start Diagnostic Session Request*.

2.2.2.5 Link Control Service (SID 87)

DDP_052 Zprávu *Link Control Service* používá IDE k vyvolání změny rychlosti přenosu dat. Změna probíhá ve dvou krocích. V prvním kroku IDE navrhne změnu rychlosti přenosu dat, včetně nové rychlosti. Po přijetí kladné zprávy od VU pak IDE odešle VU potvrzení o změně rychlosti přenosu dat (druhý krok). IDE pak přejde na novou rychlost přenosu dat. Po obdržení potvrzení přejde VU na novou rychlost přenosu dat.

2.2.2.6 Link Control Positive Response (SID C7)

DDP_053 Zprávu *Link Control Positive Response* vyšle VU jako kladnou odpověď na požadavek *Link Control Service* (první krok). Je třeba poznamenat, že na potvrzující požadavek (druhý krok) se nezasílá žádná odpověď.

2.2.2.7 Request Upload (SID 35)

DDP_009 Vysláním zprávy *Request Upload* IDE informuje VU, že je požadováno stahování. Pro splnění požadavků ISO 14229 jsou obsaženy údaje o adrese, velikosti a podrobnostech o formátu požadovaných dat. Vzhledem k tomu, že IDE tyto údaje před stahováním nezná, nastaví se adresa v paměti na 0, formát je nešifrovaný a nekomprimovaný a velikost paměti se nastaví na maximum.

2.2.2.8 Positive Response Request Upload (SID 75)

DDP_010 Zprávu *Positive Response Request Upload* odesílá VU, aby sdělil IDE, že VU je připraven na stahování dat. Pro splnění požadavků ISO 14229 jsou ve zprávě s pozitivní odpovědí obsaženy údaje, které IDE sdělují, že další zprávy *Positive Response Transfer Data* budou obsahovat maximálně 00FF hex bajtů.

2.2.2.9 Transfer Data Request (SID 36)

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:

— přehled (*Overview*, TRTP 01),

— činnosti v daný den (*Activities of a specified date*, TRTP 02),

— události a chyby (*Events and faults*, TRTP 03),

— podrobnosti o rychlosti (*Detailed speed*, TRTP 04),

— technická data (*Technical data*, TRTP 05),

— stažení dat z karty (*Card download*, TRTP 06).

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

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

2.2.2.10 Positive Response Transfer Data (SID 76)

DDP_012 Zprávu *Positive Response Transfer Data* posílá VU jako odpověď na zprávu *Transfer Data Request*. Zpráva obsahuje požadovaná data s parametrem TREP odpovídajícím parametru TRTP požadavku.

DDP055 V prvním případě (TREP 01) 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 stáhnout data (data VU),

— indikace přítomnosti karet ve VU,

— předešlé stažení dat podnikem,

— zámky podniku,

— předešlé kontroly.

2.2.2.11 Request Transfer Exit (SID 37)

DDP_013 Zprávu *Request Transfer Exit* posílá IDE, aby informovalo VU, že relace stahování je ukončena.

2.2.2.12 Positive Response Request Transfer Exit (SID 77)

DDP_014 Zprávu *Positive Response Request Transfer Exit* posílá VU, aby potvrdil přijetí požadavku *Request Transfer Exit*.

2.2.2.13 Stop Communication Request (SID 82)

DDP_015 Zprávu *Stop Communication Request* zasílá IDE, aby přerušilo komunikační spojení s VU.

2.2.2.14 Positive Response Stop Communication (SID C2)

DDP_016 Zprávu *Positive Response Stop Communication* zasílá VU, aby potvrdil přijetí požadavku *Stop Communication Request*.

2.2.2.15 Acknowledge Sub Message (SID 83)

DDP_017 Zprávu *Acknowledge Sub Message* zasílá IDE jako potvrzení o přijetí jednotlivých částí zprávy, která se přenáší jako několik dílčích zpráv. Datové pole obsahuje SID obdržený od VU a následující dvoubajtový kód:

— MsgC + 1 potvrzuje správné přijetí dílčí zprávy s číslem MsgC.

IDE požaduje od VU odeslání další dílčí zprávy.

— MsgC označuje problém při příjmu dílčí zprávy s číslem MsgC.

IDE požaduje od VU opakované odeslání dílčí zprávy.

— FFFF požaduje ukončení zprávy.

Tento kód může IDE použít k ukončení přenosu zprávy od VU z jakéhokoli důvodu.

Poslední dílčí zpráva celkové zprávy (bajt LEN < 255) může být potvrzena kterýmkoli z těchto kódů, nebo nepotvrzena.

Odpovědi VU, které se budou skládat z několika dílčích zpráv, jsou:

— *Positive Response Transfer Data* (SID 76)

2.2.2.16 Negative Response (SID 7F)

DDP_018 Zprávu *Negative Response* zasílá VU jako odpověď na výše uvedené zprávy požadavků, pokud VU nemůže požadavek splnit. Datové pole zprávy obsahuje SID odpovědi (7F), SID požadavku a kód, který upřesňuje důvod negativní odpovědi. K dispozici jsou následující kódy:

— 10 *General reject* (obecné odmítnutí)

Akci nelze provést z důvodů níže neuvedených.

— 11 *Service not supported* (služba nepodporována)

SID požadavku není srozumitelný.

— 12 *Sub function not supported* (podfunkce nepodporována)

Bajt DS_ nebo TRTP požadavku není srozumitelný, nebo není třeba přenést žádné další dílčí zprávy.

— 13 *Incorrect message length* (chybná délka zprávy)

Délka přijaté zprávy je chybná.

— 22 *Conditions not correct or Request sequence error* (nesprávné podmínky nebo chybná posloupnost požadavků)

Požadovaná služba není aktivní nebo je chybná posloupnost zpráv s požadavky.

— 31 *Request out of range* (požadavek mimo rozsah)

Záznam s parametry požadavku (datové pole) je neplatný.

— 50 *Upload not accepted* (odeslání neakceptováno)

Požadavek nelze provést (VU není v příslušném provozním režimu nebo došlo k interní závadě VU).

— 78 *Response pending* (odpověď se připravuje)

Požadovanou akci nelze včas dokončit a VU není připraven přijmout další požadavek.

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

Datový objekt požadavku na přenos dat není ve VU k dispozici (např. není vložená žádná karta atd.).

2.2.3 *Tok zpráv*

Typický tok zpráv během normálního postupu stahování dat je následující:

IDE		VU
Start Communication Request	⇨ ⇦	Positive Response
Start Diagnostic Service Request	⇨ ⇦	Positive Response
Request Upload	⇨ ⇦	Positive Response

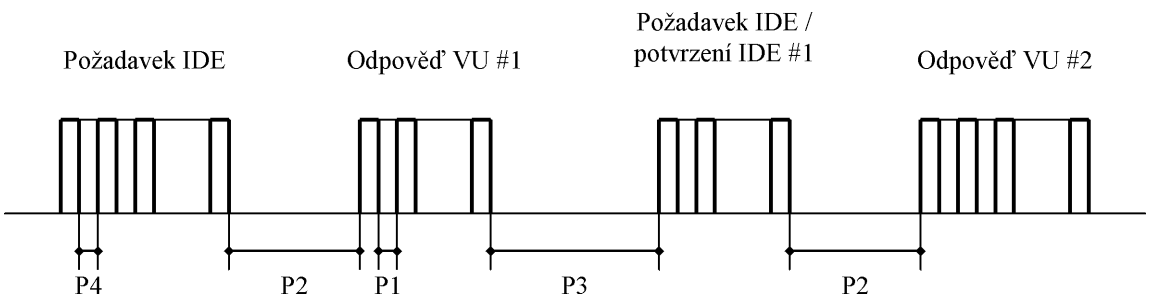
IDE		VU
Transfer Data Request Overview	⇨	
	⇦	Positive Response
Transfer Data Request #2	⇨	
	⇦	Positive Response #1
Acknowledge Sub Message #1	⇨	
	⇦	Positive Response #2
Acknowledge Sub Message #2	⇨	
	⇦	Positive Response #m
Acknowledge Sub Message #m	⇨	
	⇦	Positive Response (datové pole < 255 bajtů)
Acknowledge Sub Message (nepovinná)	⇨	
…		
Transfer Data Request #n	⇨	
	⇦	Positive Response
Request Transfer Exit	⇨	
	⇦	Positive Response
Stop Communication Request	⇨	
	⇦	Positive Response

2.2.4 *Časování*

DDP_019 Při normální činnosti platí parametry časování uvedené na následujícím obrázku:

Obrázek 1

Časování toku zpráv



kde:

P1 = prodleva mezi bajty v odpovědi VU

P2 = prodleva mezi koncem požadavku IDE a začátkem odpovědi VU nebo mezi koncem potvrzení ze strany IDE a začátkem následující odpovědi VU

P3 = prodleva mezi koncem odpovědi VU a začátkem nového požadavku IDE nebo mezi koncem odpovědi VU a začátkem potvrzení ze strany IDE nebo mezi koncem požadavku IDE a začátkem nového požadavku IDE, pokud VU neodpoví

P4 = prodleva mezi bajty v požadavku IDE

P5 = prodloužená hodnota P3 pro stahování z karty

Přípustné hodnoty parametrů časování jsou uvedeny v následující tabulce (rozšířený soubor parametrů časování protokolu KWP používaný v případě fyzického adresování k urychlení komunikace).

Parametr časování	Spodní mezní hodnota (ms)	Horní mezní hodnota (ms)
P1	0	20
P2	20	1 000 (*)
P3	10	5 000
P4	5	20
P5	10	20 minut

(*) Pokud VU odpoví zprávou *Negative Response* obsahující kód s významem „požadavek správně přijat, odpověď se připravuje“, prodlužuje se tato hodnota na horní mezní hodnotu parametru P3.

2.2.5 *Zpracování chyb*

Pokud při výměně zpráv dojde k chybě, schéma toku zpráv se změní v závislosti na tom, které zařízení chybu zjistilo a která zpráva chybu vyvolala.

Na obrázku 2 a 3 jsou znázorněny postupy zpracování chyb pro VU a pro IDE.

2.2.5.1 Fáze zahájení komunikace

DDP_020 Pokud IDE zjistí chybu ve fázi zahájení komunikace, ať už z časování, nebo z bitového toku, před zopakováním požadavku vyčká po dobu P3min.

DDP_021 Pokud VU zjistí chybu v posloupnosti přicházející z IDE, neodešle žádnou odpověď a počká na další zprávu *Start Communication Request* po dobu P3max.

2.2.5.2 Fáze komunikace

Je možné definovat dvě různé oblasti zpracování chyb:

1. **VU zjistí chybu v přenosu z IDE**

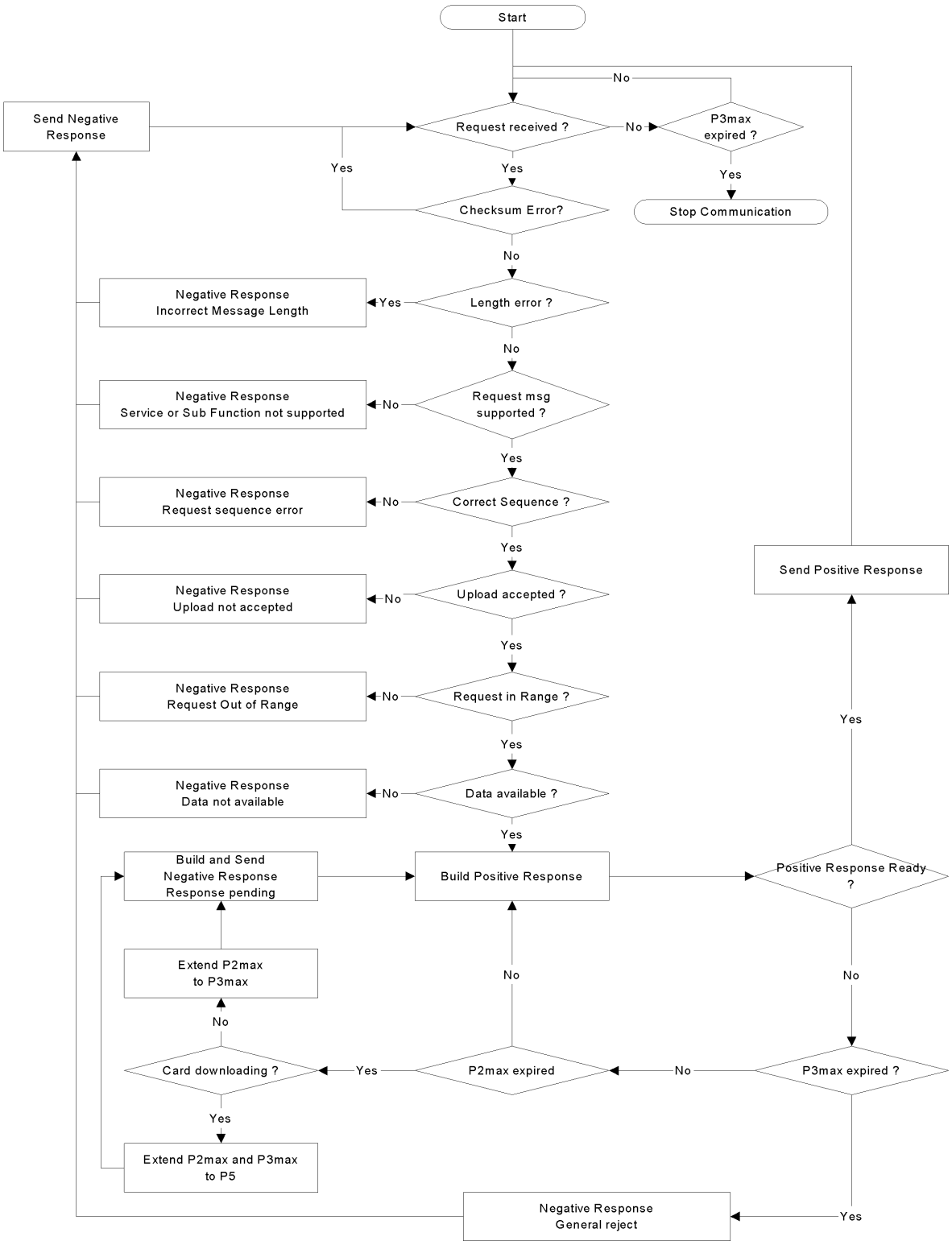
DDP_022 VU u každé přijaté zprávy detekuje chyby v časování, chyby ve formátu bajtů (např. porušení start a stop bitu) a chyby rámce (chybný počet přijatých bajtů, chybný bajt kontrolního součtu).

DDP_023 Pokud VU zjistí jednu z výše uvedených chyb, neposílá žádnou odpověď a obdrženou zprávu ignoruje.

DDP_024 VU může detekovat další chyby ve formátu nebo obsahu obdržené zprávy (např. nepodporovaná zpráva), i když zpráva splňuje požadavky na délku a kontrolní součet; v takovém případě VU odešle IDE odpověď *Negative Response* specifikující povahu chyby.

Obrázek 2

Zpracování chyb na straně VU



2. **IDE zjistí chybu v přenosu z VU**

DDP_025 IDE u každé přijaté zprávy detekuje chyby časování, chyby ve formátu bajtů (např. porušení start a stop bitu) a chyby rámce (chybný počet přijatých bajtů, chybný bajt kontrolního součtu).

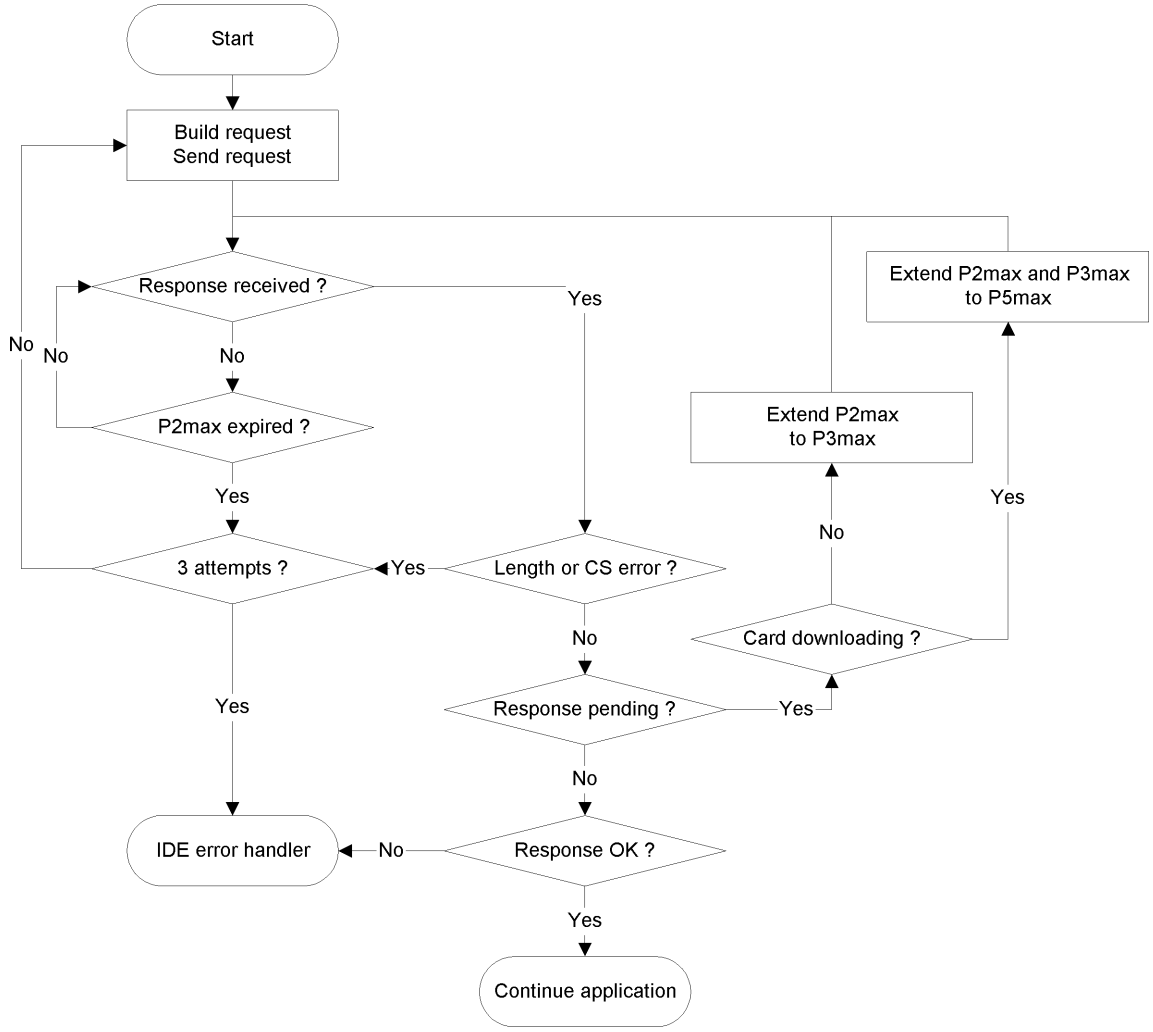
DDP_026 IDE detekuje chyby v posloupnosti, např. chybné zvyšování čítače dílčích zpráv ve zprávách přijatých za sebou.

DDP_027 Pokud IDE zjistí chybu nebo neobdrží odpověď od VU v době do P2max, pošle zprávu s požadavkem znovu. Celkem ji přenese nejvýše třikrát. Pro účely této detekce chyb se potvrzení dílčí zprávy považuje za požadavek na VU.

DDP_028 IDE před zahájením každého přenosu vyčká nejméně po dobu P3min. Čekací doba se měří od posledního vypočteného výskytu stop bitu po zjištění chyby.

Obrázek 3

Zpracování chyb na straně IDE



2.2.6 *Obsah zprávy s odpovědí*

Tento odstavec specifikuje obsah datových polí různých zpráv s kladnou odpovědí.

Datové prvky jsou definovány v datovém slovníku v dodatku 1.

Poznámka: Při stahování dat 2. generace je každý datový prvek nejvyšší úrovně reprezentován polem záznamů, i když obsahuje pouze jeden záznam. Pole záznamů začíná hlavičkou; tato hlavička obsahuje typ záznamu, velikost záznamu a počet záznamů. Pole záznamů jsou v následujících tabulkách nazvána „… RecordArray“ (s hlavičkou).

2.2.6.1 Positive Response Transfer Data Overview

DDP_029 Datové pole zprávy *Positive Response Transfer Data Overview* musí obsahovat následující data v uvedeném pořadí, přičemž se použije SID 76 hex, TREP 01 hex a patřičné rozdělení do dílčích zpráv a jejich počítání:

Datová struktura 1. generace

Datový prvek	Poznámka
MemberStateCertificate VUCertificate	Bezpečnostní certifikáty VU
VehicleIdentificationNumber VehicleRegistrationIdentification	Identifikace vozidla
CurrentDateTime	Aktuální datum a čas VU
VuDownloadablePeriod	Období, které lze stáhnout
CardSlotsStatus	Typy karet vložených do VU
VuDownloadActivityData	Předchozí stažení dat z VU
VuCompanyLocksData	Všechny uložené zámky podniku. Pokud je tato sekce prázdná, odešle se pouze noOfLocks = 0.
VuControlActivityData	Všechny záznamy o kontrole uložené ve VU. Pokud je tato sekce prázdná, odešle se pouze noOfControls = 0.
Signature	Podpis RSA všech dat (kromě certifikátů), počínaje VehicleIdentificationNumber a konče posledním bajtem posledního prvku VuControlActivityData.

Datová struktura 2. generace

Datový prvek	Poznámka
MemberStateCertificateRecordArray	Certifikát členského státu
VUCertificateRecordArray	Certifikát VU
VehicleIdentificationNumberRecordArray	Identifikace vozidla
VehicleRegistrationNumberRecordArray	Registrační značka vozidla
CurrentDateTimeRecordArray	Aktuální datum a čas VU
VuDownloadablePeriodRecordArray	Období, které lze stáhnout
CardSlotsStatusRecordArray	Typy karet vložených do VU
VuDownloadActivityDataRecordArray	Předchozí stažení dat z VU
VuCompanyLocksRecordArray	Všechny uložené zámky podniku. Pokud je tato sekce prázdná, odešle se hlavička pole s noOfRecords = 0.
VuControlActivityRecordArray	Všechny záznamy o kontrole uložené ve VU. Pokud je tato sekce prázdná, odešle se hlavička pole s noOfRecords = 0.
SignatureRecordArray	Podpis ECC všech předcházejících dat kromě certifikátů.

2.2.6.2 Positive Response Transfer Data Activities

DDP_030 Datové pole zprávy *Positive Response Transfer Data Activities* musí obsahovat následující data v uvedeném pořadí, přičemž se použije SID 76 hex, TREP 02 hex a patřičné rozdělení do dílčích zpráv a jejich počítání:

Datová struktura 1. generace

Datový prvek	Poznámka
TimeReal	Datum stahovaného dne
OdometerValueMidnight	Stav počitadla ujetých kilometrů na konci stahovaného dne
VuCardIWData	Data o cyklech vložení a vyjmutí karet. — Pokud tato sekce neobsahuje žádná dostupná data, odešle se pouze noOfVuCardIWRecords = 0. — Pokud prvek VuCardIWRecord přesahuje 00:00 (karta byla vložena předešlý den) nebo 24:00 (karta byla vyjmuta následující den), musí být celý obsažen v obou příslušných dnech.
VuActivityDailyData	Stav otvorů pro karty v 00:00 a změny činností zaznamenané pro stahovaný den.
VuPlaceDailyWorkPeriodData	Data týkající se míst zaznamenaná pro stahovaný den. Pokud je tato sekce prázdná, odešle se pouze noOfPlaceRecords = 0.
VuSpecificConditionData	Data týkající se zvláštních podmínek zaznamenaná pro stahovaný den. Pokud je tato sekce prázdná, odešle se pouze noOfSpecificConditionRecords=0.
Signature	Podpis RSA všech dat, počínaje prvkem TimeReal a konče posledním bajtem posledního záznamu zvláštních podmínek.

Datová struktura 2. generace

Datový prvek	Poznámka
DateOfDayDownloadedRecordArray	Datum stahovaného dne
OdometerValueMidnightRecordArray	Stav počitadla ujetých kilometrů na konci stahovaného dne
VuCardIWRecordArray	Data o cyklech vložení a vyjmutí karet. — Pokud tato sekce neobsahuje žádná dostupná data, odešle se hlavička pole s noOfRecords = 0. — Pokud prvek VuCardIWRecord přesahuje 00:00 (karta byla vložena předešlý den) nebo 24:00 (karta byla vyjmuta následující den), musí být celý obsažen v obou příslušných dnech.
VuActivityDailyRecordArray	Stav otvorů pro karty v 00:00 a změny činností zaznamenané pro stahovaný den.
VuPlaceDailyWorkPeriodRecordArray	Data týkající se míst zaznamenaná pro stahovaný den. Pokud je tato sekce prázdná, odešle se hlavička pole s noOfRecords = 0.
VuGNSSCDRecordArray	Polohy vozidla dle GNSS, pokud nepřetržitá doba řízení pro řidiče dosáhne násobku tří hodin. Pokud je tato sekce prázdná, odešle se hlavička pole s noOfRecords = 0.
VuSpecificConditionRecordArray	Data týkající se zvláštních podmínek zaznamenaná pro stahovaný den. Pokud je tato sekce prázdná, odešle se hlavička pole s noOfRecords = 0.
SignatureRecordArray	Podpis ECC všech předcházejících dat.

2.2.6.3 Positive Response Transfer Data Events and Faults

DDP_031 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 hex a patřičné rozdělení do dílčích zpráv a jejich počítání:

Datová struktura 1. generace

Datový prvek	Poznámka
VuFaultData	Všechny závady uložené nebo probíhající ve VU. Pokud je tato sekce prázdná, odešle se pouze noOfVuFaults = 0.
VuEventData	Všechny události (kromě překročení povolené rychlosti) uložené nebo probíhající ve VU. Pokud je tato sekce prázdná, odešle se pouze noOfVuEvents = 0.
VuOverSpeedingControlData	Data týkající se poslední kontroly překročení povolené rychlosti (výchozí hodnota, nejsou-li žádná data).
VuOverSpeedingEventData	Všechny události překročení povolené rychlosti uložené ve VU. Pokud je tato sekce prázdná, odešle se pouze noOfVuOverSpeedingEvents = 0.
VuTimeAdjustmentData	Všechny události nastavení času uložené ve VU (mimo rámec úplné kalibrace). Pokud je tato sekce prázdná, odešle se pouze noOfVuTimeAdjRecords = 0.
Signature	Podpis RSA všech dat, počínaje prvkem noOfVuFaults a konče posledním bajtem posledního záznamu o nastavení času.

Datová struktura 2. generace

Datový prvek	Poznámka
VuFaultRecordArray	Všechny závady uložené nebo probíhající ve VU. Pokud je tato sekce prázdná, odešle se hlavička pole s noOfRecords = 0.
VuEventRecordArray	Všechny události (kromě překročení povolené rychlosti) uložené nebo probíhající ve VU. Pokud je tato sekce prázdná, odešle se hlavička pole s noOfRecords = 0.
VuOverSpeedingControlDataRecordArray	Data týkající se poslední kontroly překročení povolené rychlosti (výchozí hodnota, nejsou-li žádná data).
VuOverSpeedingEventRecordArray	Všechny události překročení povolené rychlosti uložené ve VU. Pokud je tato sekce prázdná, odešle se hlavička pole s noOfRecords = 0.
VuTimeAdjustmentRecordArray	Všechny události nastavení času uložené ve VU (mimo rámec úplné kalibrace). Pokud je tato sekce prázdná, odešle se hlavička pole s noOfRecords = 0.
VuTimeAdjustmentGNSSRecordArray	
SignatureRecordArray	Podpis ECC všech předcházejících dat.

2.2.6.4 Positive Response Transfer Data Detailed Speed

DDP_032 Datové pole zprávy *Positive Response Transfer Data Detailed Speed* musí obsahovat následující data v uvedeném pořadí, přičemž se použije SID 76 hex, TREP 04 hex a patřičné rozdělení do dílčích zpráv a jejich počítání:

Datová struktura 1. generace

Datový prvek	Poznámka
VuDetailedSpeedData	Všechny podrobnosti o rychlosti uložené ve VU (jeden blok rychlostí za minutu, během níž se vozidlo pohybovalo), 60 hodnot rychlosti za minutu (jedna za sekundu).
Signature	Podpis RSA všech dat, počínaje prvkem noOfSpeedBlocks a konče posledním bajtem posledního bloku rychlostí.

Datová struktura 2. generace

Datový prvek	Poznámka
VuDetailedSpeedBlockRecordArray	Všechny podrobnosti o rychlosti uložené ve VU (jeden blok rychlostí za minutu, během níž se vozidlo pohybovalo), 60 hodnot rychlosti za minutu (jedna za sekundu).
SignatureRecordArray	Podpis ECC všech předcházejících dat.

2.2.6.5 Positive Response Transfer Data Technical Data

DDP_033 Datové pole zprávy *Positive Response Transfer Data Technical Data* musí obsahovat následující data v uvedeném pořadí, přičemž se použije SID 76 hex, TREP 05 hex a patřičné rozdělení do dílčích zpráv a jejich počítání:

Datová struktura 1. generace

Datový prvek	Poznámka
VuIdentification	
SensorPaired	
VuCalibrationData	Všechny záznamy o kalibraci uložené ve VU.
Signature	Podpis RSA všech dat, počínaje prvkem vuManufacturerName a konče posledním bajtem posledního záznamu VuCalibrationRecord.

Datová struktura 2. generace

Datový prvek	Poznámka
VuIdentificationRecordArray	
VuSensorPairedRecordArray	Všechna párování snímačů pohybu uložená ve VU.
VuSensorExternalGNSSCoupledRecordArray	Všechny vazby s vnějšími zařízeními GNSS uložené ve VU.
VuCalibrationRecordArray	Všechny záznamy o kalibraci uložené ve VU.
VuCardRecordArray	Všechna data o vložení karty uložená ve VU.
VuITSConsentRecordArray	
VuPowerSupplyInterruptionRecordArray	
SignatureRecordArray	Podpis ECC všech předcházejících dat.

2.3 **Ukládání souborů na externí paměťové médium**

DDP_034 Pokud byl součástí relace stahování přenos dat z VU, IDE uloží do jednoho fyzického souboru všechna data přijatá z VU během relace stahování ve zprávách *Positive Response Transfer Data*. Uložená data nezahrnují hlavičky zpráv, čítače dílčích zpráv, prázdné dílčí zprávy a kontrolní součty, ale zahrnují SID a TREP (jen první dílčí zprávy, pokud je dílčích zpráv více).

3. PROTOKOL PRO STAHOVÁNÍ DAT Z KARET TACHOGRAFU

3.1 **Oblast působnosti**

Tento odstavec popisuje přímé stahování dat z karty tachografu do IDE. IDE není součástí bezpečnostního prostředí, neprobíhá proto ověření pravosti mezi kartou a IDE.

3.2 **Definice**

Relace stahování: Každé stahování dat z čipové karty (ICC). Relace zahrnuje celý postup od resetování ICC zařízením IFD až po deaktivaci ICC (vyjmutí karty nebo další reset).

Podepsaný datový soubor: Soubor z ICC. Soubor se přenáší do IFD jako otevřený text. V ICC se vypočte hash souboru, soubor se podepíše a podpis se přenese do IFD.

3.3 **Stahování z karty**

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.

— Stažení EF Card_Certificate (nebo CardSignCertificate) 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 a v příslušných případech Tachograph_G2 DF), kromě EF Card_Download. Tyto informace jsou zabezpečeny digitálním podpisem.

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

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

- Events_Data,
- Faults_Data,
- Driver_Activity_Data,
- Vehicles_Used,
- Places,
- GNSS_Places (v příslušných případech),
- Control_Activity_Data,
- Specific_Conditions.

— Při stahování z karty řidiče se aktualizuje datum LastCardDownload v EF Card_Download.

— Při stahování z karty dílny se vynuluje počítadlo kalibrací v EF Card_Download.

— Při stahování z karty dílny se nestahuje EF Sensor_Installation_Data.

3.3.1 *Inicializační sekvence*

DDP_036 IDE zahájí sekvenci takto:

Karta	Směr	IDE/IFD	Význam/poznámky
	⇦	Hardwarový reset	
ATR	⇨		

Nepovinně lze pomocí PPS přepnout na vyšší rychlost přenosu dat, pokud ji ICC podporuje.

3.3.2 *Sekvence pro nepodepsané datové soubory*

DDP_037 Sekvence stahování EF ICC, IC, Card_Certificate (nebo CardSignCertificate) a CA_Certificate je následující:

Karta	Směr	IDE/IFD	Význam/poznámky
	⇦	**Select File**	Výběr podle identifikátorů souboru
OK	⇨		
	⇦	**Read Binary**	Pokud soubor obsahuje více dat, než je velikost vyrovnávací paměti čtečky nebo karty, je třeba příkaz opakovat, dokud není přečten celý soubor.
Data souboru **OK**	⇨	Uložení dat na ESM	Podle bodu **3.4** Formát uložených dat

Poznámka 1: Před vybráním EF Card_Certificate (nebo CardSignCertificate) musí být vybrána aplikace tachografu (výběr podle AID).

Poznámka 2: Výběr a čtení souboru lze rovněž provést v jednom kroku pomocí příkazu *Read Binary* s krátkým identifikátorem EF.

3.3.3 *Sekvence pro podepsané datové soubory*

DDP_038 Pro každý z následujících souborů, které je třeba stáhnout s podpisem, se použije tato sekvence:

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. 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** Formát uložených dat
	⇦	**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** Formát uložených dat

Poznámka: Výběr a čtení souboru lze rovněž provést v jednom kroku pomocí příkazu *Read Binary* s krátkým identifikátorem EF. V takovém případě lze EF vybrat a přečíst před použitím příkazu *Perform Hash of File*.

3.3.4 *Sekvence pro reset počítadla kalibrací*

DDP_039 Sekvence pro reset počítadla `NoOfCalibrationsSinceDownload` v EF `Card_Download` na kartě dílny je následující:

Karta	Směr	IDE/IFD	Význam/poznámky
	⇦	**Select File** EF Card_Download	Výběr podle identifikátorů souboru
OK	⇨		

Karta	Směr	IDE/IFD	Význam/poznámky
	⇦	**Update Binary** NoOfCalibrationsSince-Download = '00 00'	
reset počtu stažení z karty			
OK	⇨		

Poznámka: Výběr a aktualizaci souboru lze rovněž provést v jednom kroku pomocí příkazu *Update Binary* s krátkým identifikátorem EF.

3.4 **Formát uložených dat**

3.4.1 *Úvod*

DDP_040 Stažená data musí být uložena za těchto podmínek:

— Data se ukládají transparentně. To znamená, že při uložení musí být zachováno pořadí bajtů přenesených z karty, jakož i pořadí bitů uvnitř bajtů.

— Všechny soubory karty stažené během relace stahování jsou v ESM uloženy v jednom souboru.

3.4.2 *Formát souboru*

DDP_041 Soubor má formát zřetězení několika objektů TLV.

DDP_042 Tag elementárního souboru je FID plus přípona „00".

DDP_043 Tag podpisu elementárního souboru je FID souboru plus přípona „01".

DDP_044 Délka je dvoubajtová hodnota. Její hodnota určuje počet bajtů v poli s hodnotou. Hodnota „FF FF" v poli délky je vyhrazena pro budoucí použití.

DDP_045 Jestliže se nějaký soubor nestahuje, neukládá se nic, co s tímto souborem souvisí (žádný tag ani nulová délka).

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)	3 bajty
FID (2 bajty) || „01"	Tag pro podpis EF(FID)	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
05 05 01	00 80	Podpis EF Vehicles_Used

4. STAHOVÁNÍ Z KARTY TACHOGRAFU PŘES JEDNOTKU VE VOZIDLE

DDP_047 VU musí umožnit stažení obsahu vložené karty řidiče do připojeného IDE.

DDP_048 IDE tento režim zahájí zasláním zprávy *Transfer Data Request Card Download* do VU (viz bod 2.2.2.9)

DDP_049 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*.

DDP_050 IDE načte data z karty ze zprávy *Positive Response Transfer Data* (přičemž odstraní všechny hlavičky, bajty SID a TREP, čítače dílčích zpráv a kontrolní součty) a uloží je do jednoho fyzického souboru, jak popisuje odstavec 2.3.

DDP_051 VU poté v příslušných případech aktualizuje soubor `Control_Activity_Data` nebo soubor `Card_Download` na kartě řidiče.

Dodatek 8.

KALIBRAČNÍ PROTOKOL

OBSAH

1. ÚVOD

Tento dodatek popisuje, jak se vyměňují data mezi celkem ve vozidle (VU) a zkušebním zařízením po vodiči K, který tvoří část kalibračního rozhraní popsaného v dodatku 6. Popisuje také řízení signálového vodiče vstup/výstup (I/O) na kalibračním konektoru.

Navázání komunikace po vodiči K je popsáno v části 4 „Komunikační služby".

Tento dodatek používá koncepci diagnostických „relací" k tomu, aby stanovil rozsah řízení vodičem K za různých podmínek. Výchozí relací je „StandardDiagnosticSession" (standardní diagnostická relace), kdy mohou být veškerá data z celku ve vozidle čtena, ale žádná data nemohou být do celku ve vozidle zapisována.

Volba diagnostické relace je popsána v části 5 „Řídící služby".

Tento dodatek je třeba, v souladu s požadavky na interoperabilitu stanovenými v tomto nařízení, považovat za relevantní pro obě generace celků ve vozidle a karet dílny.

CPR_001 Relace „ECUProgrammingSession" (programovací relace ECU) umožňuje zadávání dat do celku ve vozidle. V případě zadávání kalibračních dat musí být celek ve vozidle navíc v pracovním režimu kalibrace (CALIBRATION).

Přenos dat po vodiči K je popsán v části 6 „Služby přenosu dat". Formáty přenášených dat jsou podrobně uvedeny v části 8 „Formáty dataRecords".

CPR_002 Relace „ECUAdjustmentSession" (seřizovací relace ECU) umožňuje volbu režimu I/O (vstup/výstup) na kalibračním signálovém vodiči I/O přes rozhraní vodiče K. Řízení kalibračního signálového vodiče I / O je popsáno v části 7 „Řízení zkušebních impulsů – Řízení funkčního celku vstup/výstup".

CPR_003 V tomto dokumentu je adresa zkušebního zařízení označována jako 'tt'. I když mohou existovat preferované adresy zkušebních zařízení, celek ve vozidle musí správně reagovat na kteroukoli adresu zkušebního zařízení. Fyzická adresa celku ve vozidle je 0xEE.

2. POJMY, DEFINICE A ODKAZY

Protokoly, zprávy a chybové kódy v podstatě vycházejí z návrhu normy ISO 14229-1 Road vehicles – Diagnostic systems – Part 1: Diagnostic services, version 6 (Silniční vozidla — Diagnostické systémy — Část 1: Diagnostické služby, verze 6 ze dne 22. února 2001).

Pro identifikátory služeb, požadavky na služby, odpovědi a pro standardní parametry se užívá bajtové kódování a hexadecimální hodnoty.

Pojem „zkušební zařízení" se vztahuje na zařízení používané pro zadávání programovacích nebo kalibračních dat do celku ve vozidle.

Pojem „klient" se vztahuje na zkušební zařízení a pojem „server" na celek ve vozidle.

Zkratka ECU znamená „elektronický řídící celek" (*Electronic Control Unit*) a vztahuje se na celek ve vozidle.

Odkazy:

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.)

Vozidla – Diagnostika.

3. PŘEHLED SLUŽEB

3.1. **Dostupné služby**

Dále uvedená tabulka podává přehled služeb, které budou dostupné v tachografu a které jsou v tomto dokumentu definovány.

CPR_004 Tabulka uvádí služby dostupné v povolené diagnostické relaci.

— **Prvý sloupec** uvádí seznam dostupných služeb.

— **Druhý sloupec** obsahuje číslo části v tomto dodatku, ve kterém je daná služba dále definována.

— **Třetí sloupec** přiděluje zprávám se žádostí hodnoty identifikátorů služeb.

— **Čtvrtý sloupec** specifikuje služby **„StandardDiagnosticSession" (SD)** (standardní diagnostická relace), které musí být implementovány v každém celku ve vozidle.

— **Pátý sloupec** specifikuje služby **„ECUAdjustmentSession" (ECUAS)**, které musí být implementovány pro umožnění řízení signálového vodiče I/O z kalibračního konektoru na čelním panelu celku ve vozidle.

— **Šestý sloupec** specifikuje služby **„ECUProgrammingSession" (ECUPS)**, které musí být implementovány pro umožnění programování parametrů v celku ve vozidle.

Tabulka 1

Souhrnná tabulka hodnot identifikátorů (Id) služeb

			Diagnostické relace		
Název diagnostické služby	Číslo části	Požadovaná hodnota identifikátoru služby	SD	ECUAS	ECUPS
StartCommunication	4.1	81	■	■	■
StopCommunication	4.2	82	■		
TesterPresent	4.3	3E	■	■	■
StartDiagnosticSession	5.1	10	■	■	■
SecurityAccess	5.2	27	■	■	■
ReadDataByIdentifier	6.1	22	■	■	■
WriteDataByIdentifier	6.2	2E			■
InputOutputControlByIdentifier	7.1	2F		■	

■ Tento symbol značí, že služba je v této diagnostické relaci povinná.

Pokud není symbol uveden, znamená to, že tato služba není v této diagnostické relaci povolena.

3.2. **Kódy odpovědí**

Kódy odpovědí jsou definovány pro každou službu.

4. KOMUNIKAČNÍ SLUŽBY

Některé služby jsou potřebné k navázání a udržování komunikace. Neobjevují se na aplikační vrstvě. Tyto dostupné služby jsou rozepsány v následující tabulce:

Tabulka 2

Komunikační služby

Název služby	Popis
StartCommunication	Klient požaduje zahájení komunikační relace se serverem (servery).
StopCommunication	Klient požaduje ukončení probíhající komunikační relace.
TesterPresent	Klient oznamuje serveru, že je stále připojen.

CPR_005 Služba StartCommunication se užívá pro zahájení komunikace. Pro navedení jakékoliv služby musí být komunikace inicializována a komunikační parametry musí odpovídat požadovanému režimu.

4.1. **Služba StartCommunication (zahájení komunikace)**

CPR_006 Po obdržení indikačního prvku StartCommunication musí celek ve vozidle ověřit, zda může být požadované komunikační spojení za současných podmínek inicializováno. Platné podmínky pro inicializaci komunikačního spojení jsou popsány v dokumentu ISO 14230-2.

CPR_007 Pak musí celek ve vozidle provést veškeré kroky potřebné pro inicializaci komunikačního spojení a musí odeslat prvek s odpovědí na StartCommunication společně se zvolenými parametry kladné odpovědi.

CPR_008 Pokud celek ve vozidle, který byl již inicializován (a který vstoupil do jakékoli diagnostické relace), obdrží nový požadavek StartCommunication (například v důsledku zotavení z chyb ve zkušebním zařízení), musí být požadavek přijat a celek ve vozidle musí být znovu inicializován.

CPR_009 Pokud nemůže být z jakéhokoliv důvodu komunikační spojení inicializováno, musí celek ve vozidle pokračovat v činnosti, kterou provozoval bezprostředně před pokusem o inicializaci komunikačního spojení.

CPR_010 Zpráva s požadavkem StartCommunication musí být fyzicky adresována.

CPR_011 Inicializace celku ve vozidle proběhne postupem „rychlé inicializace“.

— Každé činnosti předchází klidová doba sběrnice,

— Zkušební zařízení pak vyšle inicializační sekvenci.

— Veškeré informace, které jsou potřebné pro zahájení komunikace, jsou obsaženy v odpovědi celku ve vozidle.

CPR_012 Po dokončení inicializace:

— se veškeré komunikační parametry nastaví podle klíčových bajtů na hodnoty definované v tabulce 4,

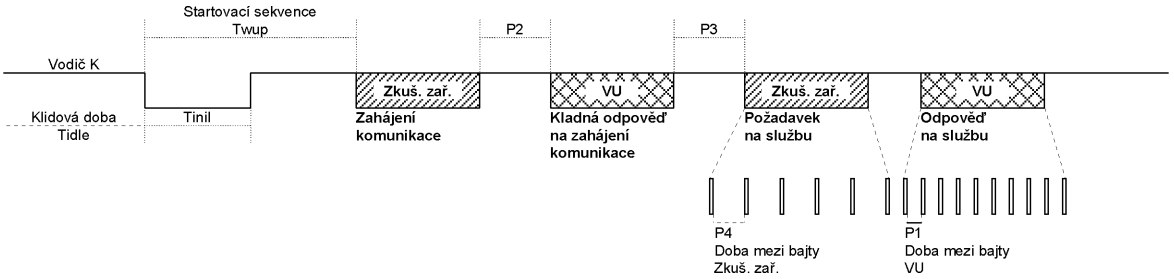
— celek ve vozidle vyčkává na první požadavek zkušebního zařízení,

— celek ve vozidle je ve výchozím diagnostickém režimu, tj. StandardDiagnosticSession,

— kalibrační signálový vodič I/O je ve výchozím stavu, tj. v neaktivním stavu.

CPR_014 Rychlost přenosu dat na vodiči K musí být 10 400 baudů.

CPR_016 Rychlá inicializace je zahájena zkušebním zařízením, které vysílá startovací sekvenci (Wup) po vodiči K. Sekvence začíná po klidové době na vodiči K nízkou úrovní po dobu Tinil. Zkušební zařízení vyšle prvý bit ze StartCommunicationService následně po době Twup po první sestupné hraně.



CPR_017 Hodnoty časování pro rychlou inicializaci a komunikaci jsou obecně rozepsány v níže uvedených tabulkách. Existují různé možnosti pro dobu klidu (*idle time*):

— První přenos po zapnutí napájení, Tidle = 300 ms.

— Po dokončení služby StopCommunication Tidle = P3 min.

— Po ukončení komunikace v důsledku překročení doby P3max, Tidle = 0.

Tabulka 3

Hodnoty časování pro rychlou inicializaci

Parametr		Minimální hodnota	Maximální hodnota
Tinil	25 ± 1 ms	24 ms	26 ms
Twup	50 ± 1 ms	49 ms	51 ms

Tabulka 4

Hodnoty časování pro komunikaci

Parametr časování	Popis parametru	Dolní mezní hodnoty (ms)	Horní mezní hodnoty (ms)
		min.	max.
P1	Doba mezi bajty pro odpověď celku ve vozidle	0	20
P2	Doba mezi požadavkem zkušebního zařízení a odpovědí celku ve vozidle nebo mezi dvěma odpověďmi celku ve vozidle	25	250
P3	Doba mezi koncem odpovědi celku ve vozidle a začátkem nového požadavku zkušebního zařízení	55	5 000
P4	Doba mezi bajty pro požadavek zkušebního zařízení	5	20

CPR_018 Formáty zprávy pro rychlou inicializaci jsou rozepsány v níže uvedených tabulkách: (POZNÁMKA: Hex znamená hexadecimální)

Tabulka 5

zpráva se žádostí StartCommunication

Bajt č.	Název parametru	Hexadecimální hodnota	Symbol
#1	Bajt formátu — fyzické adresování	81	FMT
#2	Bajt adresy cíle	EE	TGT
#3	Bajt adresy zdroje	tt	SRC
#4	**Id služby požadavku StartCommunication**	**81**	**SCR**
#5	Kontrolní součet	00-FF	CS

Tabulka 6

zpráva s kladnou odpovědí na StartCommunication

Bajt č.	Název parametru	Hexadecimální hodnota	Symbol
#1	Bajt formátu — fyzické adresování	80	FMT
#2	Bajt cílové adresy	tt	TGT
#3	Bajt adresy zdroje	EE	SRC
#4	Dodatečný bajt délky	03	LEN
#5	**Id služby kladné odpovědi na StartCommunication**	**C1**	**SCRPR**
#6	Klíčový bajt 1	EA	KB1
#7	Klíčový bajt 2	8F	KB2
#8	Kontrolní součet	00-FF	CS

CPR_019 Na zprávu StartCommunication není záporná odpověď, pokud neexistuje zpráva s kladnou odpovědí, která má být přenesena, pak se celek ve vozidle neinicializuje, nic se nepřenáší a celek ve vozidle zůstává v normálním provozu.

4.2. **Služba StopCommunication (ukončení komunikace)**

4.2.1 *Popis zprávy*

Tato služba komunikační vrstvy slouží k ukončení komunikační relace.

CPR_020 Po obdržení indikačního prvku StopCommunication musí celek ve vozidle ověřit, zda existující podmínky umožňují tuto komunikaci ukončit. V tomto případě musí celek ve vozidle provést veškeré kroky potřebné k ukončení této komunikace.

CPR_021 Pokud je komunikaci možno ukončit, musí celek ve vozidle, dříve než je komunikace ukončena, vydat prvek odpovědi StopCommunication se zvolenými parametry kladné odpovědi.

CPR_022 Pokud nemůže být komunikace z jakéhokoliv důvodu ukončena, vydá celek ve vozidle prvek odpovědi na StopCommunication se zvoleným parametrem záporné odpovědi.

CPR_023 Pokud celek ve vozidle zjistí překročení času P3max, komunikace se ukončí bez vydání prvku odpovědi.

4.2.2 *Formát zprávy*

CPR_024 Formáty zpráv pro prvky StopCommunication jsou rozepsány v níže uvedených tabulkách.

Tabulka 7

zpráva se žádostí StopCommunication

Bajt č.	Název parametru	Hexadecimální hodnota	Symbol
#1	Formátový bajt — fyzické adresování	80	FMT
#2	Bajt cílové adresy	EE	TGT
#3	Bajt adresy zdroje	tt	SRC
#4	Bajt dodatečné délky	01	LEN
#5	**Id služby požadavku StopCommunication**	**82**	**SPR**
#6	Kontrolní součet	00-FF	CS

Tabulka 8

zpráva s kladnou odpovědí na StopCommunication

Bajt č.	Název parametru	Hexadecimální hodnota	Symbol
#1	Formátový bajt — fyzické adresování	80	FMT
#2	Bajt cílové adresy	tt	TGT
#3	Bajt adresy zdroje	EE	SRC
#4	Bajt dodatečné délky	01	LEN
#5	**Id služby kladné odpovědi na StopCommunication**	**C2**	**SPRPR**
#6	Kontrolní součet	00-FF	CS

Tabulka 9

zpráva se zápornou odpovědí na StopCommunication

Bajt č.	Název parametru	Hexadecimální hodnota	Symbol
#1	Formátový bajt — fyzické adresování	80	FMT
#2	Bajt cílové adresy	tt	TGT
#3	Bajt adresy zdroje	EE	SRC
#4	Bajt dodatečné délky	03	LEN
#5	**Id služby záporné odpovědi**	**7F**	**NR**
#6	Identifikace služby požadavku StopCommunication	82	SPR
#7	responseCode = generalReject	10	RC_GR
#8	Kontrolní součet	00-FF	CS

4.2.3 *Definice parametrů*

Tato služba nevyžaduje žádné definice parametrů

4.3. **Služba TesterPresent (zkušební zařízení připojeno)**

4.3.1 *Popis zprávy*

Pomocí služby TesterPresent zkušební zařízení indikuje serveru, že je stále připojeno, aby tak bylo serveru zabráněno v automatickém návratu do normálního provozu a případnému ukončení komunikace. Tato služba, která se vysílá pravidelně, udržuje diagnostickou relaci / komunikaci aktivní tím, že vždy po obdržení požadavku na tuto službu se resetuje časovač P3.

4.3.2 *Formát zprávy*

CPR_079 Formáty zpráv pro prvky TesterPresent jsou rozepsány v níže uvedených tabulkách.

Tabulka 10

zpráva se žádostí TesterPresent

Bajt č.	Název parametru	Hexadecimální hodnota	Symbol
#1	Formátový bajt — fyzické adresování	80	FMT
#2	Bajt cílové adresy	EE	TGT
#3	Bajt adresy zdroje	tt	SRC
#4	Bajt dodatečné délky	02	LEN
#5	**Id služby požadavku TesterPresent**	**3E**	**TP**

Bajt č.	Název parametru	Hexadecimální hodnota	Symbol
#6	Podfunkce = responseRequired = [ano	01	RESPREQ_Y
	ne]	02	RESPREQ_NO
#7	Kontrolní součet	00-FF	CS

CPR_080 Je-li parametr responseRequired nastaven na „ano“, odpoví server následující kladnou zprávou. Je-li nastaven na „ne“, neodešle server žádnou odpověď.

Tabulka 11

zpráva s kladnou odpovědí na TesterPresent

Bajt č.	Název parametru	Hexadecimální hodnota	Symbol
#1	Formátový bajt — fyzické adresování	80	FMT
#2	Bajt cílové adresy	tt	TGT
#3	Bajt adresy zdroje	EE	SRC
#4	Bajt dodatečné délky	01	LEN
#5	**Id služby kladné odpovědi na TesterPresent**	**7E**	**TPPR**
#6	Kontrolní součet	00-FF	CS

CPR_081 Služba podporuje následující kódy negativních odpovědí:

Tabulka 12

zpráva se zápornou odpovědí na TesterPresent

Bajt č.	Název parametru	Hexadecimální hodnota	Symbol
#1	Formátový bajt — fyzické adresování	80	FMT
#2	Bajt cílové adresy	tt	TGT
#3	Bajt adresy zdroje	EE	SRC
#4	Bajt dodatečné délky	03	LEN
#5	**Id služby záporné odpovědi**	**7F**	**NR**
#6	Identifikace služby požadavku TesterPresent	3E	TP

Bajt č.	Název parametru		Hexadecimální hodnota	Symbol
#7	responseCode =	[SubFunctionNotSupported-InvalidFormat	12	RC_SFNS_IF
		incorrectMessageLength]	13	RC_IML
#8	Kontrolní součet		00-FF	CS

5. ŘÍDÍCÍ SLUŽBY

Dostupné služby jsou rozepsány v následující tabulce:

Tabulka 13

Řídící služby

Název služby	Popis
StartDiagnosticSession	Klient požaduje zahájení diagnostické relace s celkem ve vozidle.
SecurityAccess	Klient požaduje přístup k funkcím vyhrazeným pro autorizované uživatele.

5.1. **Služba StartDiagnosticSession**

5.1.1 *Popis zprávy*

CPR_025 Služba StartDiagnosticSession se užívá pro povolení různých diagnostických relací na serveru. Diagnostická relace umožňuje specifický soubor služeb podle tabulky 17. Relace může povolit služby specifické pro výrobce vozidel, které nejsou součástí tohoto dokumentu. Pravidla implementace musí odpovídat těmto požadavkům:

— V celku ve vozidle musí být vždy aktivní jediná diagnostická relace.

— Vždy, když je celek ve vozidle připojen na napájení, musí zahájit StandardDiagnosticSession. Pokud není zahájena jiná diagnostická relace, pak StandardDiagnosticSession probíhá tak dlouho, dokud je celek ve vozidle napájen.

— Pokud je zkušebním zařízením požadována diagnostická relace, která již probíhá, odešle celek ve vozidle zprávu s kladnou odpovědí.

— Kdykoli zkušební zařízení požaduje novou diagnostickou relaci, odešle celek ve vozidle nejprve zprávu s kladnou odpovědí na StartDiagnosticSession předtím, než se v celku ve vozidle aktivuje nová relace. Pokud není celek ve vozidle schopen zahájit požadovanou novou diagnostickou relaci, musí odpovědět zprávou se zápornou odpovědí na StartDiagnosticSession a probíhající relace musí pokračovat.

CPR_026 Diagnostická relace se zahájí pouze tehdy, pokud byla mezi klientem a celkem ve vozidle zahájena komunikace.

CPR_027 Pokud byla dříve aktivní jiná diagnostická relace, stanou se parametry časování podle definice v tabulce 4 aktivními po úspěšné StartDiagnosticSession s parametrem diagnosticSession nastaveným ve zprávě se žádostí o„StandardDiagnosticSession“.

5.1.2 *Formát zprávy*

CPR_028 Formáty zpráv pro prvky StartDiagnosticSession jsou rozepsány v níže uvedených tabulkách.

Tabulka 14

zpráva se žádostí StartDiagnosticSession

Bajt č.	Název parametru	Hexadecimální hodnota	Symbol
#1	Formátový bajt — fyzické adresování	80	FMT
#2	Bajt cílové adresy	EE	TGT
#3	Bajt adresy zdroje	tt	SRC
#4	Bajt dodatečné délky	02	LEN
#5	**Id služby požadavku StartDiagnosticSession**	**10**	**STDS**
#6	diagnosticSession = [jedna hodnota z tabulky 17]	xx	DS_…
#7	Kontrolní součet	00-FF	CS

Tabulka 15

zpráva s kladnou odpovědí na StartDiagnosticSession

Bajt č.	Název parametru	Hexadecimální hodnota	Symbol
#1	Formátový bajt — fyzické adresování	80	FMT
#2	Bajt cílové adresy	tt	TGT
#3	Bajt adresy zdroje	EE	SRC
#4	Bajt dodatečné délky	02	LEN
#5	**Id služby kladné odpovědi na StartDiagnostic-Session**	**50**	**STDSPR**
#6	diagnosticSession = [shodná hodnota s bajtem #6 tabulka 14]	xx	DS_…
#7	Kontrolní součet	00-FF	CS

Tabulka 16

zpráva se zápornou odpovědí na StartDiagnosticSession

Bajt č.	Název parametru	Hexadecimální hodnota	Symbol
#1	Formátový bajt — fyzické adresování	80	FMT
#2	Bajt cílové adresy	tt	TGT

Bajt č.	Název parametru		Hexadecimální hodnota	Symbol
#3	Bajt adresy zdroje		EE	SRC
#4	Bajt dodatečné délky		03	LEN
#5	**Id služby záporné odpovědi**		**7F**	**NR**
#6	Id služby požadavku StartDiagnosticSession		10	STDS
#7	ResponseCode =	[subFunctionNotSupported [a]	12	RC_SFNS
		incorrectMessageLength [b]	13	RC_IML
		conditionsNotCorrect [c]	22	RC_CNC
#8	Kontrolní součet		00-FF	CS

[a] – hodnota vložená do bajtu # 6 zprávy o požadavku není podporována, tj. není v tabulce 17,
[b] – délka obdržené zprávy je chybná,
[c] – kritéria pro požadavek StartDiagnosticSession nejsou splněna.

5.1.3 *Definice parametrů*

CPR_029 Parametr ***diagnosticSession (DS_)*** využívá služba StartDiagnosticSession k výběru zvláštního chování serveru (serverů). V tomto dokumentu jsou specifikovány tyto diagnostické relace:

Tabulka 17

Definice hodnot diagnosticSession

Hex	Popis	Symbol
81	**StandardDiagnosticSession** Tato diagnostická relace umožňuje všechny služby podle **tabulky 1 sloupce 4 „SD“**. Tyto služby umožňují čtení dat ze serveru (celku ve vozidle). Tato diagnostická relace je aktivní po úspěšném dokončení inicializace mezi klientem (zkušebním zařízením) a serverem (celkem ve vozidle). Tato diagnostická relace může být přepsána jinými diagnostickými relacemi specifikovanými v této části.	**SD**
85	**ECUProgrammingSession** Tato diagnostická relace umožňuje všechny služby podle **tabulky 1 sloupce 6 „ECUPS“**. Tyto služby podporují programování paměti serveru (celku ve vozidle). Tato diagnostická relace může být přepsána jinými diagnostickými relacemi specifikovanými v této části.	**ECUPS**
87	**ECUAdjustmentSession** Tato diagnostická relace umožňuje všechny služby podle **tabulky 1 sloupce 5 „ECUAS“.** Tyto služby podporují řízení vstupu/výstupu serveru (celku ve vozidle). Tato diagnostická relace může být přepsána jinými diagnostickými relacemi specifikovanými v této části.	**ECUAS**

5.2. **Služba SecurityAccess**

Zapisování kalibračních dat není možné, pokud celek ve vozidle není v režimu KALIBRACE. Kromě vložení platné karty dílny do celku ve vozidle je nezbytné dříve, než je udělen přístup k režimu KALIBRACE, vložit do celku ve vozidle příslušný PIN.

Přístup ke kalibračnímu vodiči I/O je také možný, pokud je celek ve vozidle v režimu KALIBRACE nebo KONTROLA (CONTROL).

Služba SecurityAccess poskytuje prostředky pro vložení PIN a indikuje zkušebnímu zařízení, zda celek ve vozidle je, nebo není v režimu KALIBRACE.

PIN může být vložen alternativními postupy.

5.2.1 *Popis zprávy*

Služba SecurityAccess je tvořena zprávou SecurityAccess„requestSeed“ následovanou zprávou SecurityAccess „sendKey“. Služba SecurityAccess musí být provedena po službě StartDiagnosticSession.

CPR_033 Zkušební zařízení využívá zprávu SecurityAccess „requestSeed“, pro ověření, zda je celek ve vozidle připraven k přijetí PIN.

CPR_034 Pokud je celek ve vozidle již v režimu KALIBRACE, musí odpovědět na požadavek vysláním „seed“ 0x0000 s využitím služby kladné odpovědi na SecurityAccess.

CPR_035 Pokud je celek ve vozidle připraven k přijetí PIN pro ověření kartou dílny, musí odpovědět na požadavek vysláním „seed“ většího než 0x0000 s využitím služby kladné odpovědi na SecurityAccess.

CPR_036 Pokud není celek ve vozidle připraven k přijetí PIN od zkušebního zařízení, buď protože vložená karta dílny není platná, nebo protože karta dílny nebyla vložena, nebo protože celek ve vozidle očekává PIN jiným postupem, odpoví celek ve vozidle na požadavek zápornou odpovědí s kódem odpovědi nastaveným na conditionsNotCorrectOrRequestSequenceError.

CPR_037 Zkušební zařízení pak použije k předání PIN do celku ve vozidle zprávu SecurityAccess „sendKey“. K tomu, aby byl k dispozici čas potřebný k ověření pravosti karty, použije celek ve vozidle pro prodloužení času pro odpověď kód záporné odpovědi requestCorrectlyReceived-ResponsePending. Maximální doba pro odpověď však nesmí překročit pět minut. Jakmile byla požadovaná služba dokončena, musí celek ve vozidle vyslat zprávu s kladnou odpovědí nebo zprávu se zápornou odpovědí s odlišným kódem odpovědi. Kód záporné odpovědi requestCorrectlyReceived-Response-Pending může být celkem ve vozidle opakován do dokončení požadované služby a do vyslání zprávy s konečnou odpovědí.

CPR_038 Celek ve vozidle musí na tento požadavek odpovědět užitím služby SecurityAccess PositiveResponse pouze v režimu KALIBRACE.

CPR_039 Celek ve vozidle musí v následujících případech odpovědět na tento požadavek zápornou odpovědí s kódem odpovědi nastaveným na:

— subFunctionNot supported: neplatný formát pro parametr podfunkce (accessType),

— conditionsNotCorrectOrRequestSequenceError: celek ve vozidle není připraven k přijetí PIN,

— invalidKey: PIN není platný a počet pokusů o ověření PIN není překročen,

— exceededNumberOfAttempts: PIN není platný a počet pokusů o ověření PIN je překročen,

— generalReject: PIN je správný, ale selhalo vzájemné ověření s kartou dílny.

5.2.2 *Formát zprávy – SecurityAccess – requestSeed*

CPR_040 Formáty zpráv pro prvky SecurityAccess „requestSeed“ jsou rozepsány v níže uvedených tabulkách.

Tabulka 18

požadavek SecurityAccess – zpráva requestSeed

Bajt č.	Název parametru	Hexadecimální hodnota	Symbol
#1	Formátový bajt — fyzické adresování	80	FMT
#2	Bajt cílové adresy	EE	TGT
#3	Bajt adresy zdroje	tt	SRC
#4	Bajt dodatečné délky	02	LEN
#5	**Id služby požadavku SecurityAccess**	**27**	**SA**
#6	accessType – requestSeed	7D	AT_RSD
#7	Kontrolní součet	00-FF	CS

Tabulka 19

SecurityAccess – zpráva s kladnou odpovědí requestSeed

Bajt č.	Název parametru	Hexadecimální hodnota	Symbol
#1	Formátový bajt — fyzické adresování	80	FMT
#2	Bajt cílové adresy	tt	TGT
#3	Bajt adresy zdroje	EE	SRC
#4	Bajt dodatečné délky	04	LEN
#5	**Id služby kladné odpovědi na SecurityAccess**	**67**	**SAPR**
#6	accessType – requestSeed	7D	AT_RSD
#7	Seed High	00-FF	SEEDH
#8	Seed Low	00-FF	SEEDL
#9	Kontrolní součet	00-FF	CS

Tabulka 20

zpráva se zápornou odpovědí na SecurityAccess

Bajt č.	Název parametru	Hexadecimální hodnota	Symbol
#1	Formátový bajt — fyzické adresování	80	FMT
#2	Bajt cílové adresy	tt	TGT
#3	Bajt adresy zdroje	EE	SRC

Bajt č.	Název parametru	Hexadecimální hodnota	Symbol
#4	Bajt dodatečné délky	03	LEN
#5	**Id služby záporné odpovědi**	**7F**	**NR**
#6	Id služby požadavku SecurityAccess	27	SA
#7	responseCode = [conditionsNotCorrectOrRequestSequenceError	22	RC_CNC
	incorrectMessageLength]	13	RC_IML
#8	Kontrolní součet	00-FF	CS

5.2.3 *Formát zprávy – SecurityAccess – sendKey*

CPR_041 Formáty zpráv pro prvky SecurityAccess „sendKey“ jsou rozepsány v níže uvedených tabulkách.

Tabulka 21

požadavek SecurityAccess – zpráva sendKey

Bajt č.	Název parametru	Hexadecimální hodnota	Symbol
#1	Formátový bajt — fyzické adresování	80	FMT
#2	Bajt cílové adresy	EE	TGT
#3	Bajt adresy zdroje	tt	SRC
#4	Bajt dodatečné délky	m+2	LEN
#5	**Id služby požadavku SecurityAccess**	**27**	**SA**
#6	accessType – sendKey	7E	AT_SK
#7 až #m +6	Klíč #1 (nejvýznamnější)	xx	KEY
	…	…	
	Klíč #m (nejméně významný, m musí být nejméně 4 a nejvýše 8)	xx	
#m+7	Kontrolní součet	00-FF	CS

Tabulka 22

SecurityAccess – zpráva s kladnou odpovědí na sendKey

Bajt č.	Název parametru	Hexadecimální hodnota	Symbol
#1	Formátový bajt — fyzické adresování	80	FMT
#2	Bajt cílové adresy	tt	TGT
#3	Bajt adresy zdroje	EE	SRC

Bajt č.	Název parametru	Hexadecimální hodnota	Symbol
#4	Bajt dodatečné délky	02	LEN
#5	**Id služby kladné odpovědi na SecurityAccess**	**67**	**SAPR**
#6	accessType – sendKey	7E	AT_SK
#7	Kontrolní součet	00-FF	CS

Tabulka 23

zpráva se zápornou odpovědí na SecurityAccess

Bajt č.	Název parametru		Hexadecimální hodnota	Symbol
#1	Formátový bajt — fyzické adresování		80	FMT
#2	Bajt cílové adresy		tt	TGT
#3	Bajt adresy zdroje		EE	SRC
#4	Bajt dodatečné délky		03	LEN
#5	**Id služby záporné odpovědi**		**7F**	**NR**
#6	Id služby požadavku SecurityAccess		27	SA
#7	ResponseCode =	[generalReject	10	RC_GR
		subFunctionNotSupported	12	RC_SFNS
		incorrectMessageLength	13	RC_IML
		conditionsNotCorrectOrRequestSequenceError	22	RC_CNC
		invalidKey	35	RC_IK
		exceededNumberOfAttempts	36	RC_ENA
		requestCorrectlyReceived-ResponsePending]	78	RC_RCR_RP
#8	Kontrolní součet		00-FF	CS

6. SLUŽBY PŘENOSU DAT

Dostupné služby jsou rozepsány v následující tabulce:

Tabulka 24

Služby přenosu dat

Název služby	Popis
ReadDataByIdentifier	Klient požaduje přenos aktuální hodnoty záznamu přístupem pomocí recordDataIdentifier
WriteDataByIdentifier	Klient žádá o zápis záznamu přístupem pomocí recordDataIdentifier

6.1. **Služba ReadDataByIdentifier**

6.1.1 *Popis zprávy*

CPR_050 Služba ReadDataByIdentifier je využívána klientem pro vyžádání hodnot datového záznamu ze serveru. Data jsou identifikována pomocí recordDataIdentifier. Je odpovědností výrobce celku ve vozidle, aby při výkonu této služby byly splněny podmínky serveru.

6.1.2 *Formát zprávy*

CPR_051 Formáty zpráv pro prvky ReadDataByIdentifier jsou rozepsány v níže uvedených tabulkách.

Tabulka 25

zpráva se žádostí ReadDataByIdentifier

Bajt č.	Název parametru	Hexadecimální hodnota	Symbol
#1	Formátový bajt — fyzické adresování	80	FMT
#2	Bajt cílové adresy	EE	TGT
#3	Bajt adresy zdroje	tt	SRC
#4	Bajt dodatečné délky	03	LEN
#5	**Id služby požadavku ReadDataByIdentifier**	**22**	**RDBI**
#6 až #7	recordDataIdentifier = [hodnota z tabulky 28]	xxxx	RDI_…
#8	Kontrolní součet	00-FF	CS

Tabulka 26

zpráva s kladnou odpovědí na ReadDataByIdentifier

Bajt č.	Název parametru	Hexadecimální hodnota	Symbol
#1	Formátový bajt — fyzické adresování	80	FMT
#2	Bajt cílové adresy	tt	TGT
#3	Bajt adresy zdroje	EE	SRC
#4	Bajt dodatečné délky	m+3	LEN
#5	**Id služby kladné odpovědi na ReadDataByIdentifier**	**62**	**RDBIPR**
#6 a #7	recordDataIdentifier = [stejná hodnota, jako bajty #6 and #7, tabulka 25]	xxxx	RDI_…
#8 až #m +7	dataRecord[] = [data#1 : data#m]	xx : xx	DREC_DATA1 : DREC_DATAm
#m+8	Kontrolní součet	00-FF	CS

Tabulka 27

zpráva se zápornou odpovědí na ReadDataByIdentifier

Bajt č.	Název parametru	Hexadecimální hodnota	Symbol
#1	Formátový bajt — fyzické adresování	80	FMT
#2	Bajt cílové adresy	tt	TGT
#3	Bajt adresy zdroje	EE	SRC
#4	Bajt dodatečné délky	03	LEN
#5	**Id služby záporné odpovědi**	**7F**	**NR**
#6	Id služby požadavku ReadDataByIdentifier	22	RDBI
#7	ResponseCode= [requestOutOfRange	31	RC_ROOR
	incorrectMessageLength	13	RC_IML
	conditionsNotCorrect]	22	RC_CNC
#8	Kontrolní součet	00-FF	CS

6.1.3 *Definice parametrů*

CPR_052 Parametr ***recordDataIdentifier (RDI_)*** ve zprávě o požadavku ReadDataByIdentifier identifikuje datový záznam.

CPR_053 Hodnoty recordDataIdentifier definované tímto dokumentem jsou uvedeny v níže uvedené tabulce.

Tabulka recordDataIdentifier je tvořena čtyřmi sloupci a několika řádky.

— **První sloupec (Hex)** obsahuje „hexadecimální hodnotu“ přiřazenou k recordDataIdentifier specifikovanému ve třetím sloupci.

— **Druhý sloupec (Datový prvek)** stanovuje datový prvek z dodatku 1, na kterém je založen identifikátor recordDataIdentifier (někdy je potřebné překódování).

— **Třetí sloupec (Popis)** specifikuje odpovídající název recordDataIdentifier,

— **Čtvrtý sloupec (Symbol)** specifikuje pro tento recordDataIdentifier příslušný symbol.

Tabulka 28

Definice hodnot recordDataIdentifier

Hex	Datový prvek	recordDataIdentifier Name (viz formát v bodě 8.2)	Symbol
F90B	`CurrentDateTime`	TimeDate	RDI_TD
F912	`HighResOdometer`	HighResolutionTotalVehicleDistance	RDI_HRTVD
F918	`K-ConstantOfRecordingEquipment`	Kfactor	RDI_KF

Hex	Datový prvek	recordDataIdentifier Name (viz formát v bodě 8.2)	Symbol
F91C	L-TyreCircumference	LfactorTyreCircumference	RDI_LF
F91D	W-VehicleCharacteristicConstant	WvehicleCharacteristicFactor	RDI_WVCF
F921	TyreSize	TyreSize	RDI_TS
F922	nextCalibrationDate	NextCalibrationDate	RDI_NCD
F92C	SpeedAuthorised	SpeedAuthorised	RDI_SA
F97D	vehicleRegistrationNation	RegisteringMemberState	RDI_RMS
F97E	VehicleRegistrationNumber	VehicleRegistrationNumber	RDI_ VRN
F190	VehicleIdentificationNumber	VIN	RDI_ VIN

CPR_054 Parametr ***dataRecord (DREC_)*** se použije ve zprávě s kladnou odpovědí na ReadDataByIdentifier k tomu, aby klientovi (zkušebnímu zařízení) byla dodána hodnota datového záznamu identifikovaného pomocí recordDataIdentifier. Formáty dat jsou specifikovány v části 8. Mohou být volitelně implementovány další uživatelské dataRecords včetně vstupu specifického pro VU, vnitřních a výstupních dat, ty však nejsou definovány v tomto dokumentu.

6.2. **Služba WriteDataByIdentifier**

6.2.1 *Popis zprávy*

CPR_056 Službu WriteDataByIdentifier používá klient k zápisu hodnot datového záznamu na server. Data jsou identifikována pomocí recordDataIdentifier. Je odpovědností výrobce celku ve vozidle, aby při výkonu této služby byly splněny podmínky serveru. Pro aktualizaci parametrů uvedených v tabulce 28 musí být celek ve vozidle v režimu KALIBRACE.

6.2.2 *Formát zprávy*

CPR_057 Formáty zpráv pro prvky WriteDataByIdentifier jsou rozepsány v níže uvedených tabulkách.

Tabulka 29

zpráva se žádostí WriteDataByIdentifier

Bajt č.	Název parametru	Hexadecimální hodnota	Symbol
#1	Formátový bajt — fyzické adresování	80	FMT
#2	Bajt cílové adresy	EE	TGT
#3	Bajt adresy zdroje	tt	SRC
#4	Bajt dodatečné délky	m+3	LEN
#5	**Id služby požadavku WriteDataByIdentifier**	**2E**	**WDBI**
#6 až #7	recordDataIdentifier = [hodnota z tabulky 28]	xxxx	RDI_…

Bajt č.	Název parametru	Hexadecimální hodnota	Symbol
#8 až #m +7	dataRecord[] = [data#1 : data#m]	xx : xx	DREC_DATA1 : DREC_DATAm
#m+8	Kontrolní součet	00-FF	CS

Tabulka 30

zpráva s kladnou odpovědí na WriteDataByIdentifier

Bajt č.	Název parametru	Hexadecimální hodnota	Symbol
#1	Formátový bajt — fyzické adresování	80	FMT
#2	Bajt cílové adresy	tt	TGT
#3	Bajt adresy zdroje	EE	SRC
#4	Bajt dodatečné délky	03	LEN
#5	**Id služby kladné odpovědi na WriteDataByIdentifier**	**6E**	**WDBIPR**
#6 až #7	recordDataIdentifier = [stejná hodnota, jako bajty #6 and #7, tabulka 29]	xxxx	RDI_…
#8	Kontrolní součet	00-FF	CS

Tabulka 31

zpráva se zápornou odpovědí na WriteDataByIdentifier

Bajt č.	Název parametru	Hexadecimální hodnota	Symbol
#1	Formátový bajt — fyzické adresování	80	FMT
#2	Bajt cílové adresy	tt	TGT
#3	Bajt adresy zdroje	EE	SRC
#4	Bajt dodatečné délky	03	LEN
#5	**Id služby záporné odpovědi**	**7F**	**NR**
#6	Id služby požadavku WriteDataByIdentifier	2E	WDBI

Bajt č.	Název parametru		Hexadecimální hodnota	Symbol
#7	ResponseCode=	[requestOutOfRange	31	RC_ROOR
		incorrectMessageLength	13	RC_IML
		conditionsNotCorrect]	22	RC_CNC
#8	Kontrolní součet		00-FF	CS

6.2.3 *Definice parametrů*

Parametr ***recordDataIdentifier (RDI_)*** je definován v tabulce 28.

Parametr ***dataRecord (DREC_)*** se použije ve zprávě o požadavku WriteDataByIdentifier k tomu, aby klientovi (zkušebnímu zařízení) byly dodány hodnoty datových záznamů identifikovaných pomocí recordDataIdentifier. Formáty dat jsou specifikovány v části 8.

7. ŘÍZENÍ ZKUŠEBNÍCH IMPULSŮ – ŘÍDÍCÍ FUNKČNÍ CELEK VSTUPU/VÝSTUPU

Dostupné služby jsou rozepsány v následující tabulce:

Tabulka 32

Řídící funkční celek vstupu/výstupu

Název služby	Popis
InputOutputControlByIdentifier	Klient požaduje řízení vstupu/výstupu specifické pro server.

7.1. **Služba InputOutputControlByIdentifier**

7.1.1 *Popis zprávy*

Existuje propojení přes přední konektor, které umožňuje, aby zkušební impulsy byly řízeny nebo monitorovány pomocí vhodného zkušebního zařízení.

CPR_058 Tento kalibrační signálový vodič I/O (vstup/výstup) může být konfigurován příkazem přes vodič K využitím služby InputControlByIdentifier k volbě požadované vstupní nebo výstupní funkce vodiče. Dostupné stavy vodiče jsou:

— neaktivní,

— speedSignalInput, kdy je kalibrační signálový vodič I/O použit pro vstup rychlostního signálu (zkušební signál), který nahrazuje rychlostní signál snímače pohybu; tato funkce není dostupná v režimu KONTROLA,

— realTimeSpeedSignalOutputSensor, kdy je kalibrační signálový vodič I/O použit pro výstup rychlostního signálu ze snímače pohybu,

— RTCOutput, kdy je kalibrační signálový vodič I/O použit pro výstup hodinového signálu UTC; tato funkce není dostupná v režimu KONTROLA.

CPR_059 Celek ve vozidle musí zahájit seřizovací relaci a musí být v režimu KALIBRACE, nebo KONTROLA, aby bylo možné konfigurovat stav vodiče. Pokud je celek ve vozidle v režimu KALIBRACE, mohou být vybrány čtyři stavy spojení (neaktivní, speedSignalInput, realTimeSpeedSignalOutputSensor, RTCOutput). Pokud je celek ve vozidle v režimu KONTROLA, mohou být vybrány pouze dva stavy spojení (neaktivní, realTimeSpeedOutputSensor). Při ukončení seřizovací relace, nebo režimu KALIBRACE, nebo KONTROLA musí celek ve vozidle zajistit, aby se kalibrační signálový vodič I/O vrátil do stavu „disabled“ (neaktivní) (výchozí).

CPR_060 Pokud jsou na signálovém vodiči rychlosti v reálném čase celku ve vozidle přijaty rychlostní impulsy v době, kdy je kalibrační signálový vodič I/O nastaven jako vstup, musí se kalibrační signálový vodič I/O nastavit jako výstup nebo vrátit do neaktivního stavu.

CPR_061 Sekvence je tato:

— zahájit komunikaci prostřednictvím služby StartCommunication,

— zahájit seřizovací relaci prostřednictvím služby StartDiagnosticSession a být v provozním režimu KALIBRACE, nebo KONTROLA (pořadí těchto dvou operací není důležité),

— změnit stav výstupu pomocí služby InputOutputControlByIdentifier.

7.1.2 *Formát zprávy*

CPR_062 Formáty zpráv pro prvky InputOutputControlByIdentifier jsou rozepsány v níže uvedených tabulkách.

Tabulka 33

zpráva se žádostí InputOutputControlByIdentifier

Bajt č.	Název parametru	Hexadecimální hodnota	Symbol
#1	Formátový bajt — fyzické adresování	80	FMT
#2	Bajt cílové adresy	EE	TGT
#3	Bajt adresy zdroje	tt	SRC
#4	Bajt dodatečné délky	xx	LEN
#5	**Id služby požadavku InputOutputControlByIdentifier**	**2F**	**IOCBI**
#6 a #7	InputOutputIdentifier = [CalibrationInputOutput]	F960	IOI_CIO
#8 nebo	ControlOptionRecord = [		COR_…
#8 až #9	inputOutputControlParameter – one value from tabulky 36	xx	IOCP_…
	controlState — jedna z hodnot v tabulce 37 (viz poznámka níže)	xx	CS_…
#9 nebo #10	Kontrolní součet	00-FF	CS

Poznámka: parametr controlState je přítomný jen v některých případech (viz 7.1.3).

Tabulka 34

zpráva s kladnou odpovědí na InputOutputControlByIdentifier

Bajt č.	Název parametru	Hexadecimální hodnota	Symbol
#1	Formátový bajt — fyzické adresování	80	FMT
#2	Bajt cílové adresy	tt	TGT

Bajt č.	Název parametru	Hexadecimální hodnota	Symbol
#3	Bajt adresy zdroje	EE	SRC
#4	Bajt dodatečné délky	xx	LEN
#5	**Id služby kladné odpovědi na inputOutput-ControlByIdentifier**	**6F**	**IOCBIPR**
#6 a #7	inputOutputIdentifier = [CalibrationInputOutput]	F960	IOI_CIO
#8 nebo #8 až #9	controlStatusRecord = [inputOutputControlParameter (stejná hodnota jako bajt #8 v tabulce 33) controlState (stejná hodnota jako bajt #9 v tabulce 33)] (v příslušných případech)	 xx xx	CSR_ IOCP_… CS_…
#9 nebo #10	Kontrolní součet	00-FF	CS

Tabulka 35

zpráva se zápornou odpovědí na InputOutputControlByIdentifier

Bajt č.	Název parametru	Hexadecimální hodnota	Symbol
#1	Formátový bajt — fyzické adresování	80	FMT
#2	Bajt cílové adresy	tt	TGT
#3	Bajt adresy zdroje	EE	SRC
#4	Bajt dodatečné délky	03	LEN
#5	**Id služby záporné odpovědi**	**7F**	**NR**
#6	Id služby požadavku inputOutputControlByIdentifier	2F	IOCBI
#7	responseCode=[incorrectMessageLength conditionsNotCorrect requestOutOfRange deviceControlLimitsExceeded]	 13 22 31 7A	 RC_IML RC_CNC RC_ROOR RC_DCLE
#8	Kontrolní součet	00-FF	CS

7.1.3 *Definice parametrů*

CPR_064 Parametr ***inputOutputControlParameter (IOCP_)*** je definován v následující tabulce.

Tabulka 36

Definice hodnot inputOutputControlParameter

Hex	Popis	Symbol
00	**ReturnControlToECU** Tato hodnota indikuje serveru (celku ve vozidle), že zkušební zařízení již neřídí kalibrační signálový vodič I/O.	RCTECU
01	**ResetToDefault** Tato hodnota indikuje serveru (celku ve vozidle), že se od něj požaduje nastavení kalibračního signálového vodiče I/O do výchozího stavu.	RTD
03	**ShortTermAdjustment** Tato hodnota musí indikovat serveru (celku ve vozidle), že se požaduje nastavení kalibračního signálového vodiče I/O na hodnotu obsaženou v parametru controlState.	STA

CPR_065 Parametr ***controlState*** je přítomen pouze tehdy, když je inputOutputControlParameter nastaven na ShortTermAdjustment, a je definován v následující tabulce:

Tabulka 37

Definice hodnot controlState

Režim	Hexadecimální hodnota	Popis
Neaktivní	00	I/O vodič je neaktivní (výchozí stav)
Aktivní	01	Aktivuje kalibrační spojení I/O jako speedSignalInput
Aktivní	02	Aktivuje kalibrační spojení I/O jako realTimeSpeedSignalOutput-Sensor
Aktivní	03	Aktivuje kalibrační spojení I/O jako RTCOutput

8. FORMÁTY DATARECORDS

Tato část uvádí:

— obecná pravidla, která se mají použít na rozsahy parametrů přenášených celkem ve vozidle do zkušebního zařízení,

— formáty, které mají být použity u dat přenášených pomocí služeb přenosu dat popsaných v části 6.

CPR_067 Veškeré identifikované parametry musí být podporovány celkem ve vozidle.

CPR_068 Data přenášená celkem ve vozidle do zkušebního zařízení jako odpověď na zprávu s požadavkem musí být naměřeného typu (tj. musí to být aktuální hodnota požadovaného parametru naměřená nebo zjištěná celkem ve vozidle).

8.1. **Rozsahy přenášených parametrů**

CPR_069 Tabulka 38 definuje rozsahy použité ke stanovení platnosti přenášených parametrů.

CPR_070 Hodnoty v rozsahu „error indicator“ (indikátor chyby) jsou pro celek ve vozidle prostředkem, jak okamžitě indikovat, že v důsledku nějakého druhu chyby v tachografu nejsou momentálně dostupná platná parametrická data.

CPR_071 Hodnoty v rozsahu „not available“ (nedostupné) jsou pro celek ve vozidle prostředkem, jak předat zprávu, která obsahuje parametr, který není v daném modulu dostupný nebo není podporován. Hodnoty v rozsahu „not requested“ (nevyžádané) jsou pro zařízení prostředkem, jak předat zprávu s příkazem a identifikovat ty parametry, u kterých se neočekává žádná odpověď z přijímacího zařízení.

CPR_072 Pokud závada některé součásti brání přenosu platných dat parametru, je možné místo dat parametru použít „error indicator“ (indikátor chyby) podle popisu v tabulce 38. Pokud však naměřená nebo vypočtená data poskytují hodnotu, která je platná, ale přesahuje definovaný rozsah parametru, neměl by být „error indicator“ (indikátor chyby) použit. Data by měla být přenesena s využitím přiměřené minimální nebo maximální hodnoty parametru.

Tabulka 38

rozsahy dataRecords

Název rozsahu	1 bajt (hexadecimální hodnota)	2 bajty (hexadecimální hodnota)	4 bajty (hexadecimální hodnota)	ASCII
Platný signál	00 až FA	0000 až FAFF	00000000 až FAFFFFFF	1 až 254
Specifický indikátor parametru	FB	FB00 až FBFF	FB000000 až FBFFFFFF	žádný
Rezervní rozsah pro budoucí indikační bity	FC až FD	FC00 až FDFF	FC000000 až FDFFFFFF	žádný
Indikátor chyby	FE	FE00 až FEFF	FE000000 až FEFFFFFF	0
Nedostupné nebo nevyžádané	FF	FF00 až FFFF	FF000000 až FFFFFFFF	FF

CPR_073 Pro parametry kódované v ASCII je ASCII symbol „*“ vyhrazen jako oddělovací znak.

8.2. **Formáty dataRecords**

V níže uvedených tabulkách 39 až 42 jsou podrobně uvedeny formáty, které musí být použity prostřednictvím služeb ReadDataByIdentifier a WriteDataByIdentifier.

CPR_074 V tabulce 39 je uvedena délka, rozlišení a pracovní rozsah každého z parametrů identifikovaných pomocí jeho recordDataIdentifier.

Tabulka 39

Formát dataRecords

Název parametru	Délka dat (v bajtech)	Rozlišení	Pracovní rozsah
TimeDate	8	Podrobnosti viz tabulka 40	
HighResolutionTotalVehicleDistance	4	5 m/bit, offset 0 m	0 až + 21 055 406 km
Kfactor	2	0,001 imp/m/bit, offset 0	0 až 64,255 imp/m
LfactorTyreCircumference	2	0,125 10^{-3} m /bit, offset 0	0 až + 8,031 m
WvehicleCharacteristicFactor	2	0,001 imp/m /bit, offset 0	0 až 64,255 imp/m
TyreSize	15	ASCII	ASCII

Název parametru	Délka dat (v bajtech)	Rozlišení	Pracovní rozsah
NextCalibrationDate	3	Podrobnosti viz tabulka 41	
SpeedAuthorised	2	1/256 km/h/bit, offset 0	0 až 250,996 km/h
RegisteringMemberState	3	ASCII	ASCII
VehicleRegistrationNumber	14	Podrobnosti viz tabulka 42	
VIN	17	ASCII	ASCII

CPR_075 Tabulka 40 rozepisuje formáty různých bajtů parametru TimeDate:

Tabulka 40

Rozepsaný formát TimeDate (recordDataIdentifier, s hodnotou # F90B)

Bajt	Definice parametrů	Rozlišení	Pracovní rozsah
1	Sekundy	0,25 s/bit, offset 0 s	0 až 59,75s
2	Minuty	1 min/bit, offset 0 min	0 až 59 min
3	Hodiny	1 h/bit, offset 0 h	0 až 23 h
4	Měsíc	1 měsíc/bit, offset 0 měsíců	1 až 12 měsíců
5	Den	0,25 dne/bit, offset 0 dnů (viz POZNÁMKA níže tabulka 41)	0,25 až 31,75 dne
6	Rok	1 rok/bit, offset +1985 (viz POZNÁMKA níže tabulka 41)	léta 1985 až 2235
7	Místní offset v minutách	1 min/bit, offset – 125 min	– 59 až + 59 min
8	Místní offset v hodinách	1 h/bit, offset – 125 h	– 23 až + 23 h

CPR_076 Tabulka 41 rozepisuje formáty různých bajtů parametru NextCalibrationDate.

Tabulka 41

Rozepsaný formát NextCalibrationDate (recordDataIdentifier s hodnotou # F922)

Bajt	Definice parametrů	Rozlišení	Pracovní rozsah
1	Měsíc	1 měsíc/bit, offset 0 měsíců	1 až 12 měsíců
2	Den	0,25 dne/bit, offset 0 dnů (viz POZNÁMKA níže)	0,25 až 31,75 dne
3	Rok	1 rok/bit, offset rok +1985 (viz POZNÁMKA níže)	léta 1985 až 2235

POZNÁMKA týkající se použití parametru „den“:

1) Hodnota 0 je pro datum prázdnou hodnotou. Hodnoty 1, 2, 3 a 4 se užívají k identifikaci prvního dne v měsíci; 5, 6, 7 a 8 identifikují druhý den v měsíci atd.

2) Tento parametr neovlivňuje ani nemění výše uvedený parametr hodin.

POZNÁMKA týkající se užití bajtu parametru „rok“:

Hodnota 0 označuje rok 1985; hodnota 1 označuje rok 1986 atd.

CPR_078 Tabulka 42 rozepisuje formáty různých bajtů parametru VehicleRegistrationNumber:

Tabulka 42

Rozepsaný formát VehicleRegistrationNumber (recordDataIdentifier s hodnotou # F97E)

Bajt	Definice parametrů	Rozlišení	Pracovní rozsah
1	Kódová stránka (podle definice v dodatku 1)	ASCII	01 až 0A
2 – 14	Registrační značka vozidla (podle definice v dodatku 1)	ASCII	ASCII

Dodatek 9.

SCHVÁLENÍ TYPU MINIMÁLNÍ ROZSAH POŽADOVANÝCH ZKOUŠEK

OBSAH

1. ÚVOD

1.1 **Schválení typu**

ES schválení typu pro záznamové zařízení (nebo jeho součást) nebo pro kartu tachografu se zakládá na:

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

— **osvědčení funkčnosti** prováděné příslušným orgánem členského státu, který osvědčuje, že zkoušený prvek splňuje požadavky této přílohy z hlediska prováděných funkcí, přesnosti měření a environmentálních vlastností,

— **osvědčení interoperability** prováděné příslušným subjektem, který osvědčuje, že záznamové zařízení (nebo karta tachografu) je plně interoperabilní s potřebnými modely karty tachografu (nebo záznamového zařízení) (viz kapitolu 8 této přílohy).

Tento dodatek stanoví formou minimálních požadavků, jaké zkoušky musí provést orgán členského státu při funkčních zkouškách a jaké zkoušky musí provést příslušný subjekt při zkouškách interoperability. Postup při zkouškách ani typy zkoušek se podrobněji nespecifikují.

Tento dodatek se nezabývá aspekty osvědčování bezpečnosti. Pokud se některé ze zkoušek vyžadovaných pro schválení typu provedou v průběhu hodnocení a osvědčování bezpečnosti, není třeba takové zkoušky opakovat. V takovém případě stačí posoudit výsledky těchto zkoušek bezpečnosti. Pro informaci jsou v tomto dodatku hvězdičkou „*“ označeny požadavky, u kterých se očekává, že budou zkoušeny během osvědčování bezpečnosti (nebo které úzce souvisí se zkouškami, jejichž provedení se během osvědčování bezpečnosti očekává).

Číslované požadavky odkazují na text přílohy, zatímco další požadavky odkazují na ostatní dodatky (např. PIC_001 odkazuje na požadavek PIC_001 v dodatku 3 Piktogramy).

V tomto dodatku se samostatně pojednává o schválení typu snímače pohybu, celku ve vozidle a vnějšího zařízení GNSS jako součástí záznamového zařízení. Každá součást získá vlastní osvědčení o schválení typu, ve kterém budou uvedeny ostatní kompatibilní součásti. Funkční zkouška snímače pohybu (nebo vnějšího zařízení GNSS) se provádí společně s celkem ve vozidle a naopak.

Není požadována interoperabilita všech modelů snímačů pohybu (resp. vnějších zařízení GNSS) a všech modelů celků ve vozidle. V takovém případě se schválení typu snímače pohybu (resp. vnějšího zařízení GNSS) může udělit jen ve spojení se schválením typu příslušného celku ve vozidle a naopak.

1.2 **Odkazy**

V tomto dodatku se používají tyto odkazy:

IEC 60068-2-1: *Environmental testing – Part 2-1: Tests – Test A: Cold*

IEC 60068-2-2: *Basic environmental testing procedures; part 2: tests; tests B: dry heat* (sinusoidal).

IEC 60068-2-6: *Environmental testing – Part 2: Tests – Test Fc: Vibration*

IEC 60068-2-14: *Environmental testing;* Part 2-14: *Tests; Test N: Change of temperature*

IEC 60068-2-27: *Environmental testing. Part 2: Tests. Test Ea and guidance: Shock*

IEC 60068-2-30: *Environmental testing – Part 2-30: Tests – Test Db: Damp heat, cyclic (12 h + 12 h cycle)*

IEC 60068-2-64: *Environmental testing – Part 2-64: Tests – Test Fh: Vibration, broadband random and guidance*

IEC 60068-2-78 Environmental testing – Part 2-78: Tests – Test Cab: Damp heat, steady state

ISO 16750-3 – *Mechanical loads (2012-12)*

ISO 16750-4 – *Climatic loads(2010-04).*

ISO 20653: *Road vehicles – Degree of protection (IP code) – Protection of electrical equipment against foreign objects, water and access*

ISO 10605:2008 + technická oprava: 2010 + AMD1: 2014 *Road vehicles – Test methods for electrical disturbances from electrostatic discharge*

ISO 7637-1:2002 + AMD1: 2008 *Road vehicles – Electrical disturbances from conduction and coupling – Part 1: Definitions and general considerations.*

ISO 7637-2 *Road vehicles – Electrical disturbances from conduction and coupling – Part 2: Electrical transient conduction along supply lines only.*

ISO 7637-3 *Road vehicles – Electrical disturbances from conduction and coupling – Part 3: Electrical transient transmission by capacitive and inductive coupling via lines other than supply lines.*

ISO/IEC 7816-1 *Identification cards – Integrated circuit(s) cards with contacts – Part 1: Physical characteristics.*

ISO/IEC 7816-2 *Information technology – Identification cards – Integrated circuit(s) cards with contacts – Part 2: Dimensions and location of the contacts.*

ISO/IEC 7816-3 *Information technology – Identification cards – Integrated circuit(s) cards with contacts – Part 3: Electronic signals and transmission protocol.*

ISO/IEC 10373-1:2006 + AMD1:2012 *Identification cards – Test methods – Part 1: General characteristics*

ISO/IEC 10373-3:2010 + technická oprava: 2013 *Identification cards – Test methods – Part 3: Integrated circuit cards with contacts and related interface devices*

ISO 16844-3:2004, oprava 1:2006 *Road vehicles – Tachograph systems – Part 3: Motion sensor interface (with vehicle units).*

ISO 16844-4 *Road vehicles – Tachograph systems – Part 4: CAN interface*

ISO 16844-6 *Road vehicles – Tachograph systems – Part 6: Diagnostics*

ISO 16844-7 *Road vehicles – Tachograph systems – Part 7: Parameters*

ISO 534 *Paper and board – Determination of thickness, density and specific volume*

Předpis EHK OSN č. 10: *Uniform provisions concerning the approval of vehicles with regard to electromagnetic compatibility (United Nation Economic Commission for Europe)*

2. FUNKČNÍ ZKOUŠKY CELKU VE VOZIDLE

Č.	Zkouška	Popis	Související požadavky
1	**Administrativní šetření**		
1.1	Dokumentace	Správnost dokumentace	
1.2	Výsledky zkoušek výrobce	Výsledky zkoušek provedených výrobcem 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		03, 04, 05, 07, 382,
3.2	Provozní režimy		09 až 11*, 132, 133
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*, 132
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, 132
3.8	Sledování stavu řízení		54, 55, 132

Č.	Zkouška	Popis	Související požadavky
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 88 132
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		134, 135, 136*, 137*, 139*, 140, 141 142, 143, 144*, 145*, 146*, 147, 148
3.28	Zobrazení		90, 132, 149 až 166, PIC_001, DIS_001
3.29	Tisk		90, 132, 167 až 179, PIC_001, PRT_001 až PRT_012
3.30	Varování		132, 180 až 189, PIC_001

Č.	Zkouška	Popis	Související požadavky
3.31	Stahování dat na externí paměťová média		90, 132, 190 až 194
3.32	Dálková komunikace pro cílené silniční kontroly		195 až 197
3.33	Výstup dat do dalších vnějších zařízení		198, 199
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
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 vlivu 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: *Environmental testing – Part 2-1: Tests – Test A: Cold* 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: *Basic environmental testing procedures; part 2: tests; tests B: dry heat* Zkouška podle ISO 16750-4: *Chapter 5.3.2: Rapid change of temperature with specified transition duration* (– 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

Č.	Zkouška	Popis	Související požadavky
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. 2. Náhodné vibrace: Zkouška podle ISO 16750-3: *Chapter 4.1.2.8: Test VIII: Commercial vehicle, decoupled vehicle cab* Zkouška náhodnými vibracemi, 10…2 000 Hz, efektivní vertikální zrychlení 21,3 m/s², efektivní podélné zrychlení 11,8 m/s², efektivní příčné zrychlení 13,1 m/s², 3 osy, 32 h na osu, včetně teplotního cyklu – 20…70 °C. Tato zkouška odkazuje na IEC 60068-2-64: *Environmental testing – Part 2-64: Tests – Test Fh: Vibration, broadband random and guidance* 3. Rázy: mechanický půlsinusový ráz o velikosti 3 g podle ISO 16750. Výše uvedené zkoušky se provádějí na různých vzorcích typu testovaného zařízení.	219
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

Č.	Zkouška	Popis	Související požadavky
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
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

3. FUNKČNÍ ZKOUŠKY SNÍMAČŮ POHYBU

Č.	Zkouška	Popis	Související požadavky
1.	**Administrativní šetření**		
1.1	Dokumentace	Správnost dokumentace	

Č.	Zkouška	Popis	Související požadavky
2.	**Vizuální kontrola**		
2.1.	Shoda s dokumentací		
2.2.	Identifikace/značení		225, 226,
2.3	Materiály		219 až 223
2.4.	Plomby		398, 401 až 405
3.	**Funkční zkoušky**		
3.1	Identifikační údaje snímače		95 až 97*
3.2	Párování snímače pohybu s celkem ve vozidle		122*, 204
3.3	Detekce pohybu Přesnost měření pohybu		30 až 35
3.4	Rozhraní s celkem ve vozidle		02
3.5	Ověřit, zda je snímač pohybu imunní vůči konstantnímu magnetickému poli. Alternativně ověřit, že snímač pohybu reaguje na konstantní magnetická pole, která narušují detekci pohybu vozidla, tak, že připojený celek ve vozidle detekuje, zaznamená a ukládá závady snímače.		217
4.	**Zkoušky vlivu prostředí**		
4.1	Provozní teplota	Ověřit funkčnost (jak stanoví zkouška č. 3.3) v teplotním rozsahu [– 40 °C; + 135 °C] podle: IEC 60068-2-1, zkouška Ad, s dobou trvání 96 hod při nejnižší teplotě To_{min}, IEC 60068-2-2, zkouška Bd, s dobou trvání 96 hod při nejvyšší teplotě To_{max} Zkouška podle ISO 16750-4, kapitoly 5.1.1.2: provozní zkouška při nízké teplotě (24 h při – 40 °C) Tato zkouška odkazuje na IEC 60068-2-1: *Environmental testing – Part 2-1: Tests – Test A: Cold* IEC 68-2-2 zkouška Bd, doba trvání 96 hod. při nejnižší teplotě – 40 °C. Zkouška podle ISO 16750-4, kapitoly 5.1.2.2: provozní zkouška při vysoké teplotě (96 h při 135 °C) Tato zkouška odkazuje na IEC 60068-2-2: *Basic environmental testing procedures; part 2: tests; tests B: dry heat*	213

Č.	Zkouška	Popis	Související požadavky
4.2	Teplotní cykly	Zkouška podle ISO 16750-4: *Chapter 5.3.2: Rapid change of temperature with specified transition duration* (– 40°C/135 °C, 20 cyklů, prodleva 30 min při každé teplotě) IEC 60068-2-14: *Environmental testing; Part 2-14: Tests; Test N: Change of temperature*	213
4.3	Vlhkostní cykly	Ověřit funkčnost (jak stanoveno ve zkoušce 3.3) podle IEC 60068-2-30, zkouška Db, šest 24hodinových cyklů, každý se změnou teploty od + 25 °C do + 55 °C a relativní vlhkostí od 97 % při + 25 °C resp. 93 % při + 55 °C	214
4.4	Vibrace	ISO 16750-3: *Chapter 4.1.2.6: Test VI: Commercial vehicle, engine, gearbox* Zkouška vibracemi ve smíšeném módu zahrnující: a) zkoušku sinusovými vibracemi, 20…520 Hz, 11,4 … 120 m/s², <= 0,5 oktávy/min; b) zkoušku náhodnými vibracemi, 10…2 000 Hz, efektivní zrychlení 177 m/s²; 94 h na osu, včetně teplotního cyklu -20…70 °C Tato zkouška odkazuje na IEC 60068-2-80: *Environmental testing – Part 2-80: Tests – Test Fi: Vibration – Mixed mode*	219
4.5	Mechanický ráz	ISO 16750-3: *Chapter 4.2.3: Test VI: Test for devices in or on the gearbox* půlsinusový ráz, zrychlení se dohodne v rozsahu 3 000… 15 000 m/s², délka impulsu se dohodne, avšak < 1 ms, počet rázů: dohodne se Tato zkouška odkazuje na IEC 60068-2-27: *Environmental testing. Part 2: Tests. Test Ea and guidance: Shock*	219
4.6	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 IP 64)	220, 221
4.7	Ochrana proti záměně polarity	Ověřit, že snímač pohybu vydrží přepólování napájecího napětí	216
4.8	Ochrana proti zkratu	Ověřit, že vstupní a výstupní signály jsou chráněny proti zkratu vůči napájení a uzemnění	216

Č.	Zkouška	Popis	Související požadavky
5.	**Elektromagnetická kompatibilita**		
5.1	Vyzařované emise a citlivost	Ověřit 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
5.3	Odolnost proti rušení vedenému datovými 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

4. FUNKČNÍ ZKOUŠKY KARET TACHOGRAFU

Zkoušky podle této části 4,

bodu 5 „Zkoušky protokolu“,

bodu 6 „Struktura karty“ a

bodu 7 „Funkční zkoušky“

může osoba provádějící hodnocení nebo vystavující osvědčení provádět během postupu osvědčení bezpečnosti podle *Common Criteria* pro čipový modul.

Zkoušky č. 2.3 a 4.2 jsou stejné. Jde o mechanické zkoušky kombinace těla karty a čipového modulu. Pokud se některá z těchto částí (tělo karty, čipový modul) změní, jsou tyto zkoušky nezbytné.

Č.	Zkouška	Popis	Související požadavky
1.	**Administrativní šetření**		
1.1	Dokumentace	Správnost dokumentace	
2	**Tělo karty**		
2.1	Potisk	Ověřit, že všechny ochranné prvky a viditelné údaje jsou na kartě správné natištěny a jsou v souladu s požadavky. [Označení] Příloha 1C, kapitola 4.1 „Viditelné údaje“, 227) Přední strana musí obsahovat: slova „Karta řidiče“ nebo „Kontrolní karta“ nebo „Karta dílny“ nebo „Karta podniku“ vytištěná velkými písmeny v úředním jazyce nebo jazycích členského státu vydávajícího kartu, podle typu karty. [Název členského státu] Příloha 1C, kapitola 4.1 „Viditelné údaje“, 228) Přední strana musí obsahovat: název členského státu vydávajícího kartu (volitelně). [Značka] Příloha 1C, kapitola 4.1 „Viditelné údaje“, 229) Přední strana musí obsahovat: rozlišovací značku členského státu vydávajícího kartu, která je tištěna inverzně v modrém obdélníku a je obklopena 12 žlutými hvězdami. [Číslování] Příloha 1C, kapitola 4.1 „Viditelné údaje“, 232) Rubová strana musí obsahovat: vysvětlení očíslovaných položek uvedených na přední straně karty. [Barva] Příloha 1C, kapitola 4.1 „Viditelné údaje“, 234) Karty tachografu musí být tištěny s těmito převládajícími barvami pozadí: — karta řidiče: bílá barva, — karta dílny: červená barva, — kontrolní karta: modrá barva, — karta podniku: žlutá barva.	227 až 229, 232, 234 až 236

Č.	Zkouška	Popis	Související požadavky
		[Zabezpečení] Příloha 1C, kapitola 4.1 „Viditelné údaje“, 235) Karty tachografu musí nést minimálně tyto ochranné prvky, které chrání tělo karty proti padělání a pozměňování: — bezpečnostní provedení pozadí ve formě proplétané textury a duhový tisk, — nejméně jednu dvoubarevnou mikrotiskovou linku.	
		[Značení] Příloha 1C, kapitola 4.1 „Viditelné údaje“, 236) Členské státy mohou přidat barvy nebo označení, jako jsou vnitrostátní symboly a bezpečnostní prvky.	
		[Značka schválení] Karty tachografu obsahují značku schválení. Značka schválení sestává: — z obdélníku, ve kterém je písmeno „e“ následované rozlišovacím číslem nebo písmeny země, která udělila schválení, — z čísla schválení, které odpovídá číslu osvědčení o schválení karty tachografu a které se umístí kdekoliv v bezprostřední blízkosti obdélníku.	
2.2	Mechanické zkoušky	[Velikost karet] Karty tachografu musí odpovídat normě ISO/IEC 7810, *Identification cards – Physical characteristics,* [5] *Dimension of card,* [5.1] *Card size,* [5.1.1] *Card dimensions and tolererances,* typ karty ID-1 Nepoužitá karta	240, 243 ISO/IEC 7810
		[Hrany karty] Karty tachografu musí odpovídat normě ISO/IEC 7810, *Identification cards – Physical characteristics,* [5] *Dimension of card,* [5.1] *Card size,* [5.1.2] *Card edges*	

Č.	Zkouška	Popis	Související požadavky
		[Konstrukce karet] Karty tachografu musí odpovídat normě ISO/IEC 7810, *Identification cards – Physical characteristics,* [6] *Card construction*	
		[Materiály karet] Karty tachografu musí odpovídat normě ISO/IEC 7810, *Identification cards – Physical characteristics,* [7] *Card materials*	
		[Ohybová tuhost] Karty tachografu musí odpovídat normě ISO/IEC 7810, *Identification cards – Physical characteristics,* [8] *Card characteristics,* [8.1] *Bending stiffness*	
		[Toxicita] Karty tachografu musí odpovídat normě ISO/IEC 7810, *Identification cards – Physical characteristics,* [8] *Card characteristics,* [8.3] *Toxicity*	
		[Odolnost proti chemikáliím] Karty tachografu musí odpovídat normě ISO/IEC 7810, *Identification cards – Physical characteristics,* [8] *Card characteristics,* [8.4] *Resistance to chemicals*	
		[Stabilita karet] Karty tachografu musí odpovídat normě ISO/IEC 7810, *Identification cards – Physical characteristics,* [8] *Card characteristics,* [8.5] *Card dimensional stability and warpage with temperature and humidity*	

Č.	Zkouška	Popis	Související požadavky
		[Odolnost proti světlu] Karty tachografu musí odpovídat normě ISO/IEC 7810, *Identification cards – Physical characteristics,* [8] *Card characteristics,* [8.6] *Light*	
		[Trvanlivost] Příloha 1C, kapitola 4.4 „Environmentální a elektrické specifikace“, 241) Karty tachografu musí být schopny správné funkce po dobu pěti let, pokud jsou používány ve shodě s předepsanými environmentálními a elektrickými specifikacemi.	
		[Odolnost proti loupání] Karty tachografu musí odpovídat normě ISO/IEC 7810, *Identification cards – Physical characteristics,* [8] *Card characteristics,* [8.8] *Peel strength*	
		[Adheze nebo vytváření bloků] Karty tachografu musí odpovídat normě ISO/IEC 7810, *Identification cards – Physical characteristics,* [8] *Card characteristics,* [8.9] *Adhesion or blocking*	
		[Průhyb] Karty tachografu musí odpovídat normě ISO/IEC 7810, *Identification cards – Physical characteristics,* [8] *Card characteristics,* [8.11] *Overall card warpage*	
		[Odolnost proti teplu] Karty tachografu musí odpovídat normě ISO/IEC 7810, *Identification cards – Physical characteristics,* [8] *Card characteristics,* [8.12] *Resistance to heat*	

Č.	Zkouška	Popis	Související požadavky
		[Deformace povrchu] Karty tachografu musí odpovídat normě ISO/IEC 7810, *Identification cards – Physical characteristics,* [8] *Card characteristics,* [8.13] *Surface distortions*	
		[Kontaminace] Karty tachografu musí odpovídat normě ISO/IEC 7810, *Identification cards – Physical characteristics,* [8] *Card characteristics,* [8.14] *Contamination and interaction of card components*	
2.3	Mechanické zkoušky s vloženým čipovým modulem	[Ohyb] Karty tachografu musí odpovídat normě ISO/IEC 7810:2003/Amd. 1:2009, *Identification cards – Physical characteristics, Amendment 1: Criteria for cards containing integrated circuits* [9.2] *Dynamic bending stress* Celkový počet cyklů ohybu: 4 000.	ISO/IEC 7810
		[Torze] Karty tachografu musí odpovídat normě ISO/IEC 7810:2003/Amd. 1:2009, *Identification cards – Physical characteristics, Amendment 1: Criteria for cards containing integrated circuits* [9.3] *Dynamic torsional stress* Celkový počet cyklů torze: 4 000.	
3	**Modul**		
3.1	Modul	Modulem je pouzdro čipu a kontaktní destička. [Profil povrchu] Karty tachografu musí odpovídat normě ISO/IEC 7816-1:2011, *Identification cards – Integrated circuit cards – Part 1: Cards with contacts – Physical characteristics* [4.2] *Surface profile of contacts*	ISO/IEC 7816

Č.	Zkouška	Popis	Související požadavky
		[Mechanická odolnost] Karty tachografu musí odpovídat normě ISO/IEC 7816-1:2011, *Identification cards – Integrated circuit cards – Part 1: Cards with contacts – Physical characteristics* [4.3] *Mechanical strength (of a card and contacts)*	
		[Elektrický přechodový odpor] Karty tachografu musí odpovídat normě ISO/IEC 7816-1:2011, *Identification cards – Integrated circuit cards – Part 1: Cards with contacts – Physical characteristics* [4.4] *Electrical resistance (of contacts)*	
		[Rozměry] Karty tachografu musí odpovídat normě ISO/IEC 7816-2:2007, *Identification cards – Integrated circuit cards – Part 2: Cards with contacts – Dimension and location of the contacts* [3] *Dimension of the contacts*	
		[Umístění] Karty tachografu musí odpovídat normě ISO/IEC 7816-2:2007, *Identification cards – Integrated circuit cards – Part 2: Cards with contacts – Dimension and location of the contacts* [4] *Number and location of the contacts* V případě modulů se šesti kontakty nejsou součástí tohoto požadavku na zkoušení kontakty „C4“ a „C8“.	
4	**Čip**		
4.1	Čip	[Provozní teplota] Čip karty tachografu pracuje v rozsahu teplot okolí od – 25 °C do + 85 °C.	241 až 244 Předpis EHK č. 10 ISO/IEC 7810 ISO/IEC 10373

Č.	Zkouška	Popis	Související požadavky
		[Teplota a vlhkost] Příloha 1C, kapitola 4.4 „Environmentální a elektrické specifikace“, 241) Karty tachografu musí být schopny správné funkce za všech klimatických podmínek běžně se vyskytujících na území Společenství a nejméně v rozsahu teplot od – 25 °C do + 70 °C s příležitostnými špičkami do + 85 °C; „příležitostnými“ se rozumí doba nepřesahující 4 hodiny a ne více než sto opakování v průběhu životnosti karty. Karty tachografu jsou postupně po danou dobu vystaveny následujícím teplotám a vlhkostem. Po každém kroku se zkouší elektrická funkčnost karet tachografu. 1. Teplota – 20 °C po dobu 2 h. 2. Teplota +/– 0 °C po dobu 2 h. 3. Teplota + 20 °C a relativní vlhkost 50 % po dobu 2 h. 4. Teplota + 50 °C a relativní vlhkost 50 % po dobu 2 h. 5. Teplota + 70 °C a relativní vlhkost 50 % po dobu 2 h. Teplota je chvilkově zvyšována na + 85 °C při relativní vlhkosti 50 % RH po dobu 60 min. 6. Teplota + 70 °C a relativní vlhkost 85 % po dobu 2 h. Teplota je chvilkově zvyšována na + 85 °C při relativní vlhkosti 85 % RH po dobu 30 min.	
		[Vlhkost] Příloha 1C, kapitola 4.4 „Environmentální a elektrické specifikace“, 242) Karty tachografu musí být schopny správné funkce při vlhkosti v rozsahu 10 % až 90 %.	
		[Elektromagnetická kompatibilita – EMC] Příloha 1C, kapitola 4.4 „Environmentální a elektrické specifikace“, 244) Během provozu musí karty tachografu vyhovovat požadavkům předpisu EHK č. 10 ohledně elektromagnetické kompatibility.	

Č.	Zkouška	Popis	Související požadavky
		[Statická elektřina] Příloha 1C, kapitola 4.4 „Environmentální a elektrické specifikace“, 244) Během provozu jsou karty tachografu chráněny proti elektrostatickým výbojům. Karty tachografu musí odpovídat normě ISO/IEC 7810:2003/Amd. 1:2009, *Identification cards – Physical characteristics, Amendment 1: Criteria for cards containing integrated circuits* [9.4] *Static electricity* [9.4.1] *Contact IC cards* Zkušební napětí: 4 000 V.	
		[Rentgenové záření] Karty tachografu musí odpovídat normě ISO/IEC 7810:2003/Amd. 1:2009, *Identification cards – Physical characteristics, Amendment 1: Criteria for cards containing integrated circuits* [9.1] *X-rays*	
		[Ultrafialové světlo] ISO/IEC 10373-1:2006, *Identification cards – Test methods – Part 1: General characteristics* [5.11] *Ultraviolet light*	
		[Zkouška třemi koly] Karty tachografu musí odpovídat normě ISO/IEC 10373-1:2006/Amd. 1:2012, *Identification cards – Test methods – Part 1: General characteristics, Amendment 1* [5.22] *ICC – Mechanical strength: 3 wheel test for ICCs with contacts*	
		[Navíjení] Karty tachografu musí odpovídat normě MasterCard CQM V2.03:2013 [11.1.3] *R-L3-14-8: Wrapping Test Robustness* [13.2.1.32] *TM-422: Mechanical Reliability: Wrapping Test*	

Č.	Zkouška	Popis	Související požadavky
4.2	Mechanické zkoušky čipového modulu vloženého do těla karty -> stejné jako 2.3	[Ohyb] Karty tachografu musí odpovídat normě ISO/IEC 7810:2003/Amd. 1:2009, *Identification cards – Physical characteristics, Amendment 1: Criteria for cards containing integrated circuits* [9.2] *Dynamic bending stress* Celkový počet cyklů ohybu: 4 000. [Torze] Karty tachografu musí odpovídat normě ISO/IEC 7810:2003/Amd. 1:2009, *Identification cards – Physical characteristics, Amendment 1: Criteria for cards containing integrated circuits* [9.3] *Dynamic torsional stress* Celkový počet cyklů torze: 4 000.	ISO/IEC 7810
5	**Zkoušky protokolu**		
5.1	ATR	Ověřit, že ATR splňuje požadavky	ISO/IEC 7816-3 TCS_14, TCS_17, TCS_18
5.2	T=0	Ověřit, že protokol T=0 splňuje požadavky	ISO/IEC 7816-3 TCS_11, TCS_12, TCS_13, TCS_15
5.3	PTS	Ověřit, že příkaz PTS splňuje požadavky, změnou na T=1 z T=0	ISO/IEC 7816-3 TCS_12, TCS_19, TCS_20, TCS_21
5.4	T=1	Ověřit, že protokol T=1 splňuje požadavky	ISO/IEC 7816-3 TCS_11, TCS_13, TCS_16
6	**Struktura karty**		
6.1		Ověřit, že struktura souborů karty splňuje požadavky, kontrolou přítomnosti povinných souborů na kartě a podmínek přístupu k nim	TCS_22 až TCS_28 TCS_140 až TCS_179
7	**Funkční zkoušky**		
7.1	Normální zpracování	Nejméně jednou přezkoušet každé povolené použití každého příkazu (např.: přezkoušet příkaz UPDATE BINARY s CLA = '00', s CLA = '0C' a s různými parametry P1, P2 a Lc). Zkontrolovat, zda operace byly na kartě skutečně provedeny (např. čtením souboru, na němž byl příkaz proveden).	TCS_29 až TCS_139

Č.	Zkouška	Popis	Související požadavky
7.2	Chybové zprávy	Pro každý příkaz nejméně jednou přezkoušet každou chybovou zprávu (podle specifikace v dodatku 2). Nejméně jednou přezkoušet každou obecnou chybu (kromě chyb integrity '**6400**' kontrolovaných během osvědčování bezpečnosti)	
7.3	Sada šifer a standardizované parametry domény		CSM_48, CSM_50
8	**Personalizace**		
8.1	Optická personalizace	Příloha 1C, kapitola 4.1 „Viditelné údaje", 230) Přední strana musí obsahovat: informace specifické pro vydávanou kartu. Příloha 1C, kapitola 4.1 „Viditelné údaje", 231) Přední strana musí obsahovat: data ve formátu „dd/mm/rrrr" nebo „dd.mm.rrrr" (den, měsíc, rok). Příloha 1C, kapitola 4.1 „Viditelné údaje", 235) Karty tachografu musí nést minimálně tyto ochranné prvky, které chrání tělo karty proti padělání a pozměňování: — v oblasti fotografie se musí překrývat bezpečnostní provedení pozadí a fotografie.	230, 231, 235

5. ZKOUŠKY VNĚJŠÍHO ZAŘÍZENÍ GNSS

Č.	Zkouška	Popis	Související požadavky
1.	**Administrativní šetření**		
1.1	Dokumentace	Správnost dokumentace	
2.	**Vizuální kontrola vnějšího zařízení GNSS**		
2.1.	Shoda s dokumentací		
2.2.	Identifikace/značení		224 až 226
2.3	Materiály		219 až 223
3.	**Funkční zkoušky**		
3.1	Identifikační údaje snímače		98,99
3.2	Vazba vnějšího modulu GNSS s celkem ve vozidle		123, 205

Č.	Zkouška	Popis	Související požadavky
3.3	Poloha dle GNSS		36, 37
3.4	Rozhraní celku ve vozidle, je-li přijímač GNSS vně celku ve vozidle		03
3.5	Sada šifer a standardizované parametry domény		CSM_48, CSM_50
4.	**Zkoušky vlivu 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: *Environmental testing – Part 2-1: Tests – Test A: Cold* 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: *Basic environmental testing procedures; part 2: tests; tests B: dry heat* Zkouška podle ISO 16750-4: *Chapter 5.3.2: Rapid change of temperature with specified transition duration* (– 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 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: *Chapter 4.1.2.8: Test VIII: Commercial vehicle, decoupled vehicle cab* Zkouška náhodnými vibracemi, 10…2 000 Hz, efektivní vertikální zrychlení 21,3 m/s², efektivní podélné zrychlení 11,8 m/s², efektivní příčné zrychlení 13,1 m/s², 3 osy, 32 h na osu, včetně teplotního cyklu – 20…70 °C. Tato zkouška odkazuje na IEC 60068-2-64: *Environmental testing – Part 2-64: Tests – Test Fh: Vibration, broadband random and guidance* 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 změn parametrů)	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, kapitola 4.3)	216
4.6	Ochrana proti záměně polarity	Ověřit, že celek ve vozidle vydrží přepólování napájecího napětí (ISO 16750-2, kapitola 4.7)	216
4.7	Ochrana proti zkratu	Ověřit, že vstupní a výstupní signály jsou chráněny proti zkratu vůči napájení a uzemnění (ISO 16750-2, kapitola 4.10)	216
5	**Zkoušky elektromagnetické kompatibility**		
5.1	Vyzařované emise a citlivost	Soulad s předpisem EHK č. 10	218

Č.	Zkouška	Popis	Související požadavky
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
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

6. ZKOUŠKY 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

Č.	Zkouška	Popis	Související požadavky
4.	**Zkoušky vlivu 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: *Environmental testing – Part 2-1: Tests – Test A: Cold* 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: *Basic environmental testing procedures; part 2: tests; tests B: dry heat* Zkouška podle ISO 16750-4: *Chapter 5.3.2: Rapid change of temperature with specified transition duration* (– 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 části 3 této tabulky).	213
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* (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
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	218

Č.	Zkouška	Popis	Související požadavky
		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.	

7. FUNKČNÍ ZKOUŠKY PAPÍRU

Č.	Zkouška	Popis	Související požadavky
1.	**Administrativní šetření**		
1.1	Dokumentace	Správnost dokumentace	
2	**Všeobecné zkoušky**		
2.1	Počet znaků na řádek	Vizuální kontrola výtisků.	172
2.2	Minimální velikost písma	Vizuální kontrola výtisku a kontrola znaků.	173
2.3	Podporované znakové sady	Tiskárna podporuje znaky specifikované v dodatku 1 kapitole 4 „Znakové sady“.	174
2.4	Definice výtisků	Kontrola schválení typu tachografu a vizuální kontrola výtisků	174
2.5	Čitelnost a identifikace výtisků	Kontrola výtisků Prokazuje se zkušebními zprávami a protokoly výrobce. Všechna čísla schválení tachografů, s kterými může být papír do tiskárny používán, jsou natištěna na papíru.	175, 177, 178
2.6	Doplnění rukopisných poznámek	Vizuální kontrola: je k dispozici pole pro podpis řidiče. Jsou k dispozici pole pro další rukopisné záznamy.	180

Č.	Zkouška	Popis	Související požadavky
2.7	Další podrobnosti na přední straně papíru	Přední a rubová strana papíru mohou nést další podrobnosti a informace. Tyto další podrobnosti a informace nesmí narušovat čitelnost výtisků. Vizuální kontrola.	177, 178
3	**Zkoušky skladování**		
3.1	Suché teplo	Aklimatizace před zkouškou: 16 hodin při + 23 °C ± 2 °C/ relativní vlhkosti 55 % ± 3 % Zkušební prostředí: 72 hodin při + 70 °C ± 2 °C Aklimatizace po zkoušce: 16 hodin při + 23 °C ± 2 °C/relativní vlhkosti 55 % ± 3 %	176, 178 IEC 60068-2-2-Bb
2.2	Vlhké teplo	Aklimatizace před zkouškou: 16 hodin při + 23 °C ± 2 °C/ relativní vlhkosti 55 % ± 3 % Zkušební prostředí: 144 hodin při + 55 °C ± 2 °C a rel. vlhkosti 93 % ± 3 % Aklimatizace po zkoušce: 16 hodin při + 23 °C ± 2 °C/relativní vlhkosti 55 % ± 3 %	176, 178 IEC 60068-2-78-Cab
4	**Provozní zkoušky papíru**		
4.1	Odolnost podkladu proti vlhkosti (nepotištěný papír)	Aklimatizace před zkouškou: 16 hodin při + 23 °C ± 2 °C/ relativní vlhkosti 55 % ± 3 % Zkušební prostředí: 144 hodin při + 55 °C ± 2 °C a rel. vlhkosti 93 % ± 3 % Aklimatizace po zkoušce: 16 hodin při + 23 °C ± 2 °C/relativní vlhkosti 55 % ± 3 %	176, 178 IEC 60068-2-78-Cab
4.2	Potiskovatelnost	Aklimatizace před zkouškou: 24 hodin při + 40 °C ± 2 °C/ relativní vlhkosti 93 % ± 3 % Zkušební prostředí: výtisk pořízen při + 23°C ± 2°C Aklimatizace po zkoušce: 16 hodin při + 23 °C ± 2 °C/relativní vlhkosti 55 % ± 3 %	176, 178
4.3	Odolnost proti teplu	Aklimatizace před zkouškou: 16 hodin při + 23 °C ± 2 °C/ relativní vlhkosti 55 % ± 3 % Zkušební prostředí: 2 hodiny při + 70 °C ± 2 °C, suché teplo Aklimatizace po zkoušce: 16 hodin při + 23 °C ± 2 °C/relativní vlhkosti 55 % ± 3 %	176, 178 IEC 60068-2-2-Bb
4.4	Odolnost proti nízké teplotě	Aklimatizace před zkouškou: 16 hodin při + 23 °C ± 2 °C/ relativní vlhkosti 55 % ± 3 % Zkušební prostředí: 24 hodin, – 20 °C ± 3°C, suchý chlad Aklimatizace po zkoušce: 16 hodin při + 23 °C ± 2 °C/relativní vlhkosti 55 % ± 3 %	176, 178 ISO 60068-2-1-Ab

Č.	Zkouška	Popis	Související požadavky
4.5	Odolnost proti světlu	Aklimatizace před zkouškou: 16 hodin při + 23 °C ± 2 °C/relativní vlhkosti 55 % ± 3 % Zkušební prostředí: 100 hodin při osvětlení 5 000 Lux při + 23 °C ± 2 °C/relativní vlhkosti 55 % ± 3 % Aklimatizace po zkoušce: 16 hodin při + 23 °C ± 2 °C/relativní vlhkosti 55 % ± 3 %	176, 178

Kritéria čitelnosti pro zkoušky 3.x a 4.x:

Čitelnost tisku je zaručena, pokud optické hustoty odpovídají těmto mezním hodnotám:

tištěné znaky: min. 1,0,

podklad (nepotištěný papír): max. 0,2.

Optické hustoty výsledných výtisků se měří podle normy DIN EN ISO 534.

Výtisky nevykazují žádné rozměrové změny a zůstávají jasně čitelné.

8. ZKOUŠKY INTEROPERABILITY

Č.	Zkouška	Popis
		9.1 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 nejvíce elementárních souborů na kartě. Ověřit stažením pomocí celku ve vozidle, že všechny příslušné záznamy byly řádně provedeny. Ověřit stažením dat z karty, že všechny příslušné záznamy byly řádně provedeny. Ověřit pomocí denních výtisků, že všechny záznamy lze řádně číst.
		9.2 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 nejvíce událostí nebo závad. Ověřit stažením pomocí celku ve vozidle, že všechny příslušné záznamy byly řádně provedeny. Ověřit stažením dat z karty, že všechny příslušné záznamy byly řádně provedeny. Ověřit pomocí denního výtisku, že všechny záznamy lze řádně číst.

Č.	Zkouška	Popis
9.3 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 nejvíce událostí nebo závad. Ověřit stažením pomocí celku ve vozidle, že všechny příslušné záznamy byly řádně provedeny. Ověřit stažením dat z karty, že všechny příslušné záznamy byly řádně provedeny. Ověřit pomocí denního výtisku, že všechny záznamy lze řádně číst.

Dodatek 10

BEZPEČNOSTNÍ POŽADAVKY

Tento dodatek specifikuje bezpečnostní požadavky v oblasti informačních technologií na součásti systémů inteligentních tachografů (tachografů druhé generace).

SEC_001 Z hlediska bezpečnosti musí být podle režimu *Common Criteria* certifikovány tyto součásti systémů inteligentních tachografů:

— celek ve vozidle,

— karta tachografu,

— snímač pohybu,

— vnější zařízení GNSS.

SEC_002 Minimální bezpečnostní požadavky v oblasti informačních technologií, které musí každá součást vyžadující certifikaci z hlediska bezpečnosti splňovat, musí být podle režimu *Common Criteria* vymezeny v profilu ochrany součásti.

SEC_003 Evropská komise zajistí, aby čtyři profily ochrany, jež splňují podmínky této přílohy, byly podporovány, vyvíjeny, schváleny vládními orgány pro certifikaci bezpečnosti v oblasti informačních technologií vytvořenými v rámci společné interpretační pracovní skupiny, která podporuje vzájemné uznávání osvědčení v rámci dohody o vzájemném uznávání osvědčení o posouzení bezpečnosti informačních technologií Evropského Poradního výboru pro bezpečnost informačních systémů (SOG-IS MRA), a registrovány:

— profil ochrany celku ve vozidle,

— profil ochrany karty tachografu,

— profil ochrany snímače pohybu,

— profil ochrany vnějšího zařízení GNSS.

Profil ochrany celku ve vozidle se zabývá případy, kdy je celek ve vozidle určen k tomu, aby byl, nebo nebyl používán s vnějším zařízením GNSS. V prvním případě jsou bezpečnostní požadavky na vnější zařízení GNSS uvedeny v samostatném profilu ochrany.

SEC_004 Výrobci součástí musí dle potřeby upřesnit a doplnit profil ochrany příslušné součásti, aniž by pozměnili nebo odstranili stávající hrozby, cíle, postupy a specifikace funkcí zajišťujících bezpečnost, za účelem stanovení bezpečnostního cíle, podle kterého budou požadovat bezpečnostní certifikaci součásti.

SEC_005 V průběhu hodnocení musí být konstatováno přísné dodržení uvedeného bezpečnostního cíle s odpovídajícími profilem ochrany.

SEC_006 Stupeň záruky pro každý profil ochrany musí být EAL4 rozšířený o složky záruky ATE_DPT.2 a AVA_VAN.5.

Dodatek 11

SPOLEČNÉ BEZPEČNOSTNÍ MECHANISMY

OBSAH

PREAMBULE

Tento dodatek stanovuje bezpečnostní mechanismy, které zajišťují

— vzájemné ověřování pravosti mezi různými součástmi systému tachografu,

— důvěrnost, integritu, ověřování pravosti a/nebo nepopiratelnost dat přenášených mezi různými součástmi systému tachografu nebo stahovaných do externích paměťových médií.

Tento dodatek obsahuje dvě části. Část A stanovuje bezpečnostní mechanismy pro systém tachografu první generace (digitální tachograf). Část B stanovuje bezpečnostní mechanismy pro systém digitálního tachografu druhé generace (inteligentní tachograf).

Mechanismy stanovené v části A tohoto dodatku platí, pokud alespoň jedna součást systému tachografu pro proces vzájemného ověřování pravosti a/nebo přenosu dat je zařízením první generace.

Mechanismy stanovené v části B tohoto dodatku platí, pokud obě součásti systému tachografu pro proces vzájemného ověřování pravosti a/nebo přenosu dat jsou zařízením druhé generace.

Dodatek 15 uvádí další informace týkající se používání součástí první generace ve spojení se součástmi druhé generace.

ČÁST A

SYSTÉM TACHOGRAFU PRVNÍ GENERACE

1. ÚVOD

1.1. **Zdroje**

V tomto dodatku jsou použity tyto zdroje:

SHA-1	National Institute of Standards and Technology (NIST). *FIPS Publication 180-1: Secure Hash Standard*. Duben 1995.
PKCS1	RSA Laboratories. PKCS # 1: *RSA Encryption Standard*. Verze 2.0. Říjen 1998.
TDES	National Institute of Standards and Technology (NIST). *FIPS Publication 46-3: Data Encryption Standard*. Návrh 1999.
TDES-OP	ANSI X9.52, Triple Data Encryption Algorithm Modes of Operation. 1998.
ISO/IEC 7816-4	Information Technology – Identification cards – Integrated circuit(s) cards with contacts (Informační technologie – Identifikační karty – Karty s integrovanými obvody a s kontakty) Část 4: Interindustry commands for interexchange (Mezioborové příkazy pro výměnu). První vydání: 1995 + Změna 1: 1997.
ISO/IEC 7816-6	Information Technology – Identification cards – Integrated circuit(s) cards with contacts (Informační technologie – Identifikační karty – Karty s integrovanými obvody a s kontakty) Část 6: Interindustry data elements (Mezioborové datové prvky). První vydání: 1996 + Oprava 1: 1998.
ISO/IEC 7816-8	Information Technology – Identification cards – Integrated circuit(s) cards with contacts (Informační technologie – Identifikační karty – Karty s integrovanými obvody a s kontakty) Část 8: Security related interindustry commands (Mezioborové příkazy pro bezpečnost). První vydání 1999.
ISO/IEC 9796-2	Information Technology – Security techniques – Digital signature schemes giving message recovery (Informační technologie – Bezpečnostní techniky – Schémata digitálního podpisu umožňující obnovu zprávy) – Část 2: Mechanisms using a hash function (Mechanismy využívající hašovací funkci). První vydání: 1997.
ISO/IEC 9798-3	Information Technology – Security techniques – Entity authentication mechanisms (Informační technologie – Bezpečnostní techniky – Mechanismy autentizace entit) – Část 3: Entity authentication using a public key algorithm (Autentizace entit používající algoritmus s veřejným klíčem). Druhé vydání: 1998.
ISO 16844-3	Road vehicles – Tachograph systems (Silniční vozidla – Systémy tachografů) – Část 3: Motion sensor interface (Rozhraní snímače pohybu).

1.2. **Značení a zkratky**

V tomto dodatku jsou užity následující značení a zkratky:

(K_a, K_b, K_c)	balíček klíčů pro užití trojitého algoritmu šifrování dat,
CA	certifikační autorita,
CAR	odkaz na certifikační autoritu,
CC	kryptografický kontrolní součet,
CG	kryptogram,
CH	hlavička příkazu,
CHA	autorizace držitele certifikátu,
CHR	odkaz na držitele certifikátu,
D()	dešifrování pomocí standardu pro výměnu dat DES,

DE	prvek dat,
DO	datový objekt,
d	soukromý klíč RSA, soukromý zmocněnec,
e	veřejný klíč RSA, veřejný zmocněnec,
E()	šifrování pomocí DES,
EQT	zařízení,
Hash()	hašovací hodnota, výstup hodnoty *Hash*,
Hash	hašovací funkce,
KID	identifikátor klíče,
Km	klíč TDES. Hlavní klíč podle definice ISO 16844-3,
Km_{VU}	klíč TDES vložený do celku ve vozidle,
Km_{WC}	klíč TDES, vložený do karty dílny,
m	celé číslo mezi 0 a *n*-1 reprezentující zprávu,
n	klíče RSA, modul,
PB	doplňkové bajty,
PI	indikační bajt doplnění (užití v šifře pro důvěrnost DO),
PV	otevřená hodnota,
s	celé číslo mezi 0 a *n*-1 reprezentující podpis,
SSC	čítač odeslané posloupnosti,
SM	bezpečné zpracování zpráv,
TCBC	TDEA blok číslic svazující provozní režimy,
TDEA	trojitý algoritmus šifrování dat,
TLV	hodnota délky tagu,
VU	celek ve vozidle,
X.C	certifikát uživatele X vydaný certifikační autoritou,
X.CA	certifikační autorita uživatele X,
X.CA.PK $_o$ X.C	operace rozbalení certifikátu pro extrakci veřejného klíče. Je to zaváděcí operátor, jehož levý operand je veřejným klíčem certifikační autority a jehož pravý operand je certifikátem vydaným certifikační autoritou. Výstupem je veřejný klíč uživatele X, jehož certifikát je pravým operandem,
X.PK	RSA veřejný klíč uživatele X,
X.PK[I]	RSA zašifrování některých informací I při užití veřejného klíče uživatele X,
X.SK	RSA soukromý klíč uživatele X,
X.SK[I]	RSA zašifrování některých informací I při užití soukromého klíče uživatele X,
‘xx’	hexadecimální hodnota,
||	operátor řetězení.

2. KRYPTOGRAFICKÉ SYSTÉMY A ALGORITMY

2.1. **Kryptografické systémy**

CSM_001 VU a karty tachografu musí používat klasický kryptografický systém RSA veřejného klíče k tomu, aby vytvořily tyto bezpečnostní mechanismy:

— ověřování pravosti mezi VU a kartami,

— převod trojitých DES klíčů relací mezi VU a kartami tachografu,

— digitální podpis dat stažených z VU nebo karet tachografu do externích médií.

CSM_002 VU a karty tachografu musí užívat trojitý DES symetrický kryptografický systém k tomu, aby v průběhu výměny dat uživatele mezi VU a kartami tachografu vytvořily mechanismus pro udržení integrity dat a aby v příslušných případech zajistily důvěrnost výměny dat mezi VU a kartami tachografu.

2.2. **Kryptografické algoritmy**

2.2.1 *Algoritmus RSA*

CSM_003 Algoritmus RSA je plně definován těmito rovnicemi:

$$X.SK[m] = s = m^d \bmod n$$
$$X.PK[s] = m = s^e \bmod n$$

Obsažnější popis funkce RSA lze nalézt v odkazu [PKCS1]. Veřejný exponent e pro výpočet RSA je celé číslo mezi 3 a n-1 splňující podmínku gcd(e, lcm(p-1, q-1))=1.

2.2.2 *Hašovací algoritmus*

CSM_004 Mechanismus digitálního podpisu musí užívat hašovací algoritmus SHA-1 podle definice v odkazu [SHA-1].

2.2.3 *Algoritmus šifrování dat*

CSM_005 Algoritmus, založený na DES musí být užit v provozním režimu „Cipher Block Chaining“.

3. KLÍČE A CERTIFIKÁTY

3.1. **Generování a distribuce klíčů**

3.1.1 *Generování a distribuce klíčů RSA*

CSM_006 Klíče RSA musí být generovány prostřednictvím tří funkčních hierarchických úrovní:

— evropské úrovně,

— úrovně členských států,

— úrovně zařízení.

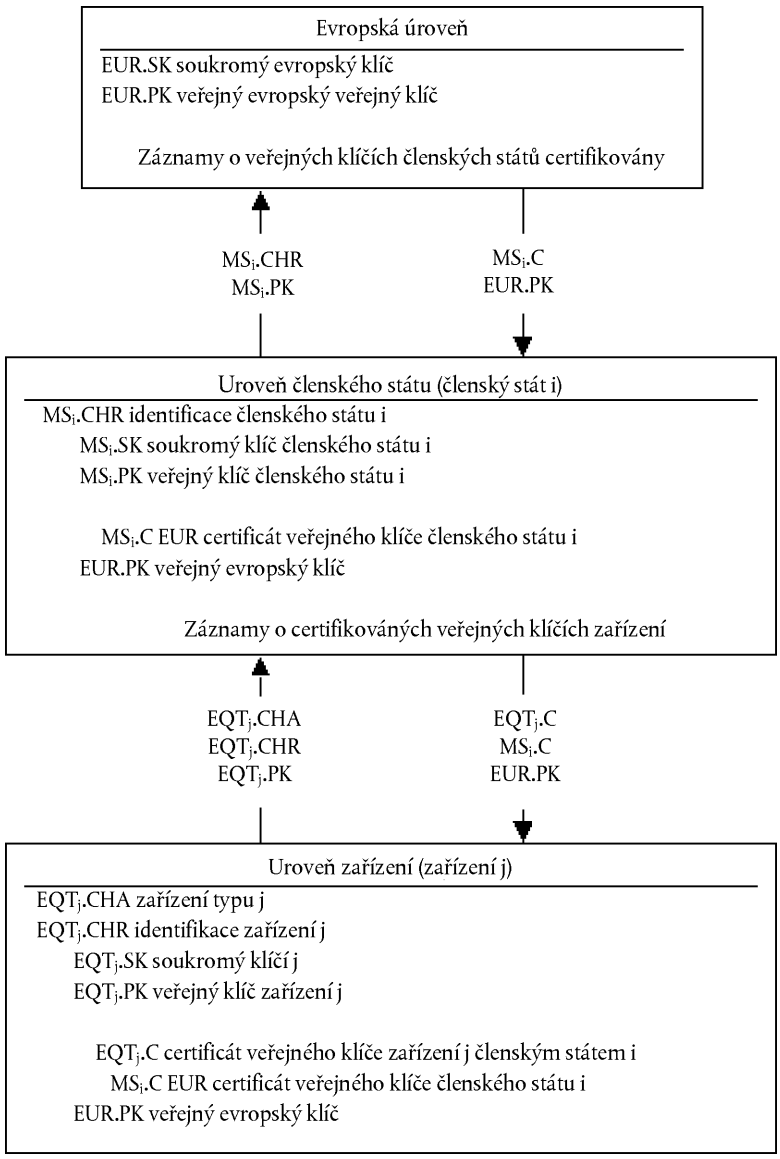
CSM_007 Na evropské úrovni musí být generován jediný pár evropských klíčů (EUR.SK a EUR.PK). K certifikaci veřejných klíčů členských států musí být používán evropský soukromý klíč. Musí být udržovány záznamy o všech certifikovaných klíčích. Tyto úkoly musí zajišťovat Evropský certifikační úřad pod pravomocí a odpovědností Evropské komise.

CSM_008 Na úrovni členského státu musí být generován pár klíčů členského státu (MS.SK a MS.PK). Veřejné klíče členských států musí být certifikovány Evropským certifikačním úřadem. Soukromý klíč členského státu se musí užívat k certifikaci veřejných klíčů, které se mají vkládat do zařízení (VU nebo karty tachografu). Musí být udržovány záznamy o všech certifikovaných veřejných klíčích spolu s identifikací zařízení, pro která jsou určeny. Tyto úkoly musí zajišťovat certifikační autorita členského státu. Členský stát může pravidelně svůj pár klíčů měnit.

CSM_009 Na úrovni zařízení musí být generován pár klíčů (EQT.SK a EQT.PK) a musí být vložen do každého zařízení. Veřejné klíče zařízení musí být certifikovány certifikační autoritou členského státu. Tyto úkoly mohou být zajišťovány výrobci zařízení, personalizátory zařízení nebo orgány členského státu. Tento pár klíčů se užívá pro ověřování pravosti, digitální podpis a šifrovací služby.

CSM_010 Během generování, dopravy (v příslušných případech) a skladování musí být zachována důvěrnost soukromých klíčů.

Toto vyobrazení shrnuje tok dat v tomto procesu:



3.1.2 *Zkušební klíče RSA*

CSM_011 Pro zkoušení zařízení (včetně zkoušek interoperability) musí Evropský certifikační úřad generovat odlišný jediný evropský pár zkušebních klíčů a nejméně dva páry zkušebních klíčů členských států, jejichž veřejné klíče musí být certifikovány soukromým evropským zkušebním klíčem. Výrobci musí do zařízení, které je podrobeno zkouškám schválení typu, vložit zkušební klíče certifikované jedním z těchto zkušebních klíčů členského státu.

3.1.3 *Klíče snímače pohybu*

Důvěrnost níže uvedených tří klíčů TDES musí být náležitě zachována v průběhu generování, dopravy (v příslušných případech) a skladování.

Na podporu vyhovění součástí tachografu normě ISO 16844 musí Evropský certifikační úřad a dále certifikační úřady členských států kromě toho zajistit následující:

CSM_036 Evropský certifikační úřad musí generovat KmVU a KmWC, dva nezávislé a jedinečné klíče Triple TDES, a generovat Km jako: $Km = Km_{VU}$ XOR Km_{WC}. Evropský certifikační úřad musí tyto klíče za příslušných zabezpečených postupů předat na vyžádání členských států jejich certifikačním autoritám.

CSM_037 Certifikační autority členských států musí:

— užít Km k šifrování dat snímače pohybu podle požadavku výrobce snímače pohybu (data, která mají být šifrována pomocí Km, definuje ISO 16844-3),

— předat Km_{VU} výrobcům VU pro vložení do VU za náležitě zabezpečených postupů,

— zajistit, aby Km_{WC} bylo v průběhu personalizace karty vloženo do všech karet dílny (`SensorInstallationSecData` do elementárního souboru `Sensor_Installation_Data`).

3.1.4 *Generování a distribuce klíčů T-DES*

CSM_012 VU a karty tachografu musí jako součást postupu vzájemného ověřování pravosti generovat a vzájemně si vyměňovat data potřebná pro vypracování společného klíče Triple DES. Důvěrnost této výměny dat musí být ochráněna šifrovacím mechanismem RSA.

CSM_013 Tento klíč musí být použit u všech následujících kryptografických operací za použití zabezpečené komunikace. Jeho platnost končí ukončením relace (vyjmutím karty nebo resetováním karty) a/nebo po 240 použitích (jedno použití klíče = jeden příkaz s využitím zabezpečené komunikace odeslaný na kartu a odpovídající odpověď).

3.2. **Klíče**

CSM_014 Klíče RSA musí mít (na kterékoliv úrovni) následující délku: modul *n* 1 024 bitů, veřejný exponent *e* 64 bitů maximálně, soukromý exponent *d* 1 024 bitů.

CSM_015 Klíče Triple DES musí mít tvar (K_a, K_b, K_a), kde K_a a K_b jsou nezávislé klíče dlouhé 64 bitů. Nenastavují se žádné bity pro detekci závad v paritě.

3.3. **Certifikáty**

CSM_016 Certifikáty RSA veřejných klíčů musí být certifikáty „*non self-descriptive*“ (nepopisné) „*card verifiable*“ (ověřující kartu) (viz ISO/IEC 7816-8)

3.3.1 *Obsah certifikátů*

CSM_017 Certifikáty veřejných klíčů RSA jsou tvořeny těmito daty v následujícím pořadí:

Data	Formát	Bajtů	Popis
CPI	INTEGER (celé číslo)	1	Identifikátor profilu certifikátu (pro tuto verzi '01')
CAR	OCTET STRING	8	Odkaz na certifikační autoritu
CHA	OCTET STRING	7	Autorizace držitele certifikátu
EOV	TimeReal	4	Konec platnosti certifikátu. Volitelné, doplněno pomocí 'FF' pokud se nepoužije.
CHR	OCTET STRING	8	Odkaz na držitele certifikátu
n	OCTET STRING	128	Veřejný klíč (modul)
e	OCTET STRING	8	Veřejný klíč (veřejný exponent)
		164	

Poznámky:

1. „Identifikátor profilu certifikátu" (CPI) stanovuje přesnou strukturu certifikátu ověření pravosti. Může být užit jako interní identifikátor zařízení pro odpovídající návěští, které popisuje řetězení prvků dat v certifikátu.

   Návěští spojené s obsahem tohoto certifikátu je následující:

'4D'	'16'	'5F 29'	'01'	'42'	'08'	'5F 4B'	'07'	'5F 24'	'04'	'5F 20'	'08'	'7F 49'	'05'	'81'	'81 80'	'82'	'08'
Tag rozšířeného návěští	Délka návěští	Tag CPI	Délka CPI	Tag CAR	Délka CAR	Tag CHA	Délka CHA	Tag EOV	Délka EOV	Tag CHR	Délka CHR	Tag veřejného klíče (sestaveného)	Délka následujících DO	Tag modulu	Délka modulu	Tag veřejného exponentu	Délka veřejného exponentu

2. „Odkaz na certifikační autoritu" (CAR) má za účel identifikovat autoritu vydávající certifikát (CA) tak, aby prvek dat mohl být použit současně jako identifikátor klíče autority pro odkaz na veřejný klíč certifikační autority (pro kódování viz níže identifikátor klíče).

3. „Autorizace držitele certifikátu“ (CHA) se používá k identifikaci práv držitele certifikátu. Je tvořena identifikací (ID) použití tachografu a typem zařízení, ke kterému je certifikát určen (podle prvku dat `EquipmentType`, „00“ pro členský stát).

4. „Odkaz na držitele certifikátu“ (CHR) má za účel jednoznačně identifikovat držitele certifikátu tak, aby mohl být užit prvek dat současně jako identifikátor klíče subjektu a odkazovat na veřejný klíč držitele certifikátu.

5. Identifikátory klíčů jednoznačně identifikují držitele certifikátu nebo certifikační autority. Jsou kódovány takto:

5.1 Zařízení (VU nebo karta):

Data	Výrobní číslo zařízení	Datum	Typ	Výrobce
Délka	4 bajty	2 bajty	1 bajt	1 bajt
Hodnota	Integer (celé číslo)	Kódování BCD mm rr	Specifické podle výrobce	Kód výrobce

Při požadování certifikátů pro VU výrobce může, nebo nemusí znát identifikaci zařízení, do kterého budou klíče vloženy.

V prvém případě zašle výrobce identifikaci zařízení s veřejným klíčem autoritě svého členského státu k certifikaci. Certifikát bude v takovém případě zahrnovat identifikaci zařízení a výrobce musí zajistit, aby klíče a certifikáty byly vloženy do uvažovaného zařízení. Identifikátor klíče má tvar uvedený výše.

Ve druhém případě musí výrobce jednoznačně identifikovat každý požadavek na certifikát a zaslat tuto identifikaci s veřejným klíčem autoritě svého členského státu k certifikaci. Certifikát bude obsahovat identifikaci požadavku. Výrobce musí po instalaci klíče do zařízení sdělit orgánu svého členského státu přiřazení klíče k zařízení (tj. identifikaci požadavku na certifikát, identifikaci zařízení). Identifikátor klíče má následující tvar:

Data	Pořadové číslo požadavku na certifikát	Datum	Typ	Výrobce
Délka	4 bajty	2 bajty	1 bajt	1 bajt
Hodnota	Integer (celé číslo)	Kódování BCD mm rr	‘FF’	Kód výrobce

5.2 Certifikační autorita:

Data	Identifikace orgánu	Pořadové číslo klíče	Přídavné informace	Identifikátor
Délka	4 bajty	1 bajt	2 bajty	1 bajt

Hodnota	1 bajt číselný kód státu 3 bajty alfanumerický kód státu	Integer (celé číslo)	Doplňující kódování (specifické pro CA) 'FF FF', pokud se nevyužije	'01'

Pořadové číslo klíče se užívá pro rozlišení různých klíčů členského státu v případě, kdy je klíč měněn.

6. Ověřovatel certifikátu musí bezpodmínečně vědět, že veřejný certifikovaný klíč je RSA klíč platný pro ověřování pravosti, ověřování digitálního podpisu a šifrování pro důvěrnost služeb (certifikát nezahrnuje žádný identifikátor objektu, který jej specifikuje).

3.3.2 *Vydané certifikáty*

CSM_018 Vydaný certifikát je digitálním podpisem s částečnou obnovou obsahu certifikátu podle ISO/IEC 9796-2 (s výjimkou přílohy A4), s připojeným „Certification Authority Reference" (Odkaz na certifikační autoritu).

$$X.C = X.CA.SK['6A' \,||\, C_r \,||\, \mathit{Hash}(Cc) \,||\, 'BC'] \,||\, C_n \,||\, X.CAR$$

Kde je obsah certifikátu = Cc = C_r || C_n

106 bajtů 58 bajtů

Poznámky:

1. Tento certifikát je dlouhý 194 bajtů.

2. K podpisu je dále připojen podpisem překrytý odkaz na certifikační autoritu (CAR) tak, že veřejný klíč certifikačního orgánu může být vybrán pro ověření certifikátu.

3. Ověřovatel certifikátu musí bezpodmínečně znát algoritmus užívaný certifikační autoritou k podepisování certifikátu.

4. Návěští spojené s vydaným certifikátem je následující:

'7F 21'	'09'	'5F 37'	'81 80'	'5F 38'	'3A'	'42'	'08'
Tag certifikátu CV (sestaveného)	Délka následujících DO	Tag podpisu	Délka podpisu	Tag zbytku	Délka zbytku	Tag CAR	Délka CAR

3.3.3 *Ověření a rozbalení certifikátu*

Ověření a rozbalení certifikátů zahrnuje ověření podpisu podle ISO/IEC 9796-2, vyhledání obsahu certifikátu a obsaženého veřejného klíče: X.PK = X.CA.PK $_{o}$ X.C, a ověření platnosti certifikátu.

CSM_019 Zahrnuje následující kroky:

Ověřte podpis a vyvolejte obsah:

— z X.C vyvolejte Sign, C_n' a CAR': X.C = Sign || C_n' || CAR'

128 bajtů 58 bajtů 8 bajtů

— z CAR' vyberte příslušný veřejný klíč certifikační autority (pokud již nebyl vybrán dříve jinými prostředky),

— otevřete Sign pomocí veřejného klíče CA: Sr'= X.CA.PK [Sign],

— ověření Sr'začíná na '6A'a končí na 'BC',

— vypočítejte C_r' a H'ze vztahu: Sr' = '6A' || C_r' || H' || 'BC'

106 bajtů 20 bajtů

— obnovte obsah certifikátu C' = C_r' || C_n',

— ověřte *Hash*(C') = H'

Pokud jsou ověření v pořádku, je certifikát pravý a jeho obsahem je C'.

Ověřte platnost. Z C':

— v příslušných případech ověřte datum ukončení platnosti.

Z C' vyvolejte a uložte veřejný klíč, identifikátor klíče, autorizaci držitele certifikátu a konec platnosti certifikátu:

— X.PK = *n* || *e*

— X.KID = CHR

— X.CHA = CHA

— X.EOV = EOV

4. MECHANISMUS VZÁJEMNÉHO OVĚŘOVÁNÍ PRAVOSTI

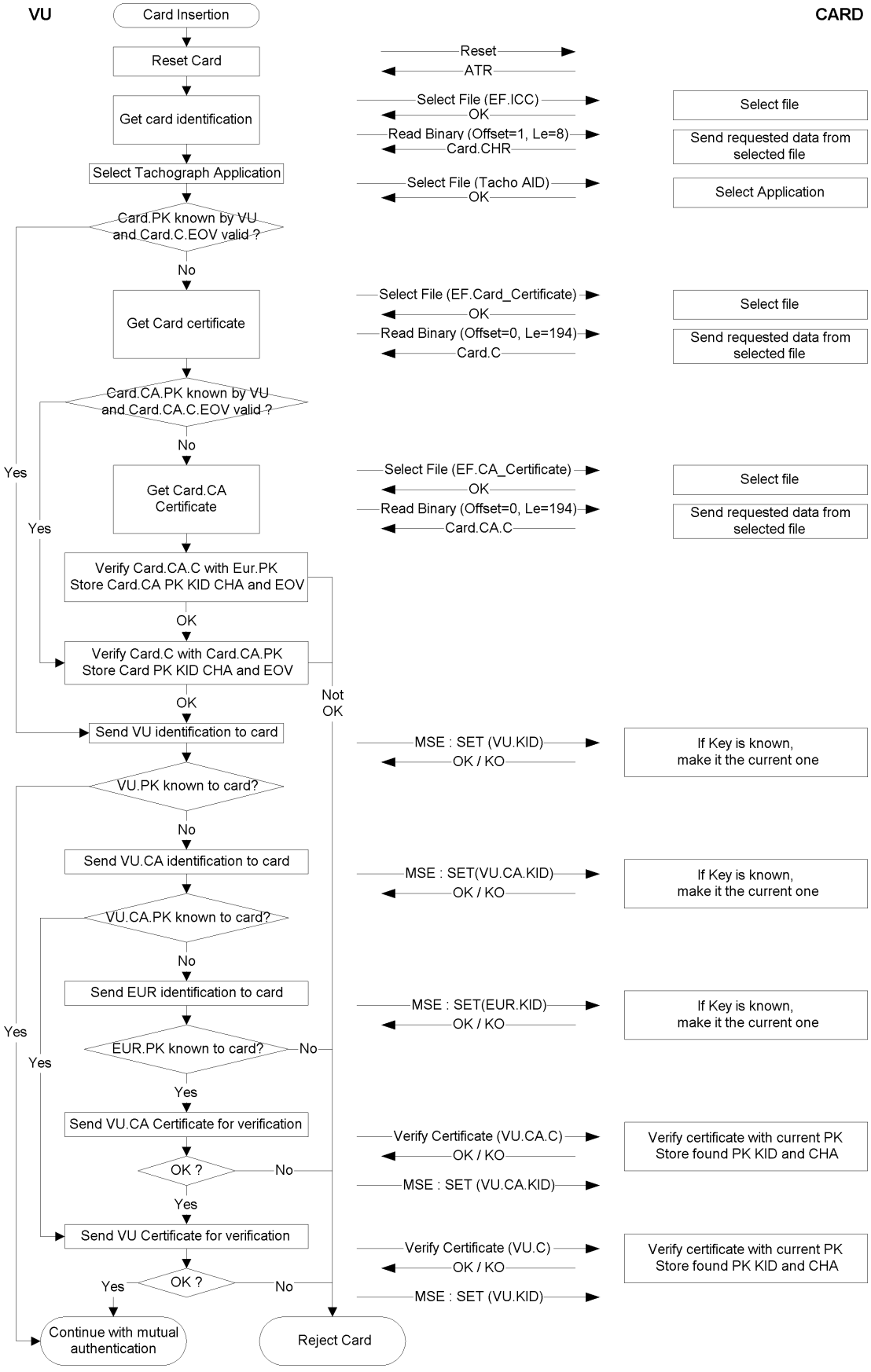
Vzájemné ověřování pravosti mezi kartami a VU je založeno na následujícím principu:

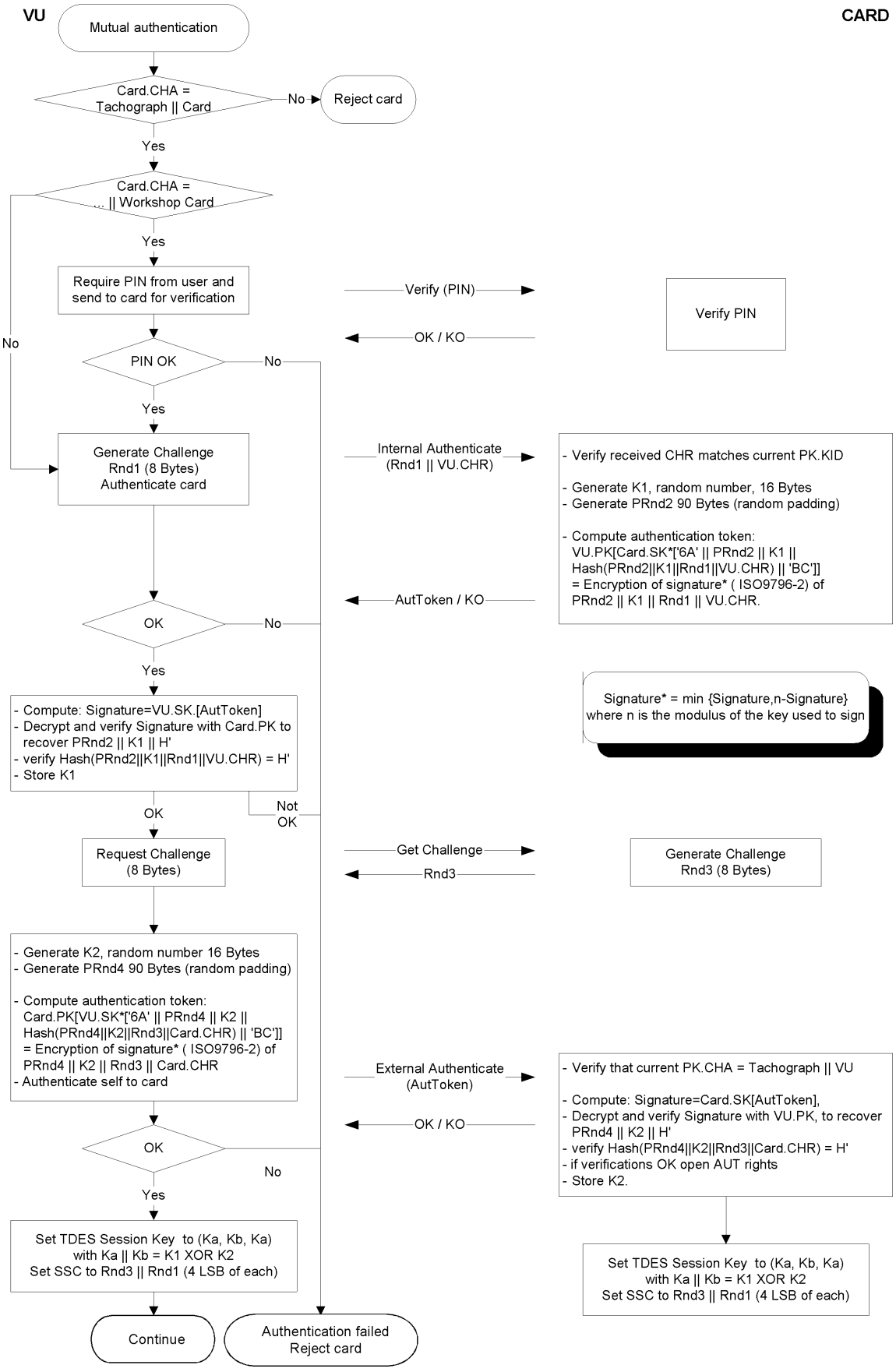
Každá strana musí druhé straně prokázat, že vlastní platný pár klíčů, z něhož veřejný klíč byl certifikován certifikační autoritou členského státu, která sama byla certifikována Evropským certifikačním úřadem.

Prokazuje se podpisem se soukromým klíčem na náhodně vybraném čísle zaslaném druhou stranou, která musí zaslané náhodné číslo při ověřování tohoto podpisu získat zpět.

Mechanismus se aktivuje vložením karty do VU. Mechanismus začíná výměnou certifikátů a rozbalením veřejných klíčů a končí nastavením klíče relace.

CSM_020 Musí být použit tento protokol (šipky označují příkazy a výměnu dat (viz dodatek 2)):




VU
CARD
Mutual authentication
Card.CHA = Tachograph || Card
No
Reject card
Yes
Card.CHA = ... || Workshop Card
Yes
No
Require PIN from user and send to card for verification
Verify (PIN)
Verify PIN
OK / KO
PIN OK
No
Yes
Generate Challenge Rnd1 (8 Bytes) Authenticate card
Internal Authenticate (Rnd1 || VU.CHR)
- Verify received CHR matches current PK.KID
- Generate K1, random number, 16 Bytes
- Generate PRnd2 90 Bytes (random padding)
- Compute authentication token: VU.PK[Card.SK*['6A' || PRnd2 || K1 || Hash(PRnd2||K1||Rnd1||VU.CHR) || 'BC']] = Encryption of signature* (ISO9796-2) of PRnd2 || K1 || Rnd1 || VU.CHR.
AutToken / KO
OK
No
Yes
Signature* = min {Signature,n-Signature} where n is the modulus of the key used to sign
- Compute: Signature=VU.SK.[AutToken]
- Decrypt and verify Signature with Card.PK to recover PRnd2 || K1 || H'
- verify Hash(PRnd2||K1||Rnd1||VU.CHR) = H'
- Store K1
Not OK
OK
Request Challenge (8 Bytes)
Get Challenge
Rnd3
Generate Challenge Rnd3 (8 Bytes)
- Generate K2, random number 16 Bytes
- Generate PRnd4 90 Bytes (random padding)
- Compute authentication token: Card.PK[VU.SK*['6A' || PRnd4 || K2 || Hash(PRnd4||K2||Rnd3||Card.CHR) || 'BC']] = Encryption of signature* (ISO9796-2) of PRnd4 || K2 || Rnd3 || Card.CHR
- Authenticate self to card
External Authenticate (AutToken)
- Verify that current PK.CHA = Tachograph || VU
- Compute: Signature=Card.SK[AutToken],
- Decrypt and verify Signature with VU.PK, to recover PRnd4 || K2 || H'
- verify Hash(PRnd4||K2||Rnd3||Card.CHR) = H'
- if verifications OK open AUT rights
- Store K2.
OK / KO
OK
No
Yes
Set TDES Session Key to (Ka, Kb, Ka) with Ka || Kb = K1 XOR K2
Set SSC to Rnd3 || Rnd1 (4 LSB of each)
Set TDES Session Key to (Ka, Kb, Ka) with Ka || Kb = K1 XOR K2
Set SSC to Rnd3 || Rnd1 (4 LSB of each)
Continue
Authentication failed Reject card

5. DŮVĚRNOST PŘENOSU DAT KARET VU, INTEGRITA A MECHANISMUS OVĚŘOVÁNÍ PRAVOSTI

5.1. **Bezpečné předávání zpráv**

CSM_021 Integrita přenosu dat VU karet musí být chráněna prostřednictvím bezpečného předávání zpráv s odkazem na normy [ISO/IEC 7816-4] a [ISO/IEC 7816-8].

CSM_022 Pokud je třeba data v průběhu přenosu chránit, musí se k datovým objektům zasílaným v příkazech nebo odpovědích připojit datový objekt kryptografický kontrolní součet (Cryptographic Checksum). Kryptografický kontrolní součet je kontrolován příjemcem.

CSM_023 Kryptografický kontrolní součet zaslaný v rámci příkazu musí zahrnovat záhlaví příkazu a veškeré odeslané datové objekty (=>CLA = '0C' a veškeré datové objekty musí být uzavřeny tagy, ve kterých b1=1).

CSM_024 Pokud odpověď neobsahuje datové pole, musí být stavové informační bajty ochráněny kryptografickým kontrolním součtem.

CSM_025 Kryptografický kontrolní součet musí být dlouhý čtyři bajty.

Struktura příkazů a odpovědí při použití bezpečného předávání zpráv je proto následující:

Užité objekty DO jsou částečné soubory bezpečného předávání zpráv datových objektů podle popisu v ISO/IEC 7816-4:

Tag	Symbol	Význam
'81'	T_{PV}	Otevřená hodnota, nikoliv kódovaná data BER-TLV (chráněno pomocí CC)
'97'	$\mathbf{T_{LE}}$	Hodnota Le v nechráněném příkazu (chráněno pomocí CC)
'99'	T_{SW}	Status-Info (chráněno pomocí CC)
'8E'	T_{CC}	Kryptografický kontrolní součet
'87'	$T_{PI\ CG}$	Bajtový indikátor naplnění || Kryptogram (otevřená hodnota nekódovaná v BER-TLV)

Z nechráněného páru odpovědi na příkaz vychází:

Záhlaví příkazu				Tělo příkazu		
CLA	INS	P1	P2	[L_c field]	[Data field]	[L_e field]
čtyři bajty				L bajty, označené jako B_1 až B_L		

Tělo odpovědi	Konec odpovědi	
[Data field]	SW1	SW2
L_r datové bajty	dva bajty	

Odpovídající pár zabezpečené odpovědi na příkaz:

Zabezpečený příkaz:

Záhlaví příkazu (CH)				Tělo příkazu										
CLA	INS	P1	P2	[New L_c field]	[New Data field]									[New L_e field]
'OC'				Délka New Data field	T_{PV}	L_{PV}	PV	T_{LE}	L_{LE}	L_e	T_{CC}	L_{CC}	CC	'00'
					'81'	L_c	Datové pole	'97'	'01'	L_e	'8E'	'04'	CC	

Data, která mají být zahrnuta do kontrolního součtu = CH || PB || T_{PV} || L_{PV} || PV || T_{LE} || L_{LE} || L_e || PB

PB = doplňkové bajty (80 .. 00) podle ISO-IEC 7816-4 a ISO 9797 metoda 2.

PV a LE z objektů DO jsou přítomny pouze tehdy, pokud jsou odpovídající data umístěna v nezabezpečeném příkazu.

Zabezpečená odpověď:

1. Případ, kdy datové pole odpovědi není prázdné a nepotřebuje být chráněno na důvěrnost:

Tělo odpovědi						Konec odpovědi
[New Data field]						Nové SW1 SW2
T_{PV}	L_{PV}	PV	T_{CC}	L_{CC}	CC	
'81'	L_r	Datové pole	'8E'	'04'	CC	

Data, která mají být zahrnuta do kontrolního součtu = T_{PV} || L_{PV} || PV || PB

2. Případ, kdy datové pole odpovědi není prázdné a potřebuje být chráněno na důvěrnost:

Tělo odpovědi						Konec odpovědi
[New Data field]						Nové SW1 SW2
$T_{PI\ CG}$	$L_{PI\ CG}$	PI CG	T_{CC}	L_{CC}	CC	
'87'		PI || CG	'8E'	'04'	CC	

Data v CG: nekódovaná data BER-TLV a bajty doplnění.

Data, která mají být zahrnuta do kontrolního součtu = $T_{PI\ CG}$ || $L_{PI\ CG}$ || PI CG || PB

3. Případ, kdy je datové pole odpovědi prázdné:

Tělo odpovědi						Konec odpovědi
[New Data field]						nové SW1 SW2
T_{SW}	L_{SW}	SW	T_{CC}	L_{CC}	CC	
'99'	'02'	Nové SW1 SW2	'8E'	'04'	CC	

Data, která mají být zahrnuta do kontrolního součtu = T_{SW} || L_{SW} || SW || PB

5.2. Zacházení s chybami v bezpečném předávání zpráv (SM)

CSM_026 Když karta tachografu při interpretaci příkazu zjistí chybu SM, pak se bajty statusu musí vrátit bez SM. Podle ISO/IEC 7816-4 jsou pro indikaci chyb SM definovány následující bajty statusu:

'66 88' selhalo ověření kryptografického kontrolního součtu,

'69 87' chybí očekávané datové objekty SM,

'69 88' datové objekty SM nesprávné.

CSM_027 Pokud karta tachografu vrátí bajty statusu bez SM DO nebo s chybným SM DO, musí VU relaci přerušit.

5.3. Algoritmus výpočtu kryptografického kontrolního součtu

CSM_028 Kryptografické kontrolní součty jsou tvořeny užitím obvyklého MAC podle ANSI X.9.19 s DES:

— Výchozí stav: výchozím zkušebním blokem y0 je E(Ka, SSC).

— Následující krok: Kontrolní bloky y1, .., yn se vypočtou pomocí Ka.

— Konečný krok: kryptografický kontrolní součet se vypočte z posledního zkušebního bloku yn takto: E(Ka, D(Kb, yn)).

kde E() znamená šifrování s DES a D() znamená rozšifrování s DES.

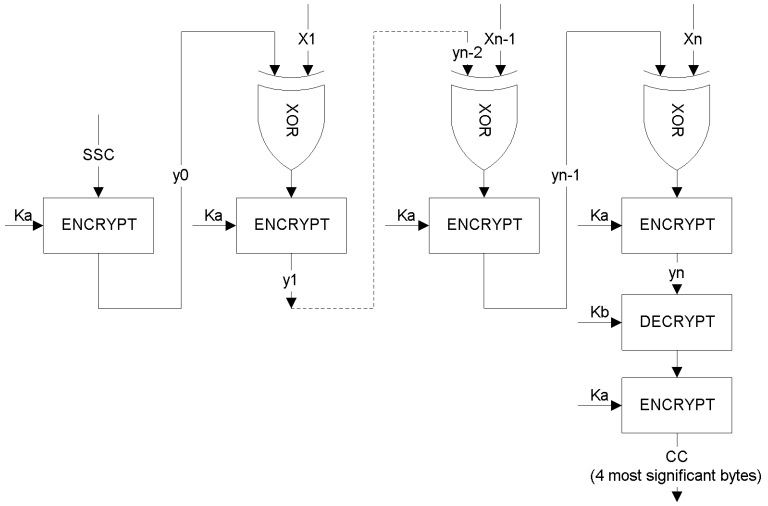
Přenášejí se čtyři nejvýznamnější bajty kryptografického kontrolního součtu.

CSM_029 V průběhu odsouhlasení klíče se „čítač odeslané posloupnosti" (SSC) inicializuje takto:

Výchozí SSC: Rnd3 (4 nejméně významné bajty) || Rnd1 (4 nejméně významné bajty).

CSM_030 Na čítači odeslané posloupnosti se hodnota zvýší o 1 před každým výpočtem MAC (tj. SSC pro první příkaz je výchozí SSC + 1, SSC pro prvou odpověď je výchozí SSC + 2).

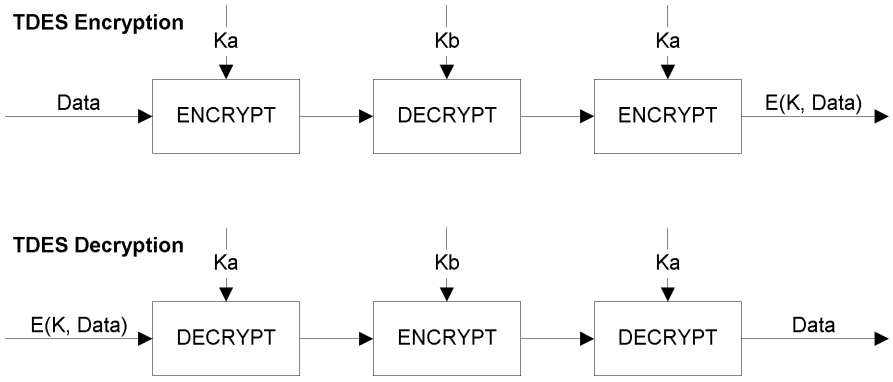
Následující vyobrazení uvádí výpočet retail MAC:



5.4. **Algoritmus výpočtu šifer pro důvěrnost objektů DO**

CSM_031 Kryptogramy se vypočtou pomocí TDEA v režimu TCBC podle odkazů [TDES] a [TDES-OP] spolu s nulovým vektorem jako výchozí blok hodnot.

Toto vyobrazení uvádí využití klíčů v TDES:



6. MECHANISMY DIGITÁLNÍCH PODPISŮ PŘI STAHOVÁNÍ DAT

CSM_032 Inteligentní vyhrazené zařízení (IDE) ukládá data ze zařízení (VU nebo karty) v průběhu relace stahování do jednoho fyzického souboru dat. Tento soubor musí zahrnovat certifikáty MS_i.C a EQT.C. Soubor obsahuje digitální podpisy datových bloků podle specifikace doplňku 7 – Protokoly stahování dat.

CSM_033 Digitální podpisy stažených dat musí užívat schéma digitálního podpisu s dodatkem tak, aby stažená data mohla být v případě požadavku čtena bez jakéhokoliv dešifrování.

6.1. **Generování podpisu**

CSM_034 Generování dat podpisu zařízením probíhá podle schématu podpisu s dodatkem definovaného v odkazu [PKCS1] s hašovací funkcí SHA-1:

Podpis = EQT.SK[‘00’ || ‘01’ || *PS* || ‘00’ || DER(SHA-1(Data))]

PS = doplňkový řetězec oktetů s hodnotou 'FF' takový, aby délka byla 128.

DER(SHA-1(*M*)) je kódováním algoritmu ID pro hašovací funkci a hodnotou hash do hodnoty ASN.1 typu DigestInfo (zvláštní kódovací pravidla):

'30'||'21'||'30'||'09'||'06'||'05'||'2B'||'0E'||'03'||'02'||'1A'||'05'||'00'||'04'||'14'||hodnota Hash.

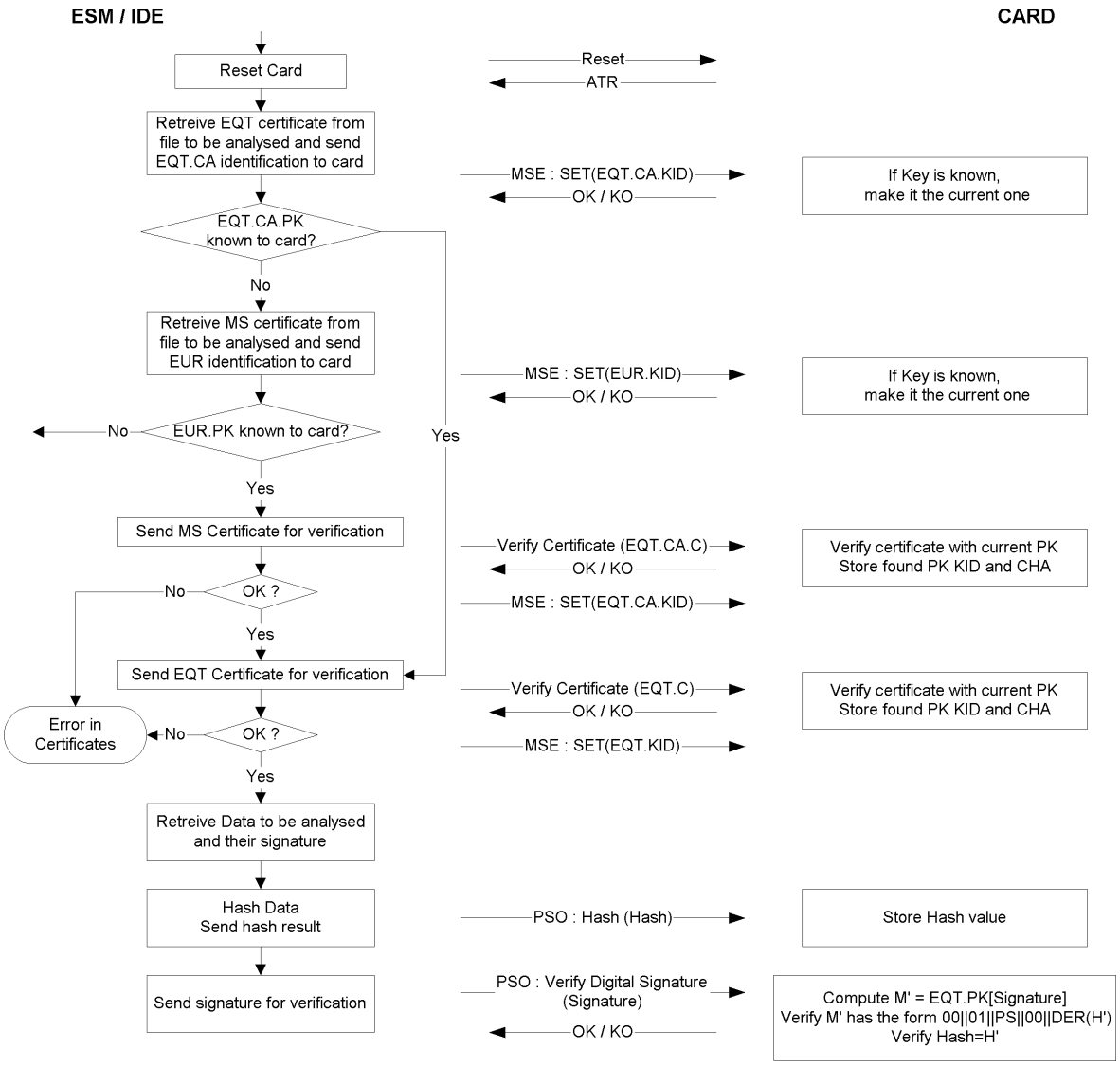
6.2. **Ověření podpisu**

CSM_035 Ověření dat podpisu stažených dat probíhá podle schématu podpisu s dodatkem definovaného v odkazu [PKCS1] s hašovací funkcí SHA-1.

Evropský klíč EUR.PK musí být ověřujícímu znám z nezávislé (a důvěryhodné) strany.

Následující tabulka zobrazuje protokol, podle kterého může IDE s kontrolní kartou ověřit integritu stažených dat uložených na externí paměťové médium (ESM). Pro dešifrování digitálních podpisů se užije kontrolní karta. Tato funkce nemá být v tomto případě zahrnuta do IDE.

Zařízení, které data, jež se mají analyzovat, stáhlo a podepsalo, se označí jako EQT.



ČÁST B

SYSTÉM TACHOGRAFU DRUHÉ GENERACE

7. ÚVOD

7.1. **Zdroje**

V této části dodatku jsou užívány následující odkazy.

AES	National Institute of Standards and Technology (NIST), FIPS PUB 197: Advanced Encryption Standard (AES), listopad 26, 2001
DSS	National Institute of Standards and Technology (NIST), FIPS PUB 186-4: Digital Signature Standard (DSS), červenec 2013
ISO 7816-4	ISO/IEC 7816-4, Identification cards – Integrated circuit cards – Part 4: Organization, security and commands for interchange. Third edition 2013-04-15
ISO 7816-8	ISO/IEC 7816-8, Identification cards – Integrated circuit cards – Part 8: Commands for security operations. Second edition 2004-06-01
ISO 8825-1	ISO/IEC 8825-1, Information technology – ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER). Fourth edition, 2008-12-15
ISO 9797-1	ISO/IEC 9797-1, Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher. Second edition, 2011-03-01
ISO 10116	ISO/IEC 10116, Information technology – Security techniques – Modes of operation of an *n*-bit block cipher. Third edition, 2006-02-01
ISO 16844-3	ISO/IEC 16844-3, Road vehicles – Tachograph systems – Part 3: Motion sensor interface. First edition 2004, including Technical Corrigendum 1 2006
RFC 5480	Elliptic Curve Cryptography Subject Public Key Information, March 2009
RFC 5639	Elliptic Curve Cryptography (ECC) – Brainpool Standard Curves and Curve Generation, 2010
RFC 5869	HMAC-based Extract-and-Expand Key Derivation Function (HKDF), May 2010
SHS	National Institute of Standards and Technology (NIST), FIPS PUB 180-4: Secure Hash Standard, March 2012
SP 800-38B	National Institute of Standards and Technology (NIST), Special Publication 800-38B: Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, 2005
TR-03111	BSI Technical Guideline TR-03111, Elliptic Curve Cryptography, version 2.00, 2012-06-28

7.2. **Značení a zkratky**

V tomto dodatku jsou užity následující značení a zkratky:

AES	pokročilý standard pro šifrování
CA	certifikační orgán
CAR	Odkaz na certifikační orgán
CBC	řetězení šifrového textu (operační mód)

CH	hlavička příkazu
CHA	Autorizace držitele certifikátu
CHR	Odkaz na držitele certifikátu
CV	konstantní vektor
DER	zvláštní kódovací pravidla
DO	datový objekt
DSRC	vyhrazená komunikace krátkého dosahu
ECC	kryptografie na bázi eliptických křivek
ECDSA	algoritmus digitálního podpisu na bázi eliptických křivek
ECDH	Diffie-Hellmanova eliptická křivka (algoritmus odsouhlasení klíče)
EGF	vnější zařízení GNSS
EQT	Zařízení
IDE	inteligentní vyhrazené zařízení
K_M	hlavní klíč snímače pohybu, umožňující párování VU se snímačem pohybu
K_{M-VU}	klíč vložený do VU, umožňující VU odvodit hlavní klíč snímače pohybu při vložení karty dílny do VU
K_{M-WC}	klíč vložený do karet dílny, umožňující VU odvodit hlavní klíč snímače pohybu při vložení karty dílny do VU
MAC	kód ověřování zprávy
MoS	snímač pohybu
MSB	nejdůležitější bit
PKI	infrastruktura veřejného klíče
RCF	zařízení vzdálené komunikace
SSC	čítač odeslané posloupnosti
SM	Bezpečné předávání zpráv
TDES	trojitý standard šifrování dat
TLV	hodnota délky tagu
VU	celek ve vozidle
X.C	certifikát veřejného klíče uživatele X
X.CA	certifikační orgán, který vydal certifikát uživatele X
X.CAR	odkaz na certifikační orgán uvedený v certifikátu uživatele X
X.CHR	odkaz na držitele certifikátu uvedený v certifikátu uživatele X
X.PK	veřejný klíč uživatele X
X.SK	soukromý klíč uživatele X
$X.PK_{eph}$	přechodný veřejný klíč uživatele X
$X.SK_{eph}$	přechodný soukromý klíč uživatele X
‘xx’	hexadecimální hodnota
||	operátor řetězení

7.3. **Definice**

Definice termínů používaných v tomto dodatku jsou uvedeny v části I přílohy 1C.

8. KRYPTOGRAFICKÉ SYSTÉMY A ALGORITMY

8.1. **Kryptografické systémy**

CSM_38 VU a karty tachografu musí užívat systém šifrování veřejného klíče na bázi eliptických křivek k tomu, aby zajistily následující bezpečnostní služby:

— vzájemné ověřování pravosti mezi VU a kartou,

— odsouhlasení klíčů relace AES mezi VU a kartou,

— zajištění pravosti, integrity a nepopiratelnosti dat stahovaných z VU nebo karet tachografu na externí média.

CSM_39 VU a vnější zařízení GNSS musí užívat kryptografický systém veřejného klíče na bázi eliptických křivek k tomu, aby zajistily následující bezpečnostní služby:

— vazbu VU a vnějšího zařízení GNSS,

— vzájemné ověřování pravosti mezi VU a vnějším zařízením GNSS,

— odsouhlasení klíčů relace AES mezi VU a vnějším zařízením GNSS.

CSM_40 VU a karty tachografu musí užívat symetrický kryptografický systém na bázi AES k tomu, aby zajistily následující bezpečnostní služby:

— zajištění pravosti a integrity dat vyměňovaných mezi VU a kartou tachografu,

— v příslušných případech zajištění důvěrnosti dat vyměňovaných mezi VU a kartou tachografu.

CSM_41 VU a vnější zařízení GNSS musí užívat symetrický kryptografický systém na bázi AES k tomu, aby zajistily následující bezpečnostní služby:

— zajištění pravosti a integrity dat vyměňovaných mezi VU a vnějším zařízením GNSS.

CSM_42 VU a snímače pohybu musí užívat symetrický kryptografický systém na bázi AES k tomu, aby zajistily následující bezpečnostní služby:

— párování VU a snímače pohybu,

— vzájemné ověřování pravosti mezi VU a snímačem pohybu,

— zajištění důvěrnosti dat vyměňovaných mezi VU a snímačem pohybu.

CSM_43 VU a kontrolní karty musí užívat symetrický kryptografický systém na bázi AES k tomu, aby zajistily následující bezpečnostní služby na rozhraní vzdálené komunikace:

— zajištění důvěrnosti, pravosti a integrity dat předávaných z VU do kontrolní karty.

Poznámky:

— Data jsou v praxi předávána z VU na vzdálené dotazovací zařízení pod dohledem kontrolního úředníka pomocí zařízení vzdálené komunikace, které může být vnitřní nebo vnější jednotkou vůči VU, viz dodatek 14. Vzdálené dotazovací zařízení však odesílá přijatá data na kontrolní kartu pro dekódování a validaci pravosti. Z bezpečnostního hlediska jsou zařízení vzdálené komunikace a vzdálené dotazovací zařízení zcela transparentní.

— Karta dílny poskytuje stejné bezpečnostní služby pro rozhraní DSRC jako kontrolní karta. To dílně umožňuje validovat správnou funkci rozhraní vzdálené komunikace VU, včetně zabezpečení. Další informace jsou uvedeny v části 9.2.2.

8.2. **Kryptografické algoritmy**

8.2.1 *Symetrické algoritmy*

CSM_44 VU, karty tachografu, snímače pohybu a vnější zařízení GNSS musí podporovat algoritmy AES podle definice v [AES], s délkami klíčů 128, 192 a 256 bitů.

8.2.2 *Asymetrické algoritmy a standardní parametry domény*

CSM_45 VU, karty tachografu a vnější zařízení GNSS musí podporovat kryptografii na bázi eliptických křivek s velikostí klíče 256, 384 a 512/521 bitů.

CSM_46 VU, karty tachografu a vnější zařízení GNSS musí podporovat podpisový algoritmus ECDSA podle ustanovení [DSS].

CSM_47 VU, karty tachografu a vnější zařízení GNSS musí podporovat algoritmus odsouhlasení klíčů ECKA-EG podle ustanovení [TR 03111].

CSM_48 VU, karty tachografu a vnější zařízení GNSS musí podporovat všechny standardní parametry domén stanovené v Tabulka 1 níže pro kryptografii na bázi eliptických křivek.

Tabulka 1

Standardní parametry domén

Název	Velikost (bity)	Odkaz	Identifikátor objektu
NIST P-256	256	[DSS], [RFC 5480]	`secp256r1`
BrainpoolP256r1	256	[RFC 5639]	`brainpoolP256r1`
NIST P-384	384	[DSS], [RFC 5480]	`secp384r1`
BrainpoolP384r1	384	[RFC 5639]	`brainpoolP384r1`
BrainpoolP512r1	512	[RFC 5639]	`brainpoolP512r1`
NIST P-521	521	[DSS], [RFC 5480]	`secp521r1`

Poznámka: Identifikátory objektu uvedené v posledním sloupci Tabulka 1 jsou stanoveny v [RFC 5639] pro křivky Brainpool a v [RFC 5480] pro křivky NIST.

Příklad 1: Identifikátor objektu křivky BrainpoolP256r1 je `{iso(1) identified-organization(3) teletrust(36) algorithm(3) signaturealgorithm(3) ecSign(2) ecStdCurvesAndGeneration (8) ellipticCurve(1) versionOne(1) 7}`.

Nebo v bodovém záznamu: `1.3.36.3.3.2.8.1.1.7`.

Příklad 2: Identifikátor předmětu křivky NIST P-384 je

`{iso(1) identified-organization(3) certicom(132) curve(0) 34}`.

Nebo v bodovém záznamu: `1.3.132.0.34`.

8.2.3 *Hašovací algoritmy*

CSM_49 VU a karty tachografu musí podporovat algoritmy transformace SHA-256, SHA-384 a SHA-512 stanovené v [SHS].

8.2.4 *Šifrovací soustavy*

CSM_50 V případě symetrického algoritmu se asymetrický algoritmus a/nebo hašovací algoritmus používají společně a vytvářejí bezpečnostní protokol, jejich příslušné délky klíče a velikosti hash musí mít (zhruba) stejnou sílu. Tabulka 2 zobrazuje schválené sady šifer:

Tabulka 2

Povolené sady šifer

ID sady šifer	Velikost klíče ECC (bity)	Délka klíče AES (bity)	Hašovací algoritmus	Délka MAC (bajty)
CS#1	256	128	SHA-256	8
CS#2	384	192	SHA-384	12
CS#3	512/521	256	SHA-512	16

Poznámka: Velkosti klíče ECC 512 bitů a 521 bitů jsou považovány, že jsou stejné síly pro všechny účely v rámci tohoto dodatku.

9. KLÍČE A CERTIFIKÁTY

9.1. **Asymetrické páry klíčů a certifikáty veřejných klíčů**

9.1.1 *Obecné informace*

Poznámka: Klíče popisované v této části jsou používány pro vzájemné ověřování pravosti a bezpečné předávání zpráv mezi VU a kartami tachografu a mezi VU a vnějšími zařízeními GNSS. Tyto procesy jsou podrobně popsány v kapitolách 10 a 11 tohoto dodatku.

CSM_51 V rámci systému evropského inteligentního tachografu musí být páry klíčů ECC a příslušné certifikáty generovány a spravovány prostřednictvím tří funkčních hierarchických úrovní:

— evropské úrovně,

— úrovně členských států,

— úrovně zařízení.

CSM_52 V rámci systému evropského inteligentního tachografu musí být veřejné i soukromé klíče a certifikáty generovány, spravovány a předávány pomocí standardních a bezpečných metod.

9.1.2 *Evropská úroveň*

CSM_53 Na evropské úrovni musí být generován jediný pár evropských klíčů ECC označený jako EUR. Musí sestávat ze soukromého klíče (EUR.SK) a veřejného klíče (EUR.PK). Tento pár klíčů představuje kořenový pár klíčů celé PKI evropského inteligentního tachografu. Tento úkol musí zajišťovat Evropský úřad kořenových certifikátů (ERCA) pod pravomocí a odpovědností Evropské komise.

CSM_54 ERCA musí užívat evropský soukromý klíč k podpisu (automatickému) kořenového certifikátu evropského veřejného klíče a tento evropský kořenový certifikát sdělovat všem členským státům.

CSM_55 ERCA musí na požádání užívat evropský soukromý klíč k podpisu certifikátů veřejných klíčů členských států. ERCA musí udržovat záznamy o všech podepsaných certifikátech veřejných klíčů členských států.

CSM_56 Podle popisu na Obrázek 1 v části 9.1.7 musí ERCA generovat nový evropský kořenový pár klíčů každých 17 let. Kdykoli ERCA generuje nový evropský kořenový pár klíčů, vytvoří nový automaticky podepsaný kořenový certifikát pro nový evropský veřejný klíč. Doba platnosti evropského kořenového certifikátu je 34 let a 3 měsíce.

Poznámka: Zavedení nového kořenového páru klíčů rovněž předpokládá, že ERCA generuje nový hlavní klíč pro snímač pohybu a nový hlavní klíč DSRC, viz části 9.2.1.2 and 9.2.2.2.

CSM_57 Před vygenerováním nového evropského kořenového páru klíčů musí ERCA provést analýzu kryptografické síly, která je potřebná pro nový pár klíčů, aby mohl být bezpečný pro dalších 34 let. V případě potřeby ERCA přejde na sadu šifer, která je silnější než sada stávající, podle popisu v CSM_50.

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. To je také znázorněno na Obrázek 1 v bodě 9.1.7.

Poznámka: Protože spojovací certifikát obsahuje veřejný klíč ERCA generace *X* a je podepsán soukromým klíčem ERCA generace *X-1*, poskytuje tento spojovací certifikát zařízení vytvořenému za generace *X-1* základ pro důvěru zařízení vytvořenému za generace *X*.

CSM_59 ERCA nesmí užívat soukromý klíč kořenového páru klíčů k jakémukoli účelu od okamžiku vstupu nového kořenového certifikátu klíče v platnost.

CSM_60 ERCA kdykoli zlikviduje tyto kryptografické klíče a certifikáty:

— Stávající pár klíčů EUR a příslušný certifikát

— Všechny předchozí certifikáty EUR používané pro ověření dosud platných certifikátů MSCA

— Spojovací certifikáty pro všechny generace certifikátů EUR s výjimkou prvního

9.1.3 *Úroveň členských států*

CSM_61 Na úrovni členských států musí všechny členské státy, které podepisují certifikáty karet tachografu, generovat jeden nebo více jedinečných párů klíčů ECC označených jako MSCA_Card. Všechny členské státy, které podepisují certifikáty pro VU nebo vnější zařízení GNSS, musí navíc generovat jeden nebo více jedinečných párů klíčů ECC označených jako MSCA_VU-EGF.

CSM_62 Úkol generování párů klíčů členského státu musí zajišťovat certifikační orgán členského státu (MSCA). Kdykoli MSCA generuje pár klíčů členského státu, odešle do ERCA veřejný klíč, aby obdržel příslušný certifikát členského státu podepsaný ERCA.

CSM_63 MSCA musí zvolit sílu páru klíčů členského státu odpovídající síle evropského kořenového páru klíčů užívaného k podpisu příslušného certifikátu členského státu.

CSM_64 Případný pár klíčů MSCA_VU-EGF obsahuje soukromý klíč MSCA_VU-EGF.SK a veřejný klíč MSCA_VU-EGF.PK. MSCA musí soukromý klíč MSCA_VU-EGF.SK užívat výhradně k podpisu certifikátů veřejného klíče VU a vnějších zařízení GNSS.

CSM_65 Pár klíčů MSCA_Card obsahuje soukromý klíč MSCA_Card.SK a veřejný klíč MSCA_Card.PK. MSCA musí soukromý klíč MSCA_Card.SK užívat výhradně k podpisu certifikátů veřejného klíče karet tachografu.

CSM_66 MSCA musí udržovat záznamy všech podepsaných certifikátů VU, certifikátů vnějších zařízení GNSS a certifikátů karet společně s identifikací zařízení, pro které je každý certifikát určen.

CSM_67 Doba platnosti certifikátu MSCA_VU-EGF je 17 let plus 3 měsíce. Doba platnosti certifikátu MSCA_Card je 7 let plus 1 měsíc.

CSM_68 Jak je patrné z Obrázek 1 v části 9.1.7, soukromý klíč z páru klíčů MSCA_VU-EGF a soukromý klíč z páru klíčů MSCA_Card musí být používány po dobu dvou let.

CSM_69 MSCA nesmí soukromý klíč páru klíčů MSCA_VU-EGF od chvíle, kdy skončí doba jeho použitelnosti, užívat k žádnému účelu. MSCA nesmí od chvíle, kdy skončí jeho doba použitelnosti, užívat k žádnému účelu ani soukromý klíč páru klíčů MSCA_Card.

CSM_70 MSCA musí kdykoli zlikvidovat tyto kryptografické klíče a certifikáty:

— Stávající pár klíčů MSCA_Card a příslušný certifikát

— Všechny předchozí certifikáty MSCA_Card užívané pro ověřování dosud platných certifikátů karet tachografu

— Současný certifikát EUR potřebný pro ověřování stávajícího certifikátu MSCA

— Všechny předchozí certifikáty EUR potřebné pro ověřování všech dosud platných certifikátů MSCA

CSM_71 Má-li MSCA podepsat certifikáty pro VU nebo vnější zařízení GNSS, musí navíc zlikvidovat tyto klíče a certifikáty:

— Stávající pár klíčů MSCA_VU-EGF a příslušný certifikát

— Všechny předchozí veřejné klíče MSCA_VU-EGF užívané pro ověřování dosud platných certifikátů VU nebo vnějších zařízení GNSS

9.1.4 *Úroveň zařízení: celky ve vozidle*

CSM_72 Pro každý VU musí být generovány dva jedinečné páry klíčů ECC označené jako VU_MA a VU_Sign. Tento úkol musí zajišťovat výrobci VU. Při každém generování páru klíčů VU zašle strana generující klíč MSCA země, v níž sídlí, veřejný klíč, aby mohla obdržet příslušný certifikát VU podepsaný MSCA. Soukromý klíč užívá pouze VU.

CSM_73 Certifikáty VU_MA a VU_Sign příslušného celku ve vozidle musí mít stejné datum účinnosti.

CSM_74 Výrobce VU musí zvolit sílu páru klíčů VU odpovídající síle páru klíčů MSCA užívaného k podpisu příslušného certifikátu VU.

CSM_75 Celek ve vozidle musí užívat svůj pár klíčů VU_MA obsahující soukromý klíč VU_MA.SK a veřejný klíč VU_MA.PK výhradně pro ověřování pravosti VU vůči kartám tachografu a vnějším zařízením GNSS podle pokynů v částech 10.3 a 11.4 tohoto dodatku.

CSM_76 Celek ve vozidle musí být schopen generovat přechodné páry klíčů ECC a musí užívat přechodný pár klíčů výhradně pro odsouhlasení klíče relace s kartou tachografu nebo vnějším zařízením GNSS podle pokynů v částech 10.4 a 11.4 tohoto dodatku.

CSM_77 Celek ve vozidle musí užívat soukromý klíč VU_Sign.SK svého páru klíčů VU_Sign výhradně k podpisu stahovaných souborů dat podle pokynů v kapitole 14 tohoto dodatku. Příslušný veřejný klíč VU_Sign.PK musí být užíván výhradně pro ověřování podpisů vytvořených celkem ve vozidle.

CSM_78 Podle pokynů Obrázek 1 v části 9.1.7 musí být doba platnosti certifikátu VU_MA 15 let a 3 měsíce. Doba platnosti certifikátu VU_Sign musí být rovněž 15 let a 3 měsíce.

Poznámky:

— Prodloužená doba platnosti certifikátu VU_Sign umožňuje VU vytvářet platné podpisy stahovaných dat během prvních tří měsíců po skončení platnosti podle ustanovení nařízení (EU) č. 581/2010.

— Prodloužená doba platnosti certifikátu VU_MA je potřebná k tomu, aby VU mohl prokázat pravost kontrolní karty nebo karty společnosti během prvních tří měsíců po skončení platnosti, aby bylo možné stahovat data.

CSM_79 Celek ve vozidle nesmí používat soukromý klíč páru klíčů VU po skončení platnosti příslušného certifikátu užívat k žádnému účelu.

CSM_80 Páry klíčů VU (s výjimkou přechodných párů klíčů) a příslušné certifikáty daného celku ve vozidle nesmí být vyměňovány nebo obnovovány v terénu poté, co byl celek ve vozidle uveden do provozu.

Poznámky:

— Přechodné páry klíčů nejsou do tohoto požadavku zahrnuty, protože nový přechodný pár klíčů je generován VU při každém ověřování pravosti čipu a odsouhlasení klíče relace, viz část 10.4. Přechodné páry klíčů ostatně nemají příslušné certifikáty.

— Tento požadavek nebrání možnosti výměny statických párů klíčů VU během renovace nebo opravy v bezpečném prostředí kontrolovaném výrobcem VU.

CSM_81 Při uvedení do provozu musí celky ve vozidle obsahovat tyto kryptografické klíče a certifikáty:

— soukromý klíč VU_MA a příslušný certifikát,

— soukromý klíč VU_Sign a příslušný certifikát,

— certifikát MSCA_VU-EGF obsahující veřejný klíč MSCA_VU-EGF.PK užívaný k ověřování certifikátu VU_MA a certifikátu VU_Sign,

— certifikát EUR obsahující veřejný klíč EUR.PK používaný pro ověření certifikátu MSCA_VU-EGF,

— certifikát EUR, jehož doba platnosti přímo předchází době platnosti certifikátu EUR používaného pro ověření certifikátu MSCA_VU-EGF, pokud existuje,

— spojovací certifikát spojující tyto dva certifikáty EUR, pokud existuje.

CSM_82 Kromě kryptografických klíčů a certifikátů uvedených v CSM_81 musí celky ve vozidle rovněž obsahovat klíče a certifikáty uvedené v části A tohoto dodatku, které celku ve vozidle umožňují spolupracovat s kartami tachografu první generace.

9.1.5 *Úroveň zařízení: karty tachografu*

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 MSCA země, v níž sídlí, veřejný klíč, aby mohla obdržet příslušný certifikát karty podepsaný MSCA. Soukromý klíč užívá pouze karta tachografu.

CSM_84 Certifikáty Card_MA a Card_Sign příslušné karty řidiče nebo karty dílny musí mít stejné datum vstupu v platnost.

CSM_85 Výrobce karet nebo personalizátor karet musí zvolit sílu páru klíčů karty odpovídající síle páru klíčů MSCA užívaného k podpisu příslušného certifikátu karty.

CSM_86 Karta tachografu musí svůj pár klíčů Card_MA obsahující soukromý klíč Card_MA.SK a veřejný klíč Card_MA.PK užívat výhradně pro vzájemné ověřování pravosti a odsouhlasení klíče relace vůči celkům ve vozidle podle pokynů v částech 10.3 a 10.4 tohoto dodatku.

CSM_87 Karta řidiče nebo karta dílny musí soukromý klíč Card_Sign.SK svého páru klíčů Card_Sign užívat výhradně k podpisu stahovaných souborů dat podle pokynů v kapitole 14 tohoto dodatku. Příslušný veřejný klíč Card_Sign.PK se užívá výhradně k ověřování podpisů vytvářených kartou.

CSM_88 Doba platnosti certifikátu Card_MA je následující:

— pro karty řidiče: 5 let

— pro karty společnosti: 2 roky

— pro kontrolní karty: 2 roky

— pro karty dílny: 1 rok

CSM_89 Doba platnosti certifikátu Card_Sign je následující:

— pro karty řidiče: 5 let a 1 měsíc,

— pro karty dílny: 1 rok a 1 měsíc.

Poznámka: Prodloužená doba platnosti certifikátu Card_Sign umožňuje kartě řidiče vytvářet platné podpisy stahovaných dat během prvního měsíce po skončení platnosti. To je nutné s ohledem na nařízení (EU) č. 581/2010, které vyžaduje, aby bylo stahování dat z karty řidiče možné do 28 dnů po zaznamenání posledních dat.

CSM_90 Páry klíčů a příslušné certifikáty dané karty tachografu nesmí být po vydání karty vyměňovány nebo obnovovány.

CSM_91 Při vydání obsahují karty tachografu tyto kryptografické klíče a certifikáty:

— soukromý klíč Card_MA a příslušný certifikát,

— pro karty řidiče a karty dílny navíc: soukromý klíč Card_Sign a příslušný certifikát,

— certifikát MSCA_Card obsahující veřejný klíč MSCA_Card.PK užívaný k ověřování certifikátu Card_MA a certifikátu Card_Sign,

— certifikát EUR obsahující veřejný klíč EUR.PK užívaný k ověřování certifikátu MSCA_Card,

— certifikát EUR, jehož doba platnosti přímo předchází době platnosti certifikátu EUR užívaného k ověřování certifikátu MSCA_Card, pokud existuje,

— spojovací certifikát spojující tyto dva certifikáty EUR, pokud existuje.

CSM_92 Kromě kryptografických klíčů a certifikátů uvedených v CSM_91 musí karty tachografu rovněž obsahovat klíče a certifikáty uvedené v části A tohoto dodatku, které těmto kartám umožňují spolupracovat s VU první generace.

9.1.6 *Úroveň zařízení: vnější zařízení GNSS*

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 strana generující klíč zašle MSCA země, v níž sídlí, veřejný klíč, aby mohla obdržet příslušný certifikát EGF_MA podepsaný MSCA. Soukromý klíč užívá pouze vnější zařízení GNSS.

CSM_94 Výrobce EGF musí zvolit sílu páru klíčů EGF_MA odpovídající síle páru klíčů MSCA užívaného k podpisu příslušného certifikátu EGF_MA.

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 části 11.4 a 11.4 tohoto dodatku.

CSM_96 Doba platnosti certifikátu EGF_MA je 15 let.

CSM_97 Vnější zařízení GNSS nesmí užívat soukromý klíč svého páru klíčů EGF_MA pro vazbu s celkem ve vozidle po skončení platnosti příslušného certifikátu.

Poznámka: Podle pokynů v části 11.3.3 může EGF potenciálně užívat svůj soukromý klíč pro vzájemné ověřování pravosti vůči VU, s nímž je již spárováno, i po skončení platnosti příslušného certifikátu.

CSM_98 Pár klíčů EGF_MA a příslušný certifikát daného vnějšího zařízení GNSS nesmí být vyměňovány nebo obnovovány v terénu poté, co bylo EGF uvedeno do provozu.

Poznámka: Tento požadavek nebrání možnosti výměny párů klíčů EGF během renovace nebo opravy v bezpečném prostředí kontrolovaném výrobcem EGF.

CSM_99 Při uvedení do provozu musí vnější zařízení GNSS obsahovat tyto kryptografické klíče a certifikáty:

— soukromý klíč EGF_MA a příslušný certifikát,

— certifikát MSCA_VU-EGF obsahující veřejný klíč MSCA_VU-EGF.PK používaný pro ověření certifikátu EGF_MA,

— certifikát EUR obsahující veřejný klíč EUR.PK používaný pro ověření certifikátu MSCA_VU-EGF,

— certifikát EUR, jehož doba platnosti přímo předchází době platnosti certifikátu EUR používaného pro ověření certifikátu MSCA_VU-EGF, pokud existuje,

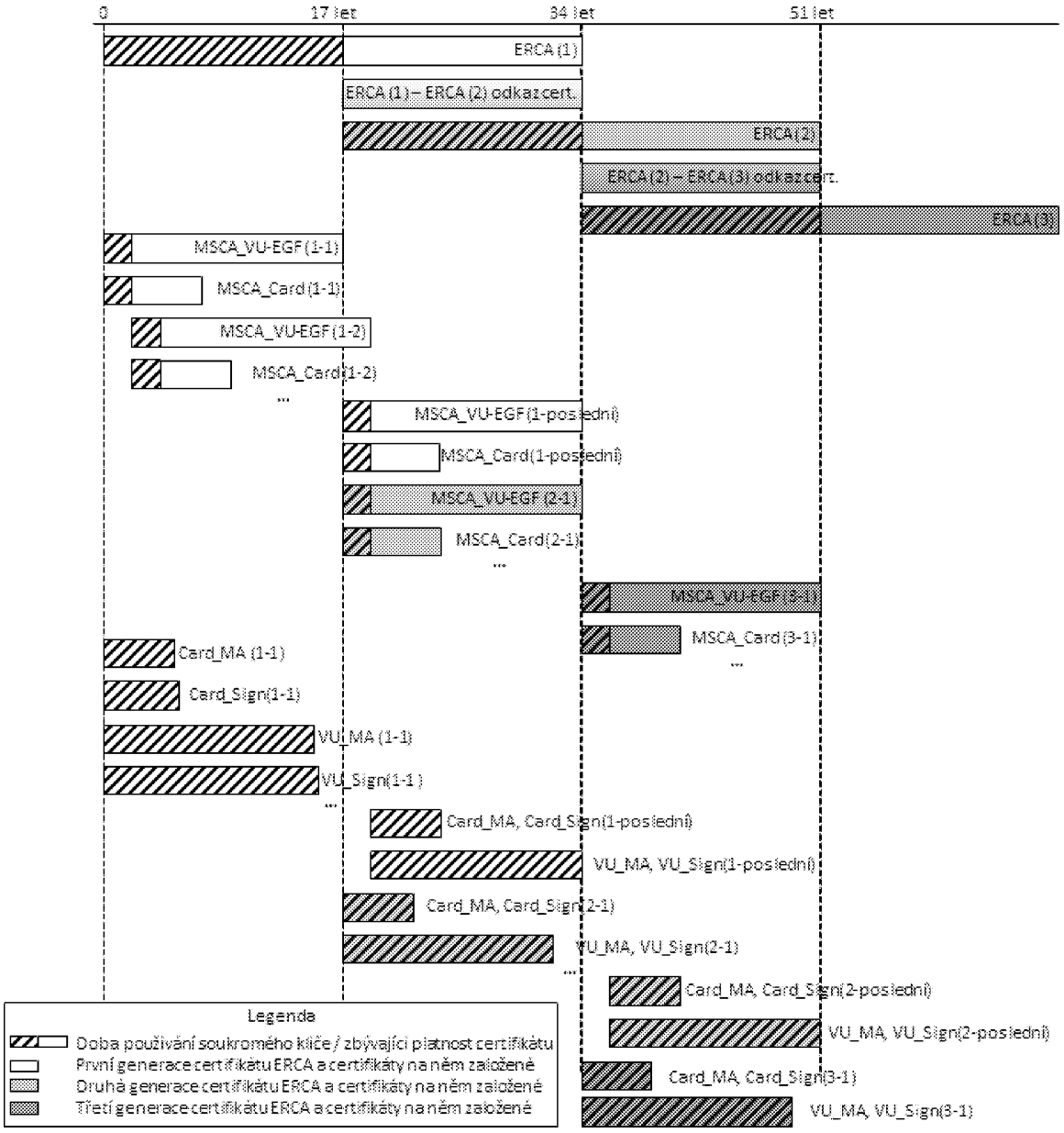
— spojovací certifikát spojující tyto dva certifikáty EUR, pokud existuje.

9.1.7 *Přehled: výměna certifikátu*

Obrázek 1 níže zobrazuje vydávání a užívání různých generací kořenových certifikátů ERCA, spojovacích certifikátů ERCA, certifikátů MSCA a certifikátů zařízení (VU a karta):

Obrázek 1

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



Poznámky k Obrázek 1:

1. Různé generace kořenového certifikátu jsou označeny číslem v závorkách. Např. ERCA (1) je první generace kořenového certifikátu ERCA; ERCA (2) je druhá generace atd.

2. Ostatní certifikáty jsou označeny dvěma čísly v závorkách, první z nich označuje generaci kořenového certifikátu, v níž jsou vydány, druhé generaci samotného certifikátu. Např. MSCA_Card (1-1) je první certifikát MSCA_Card vydaný v rámci ERCA (1); MSCA_Card (2-1) je první certifikát MSCA_Card vydaný v rámci ERCA (2); MSCA_Card (2-last) je poslední certifikát MSCA_Card vydaný v rámci ERCA (2); Card_MA (2-1) je první certifikát Card pro vzájemné ověřování pravosti vydaný v rámci ERCA (2) atd.

3. Certifikáty MSCA_Card (2-1) a MSCA_Card (1-last) jsou vydány téměř ke stejnému datu, ale nikoli úplně přesně. MSCA_Card (2-1) je první certifikát MSCA_Card vydaný v rámci ERCA (2) a bude vydán poněkud později než MSCA_Card (1-last), poslední certifikát MSCA_Card v rámci ERCA (1).

4. Jak je zobrazeno na obrázku, první certifikát VU a certifikáty karty vydané v rámci ERCA (2) budou vydány téměř dva roky před vydáním posledního certifikátu VU a certifikátu karty vydaných v rámci ERCA (1). Důvodem je skutečnost, že certifikát VU a certifikát karty jsou vydány v rámci certifikátu MSCA, nikoli přímo v rámci certifikátu ERCA. Certifikát The MSCA (2-1) bude vydán přímo po vstupu ERCA (2) v platnost, ale certifikát MSCA (1-last) bude vydán pouze nedlouho před touto dobou, v posledním okamžiku, kdy je certifikát ERCA (1) ještě platný. Tyto dva certifikáty MSCA mají proto téměř stejnou dobu platnosti, ačkoli jsou zástupci různých generací.

5. Doba platnosti uvedená pro karty je stejná jako pro karty řidiče (5 let).

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

9.2. **Symetrické klíče**

9.2.1 *Klíče pro zabezpečení VU – komunikace snímače pohybu*

9.2.1.1 *Obecné informace*

Poznámka: Čtenáři této části by měli být seznámeni s obsahem [ISO 16844-3] popisujícím rozhraní mezi celkem ve vozidle a snímačem pohybu. Proces párování mezi VU a snímačem pohybu je podrobně popsán v kapitole 12tohoto dodatku.

CSM_100 Pro párování celků ve vozidle a snímačů pohybu, pro vzájemné ověřování pravosti mezi celky ve vozidle a snímači pohybu a pro šifrování komunikace mezi celky ve vozidle a snímači pohybu je zapotřebí řada symetrických klíčů podle Tabulka 3. Všechny tyto klíče jsou klíče AES s délkou odpovídající délce hlavního klíče snímače pohybu, který musí být spojen s délkou (předpokládaného) evropského kořenového páru klíčů podle popisu v CSM_50.

Tabulka 3

Klíče pro zabezpečení celku ve vozidle – komunikace snímače pohybu

Klíč	Značka	Generován	Metoda generace	Uložen kým
Hlavní klíč snímače pohybu – část VU	$K_{M\text{-}VU}$	ERCA	Náhodný výběr	ERCA, MSCA účastnící se vydávání certifikátů VU, výrobci VU, celky ve vozidle

Klíč	Značka	Generován	Metoda generace	Uložen kým
Hlavní klíč snímače pohybu – část dílny	K_{M-WC}	ERCA	Náhodný výběr	ERCA, MSCA, výrobci karet, karty dílny
Hlavní klíč snímače pohybu	K_M	Negenerovaný nezávisle	Vypočtená jako $K_M = K_{M-VU}$ XOR K_{M-WC}	ERCA, MSCA účastnící se vydávání klíčů snímačů pohybu (volitelně) (*)
Identifikační klíč	K_{ID}	Negenerovaný nezávisle	Vypočtená jako $K_{ID} = K_M$ XOR CV, kde CV je specifkováno v CSM_106	ERCA, MSCA účastnící se vydávání klíčů snímačů pohybu (volitelně) (*)
Párovací klíč	K_P	Výrobce snímače pohybu	Náhodný výběr	Jeden snímač pohybu
Klíč relace	K_S	VU (během párování VU a snímače pohybu)	Náhodný výběr	Jeden VU a jeden snímač pohybu

(*) Uložení K_M a K_{ID} je volitelné, protože tyto klíče lze odvodit z K_{M-VU}, K_{M-WC} a CV.

CSM_101 Evropský úřad kořenových certifikátů (ERCA) musí generovat K_{M-VU} a K_{M-WC}, dva náhodné a jedinečné klíče AES, z nichž lze vypočítat hlavní klíč snímače pohybu K_M jako K_{M-VU} XOR K_{M-WC}. ERCA musí na požádání sdělit K_M, K_{M-VU} a K_{M-WC} certifikačním orgánům členských států.

CSM_102 ERCA musí každému hlavnímu klíči snímače pohybu K_M přidělit jedinečné číslo verze, které je rovněž použitelné pro ustavující klíče K_{M-VU} a K_{M-WC} a pro příslušný identifikační klíč K_{ID}. ERCA musí MSCA sdělit číslo verze při zaslání K_{M-VU} a K_{M-WC}.

Poznámka: Číslo verze se užívá pro rozlišování různých generací těchto klíčů, jak je podrobně uvedeno v části 9.2.1.2.

CSM_103 Certifikační orgán členského státu musí K_{M-VU} společně s jeho číslem verze předat na požádání výrobcům celků ve vozidle. Výrobci VU musí vložit K_{M-VU} a jeho číslo verze do všech vyrobených VU.

CSM_104 Certifikační orgán členského státu musí zajistit, aby byl K_{M-WC} společně s číslem verze vložen do všech karet dílny vydaných v rámci jeho odpovědnosti.

Poznámky:

— Viz popis datového typu `SensorInstallationSecData` v dodatku 2.

— Podle vysvětlení v části 9.2.1.2 musí být do jedné karty dílny prakticky možné vkládat více generací K_{M-WC}.

CSM_105 Kromě klíče AES uvedeného v CSM_104 musí MSCA zajistit, aby klíč TDES Km_{WC}, stanovený v požadavku CSM_037 v části A tohoto dodatku byl vložen do každé karty dílny vydané v rámci jeho odpovědnosti.

Poznámky:

— Tím se umožní užívání karty dílny druhé generace pro párování s VU první generace.

— Karta dílny druhé generace obsahuje dvě různé aplikace, z nichž jedna odpovídá části B tohoto dodatku a druhá odpovídá části A. Ta obsahuje klíč TDES Km_{WC}.

CSM_106 MSCA účastnící se vydávání snímačů pohybu musí odvodit identifikační klíč z hlavního klíče snímače pohybu pomocí operace XOR s konstantním vektorem CV. CV má tuto hodnotu:

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

— Pro 192-bitové hlavní klíče snímače pohybu: CV = '72 AD EA FA 00 BB F4 EE F4 99 15 70 5B 7E EE BB 1C 54 ED 46 8B 0E F8 25'

— Pro 256-bitové hlavní klíče snímače pohybu: CV = '1D 74 DB F0 34 C7 37 2F 65 55 DE D5 DC D1 9A C3 23 D6 A6 25 64 CD BE 2D 42 0D 85 D2 32 63 AD 60'

Poznámka: Konstantní vektory byly generovány takto:

Pi_10 = prvních 10 bajtů decimální části matematické konstanty π = '24 3F 6A 88 85 A3 08 D3 13 19'

CV_128-bitů = prvních 16 bajtů SHA-256(Pi_10)

CV_192-bitů = prvních 24 bajtů SHA-384(Pi_10)

CV_256-bitů = prvních 32 bajtů SHA-512(Pi_10)

CSM_107 Výrobci snímačů pohybu musí generovat náhodný a jedinečný párovací klíč $K_P$pro každý snímač pohybu a odeslat každý párovací klíč certifikačnímu orgánu 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.

Poznámka: Podle pokynů v části 9.2.1.2 musí být výrobce snímačů pohybu prakticky schopen generovat vícenásobné jedinečné párovací klíče pro jeden snímač pohybu.

CSM_108 Výrobci snímačů pohybu musí generovat jedinečné sériové číslo pro každý snímač pohybu a odeslat všechna sériová čísla certifikačnímu orgánu 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}.

CSM_109 Pro požadavky CSM_107 a CSM_108 musí MSCA užívat algoritmy AES v operačním režimu řetězení šifrového textu podle definice v [ISO 10116] s vloženým parametrem *m* = 1 a inicializačním vektorem SV = '00' {16}, tj. šestnáct bajtů s binární hodnotou 0. V případě potřeby musí MSCA užívat metodu doplnění 2 definovanou v [ISO 9797-1].

CSM_110 Výrobce snímačů pohybu musí uložit zašifrovaný párovací klíč a zašifrované sériové číslo do určeného snímače pohybu společně s příslušnými otevřenými textovými hodnotami a číslem verze K_M a K_{ID} užívanými pro šifrování.

Poznámka: Podle pokynů v části 9.2.1.2 musí být výrobce snímačů pohybu prakticky schopen vkládat vícenásobné zašifrované párovací klíče a vícenásobná zašifrovaná sériová čísla do jednoho snímače pohybu.

CSM_111 Kromě kryptografického materiálu na bázi AES uvedeného v CSM_110 může výrobce snímačů pohybu rovněž do každého snímače pohybu ukládat kryptografický materiál na bázi TDES uvedený v požadavku CSM_037 v části A tohoto dodatku.

Poznámka: Snímači pohybu druhé generace je tak umožněno párování s VU první generace.

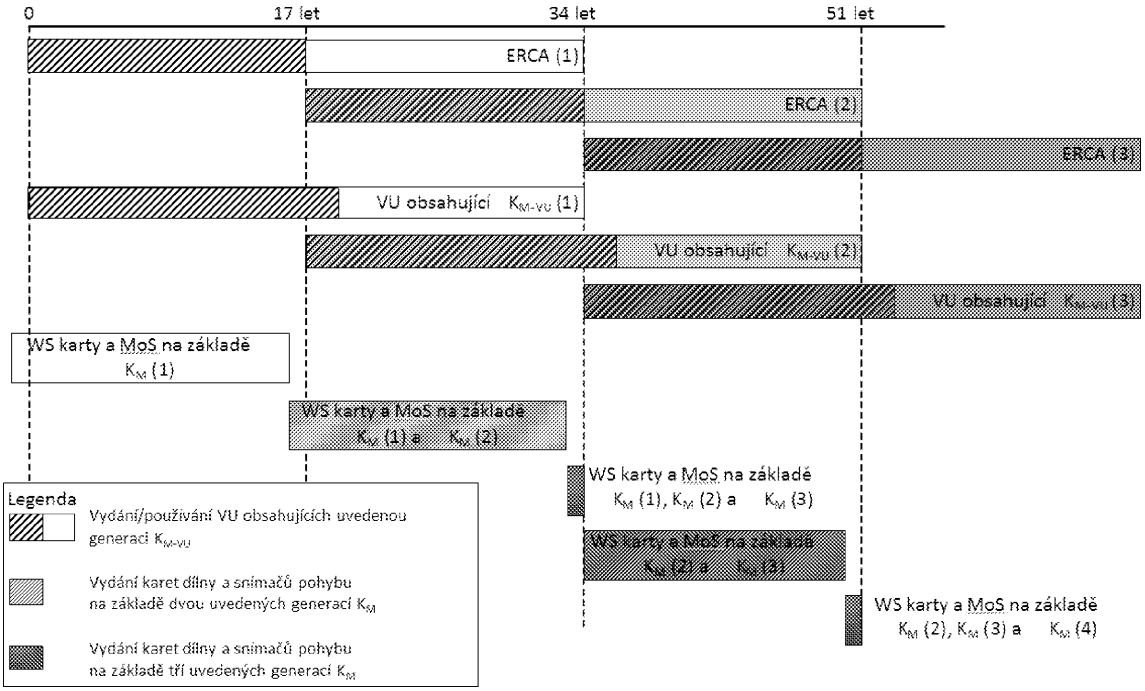
CSM_112 Délka klíče relace K_S generovaného VU během párování se snímačem pohybu musí být spojena s délkou jeho K_{M-VU} podle popisu v CSM_50.

9.2.1.2 *Výměna hlavního klíče snímače pohybu v zařízení druhé generace*

CSM_113 Každý hlavní klíč snímače pohybu a všechny související klíče (viz Tabulka 3) jsou přiřazeny k určité generaci kořenového páru klíčů ERCA. Tyto klíče proto musí být vyměněny každých 17 let. Doba platnosti každé generace hlavního klíče snímače pohybu musí začínat jeden rok před vstupem příslušného kořenového páru klíčů ERCA v platnost a končit se skončením platnosti příslušného kořenového páru klíčů ERCA. To je znázorněno na Obrázek 2.

Obrázek 2

Vydávání a užívání různých generací hlavního klíče snímače pohybu v celcích ve vozidle, snímačích pohybu a kartách dílny



CSM_114 Nejméně jeden rok před generováním nového evropského kořenového páru klíčů podle popisu v CSM_56 musí ERCA generovat nový hlavní klíč snímače pohybu $K_M$generováním nových klíčů K_{M-VU} a K_{M-WC}. Délka hlavního klíče snímače pohybu je spojena s předpokládanou délkou nového evropského kořenového páru klíčů podle CSM_50. ERCA musí na požádání oznámit MSCA nové klíče K_M, K_{M-VU} and K_{M-WC} společně s jejich číslem verze.

CSM_115 MSCA musí zajistit uložení všech platných generací K_{M-WC} do každé karty dílny vydané v rámci jeho pravomoci společně s jejich čísly verze podle Obrázek 2.

Poznámka: To předpokládá, že v posledním roce doby platnosti certifikátu ERCA budou vydány karty dílny se třemi různými generacemi K_{M-WC} podle Obrázek 2.

CSM_116 Ve vztahu k procesu popsanému výše v CSM_107 a CSM_108: MSCA musí šifrovat každý párovací klíč K_P, který obdrží od výrobce snímačů pohybu samostatně s každou platnou generací hlavního klíče snímače pohybu K_M. MSCA musí rovněž šifrovat každé sériové číslo, které obdrží od výrobce snímačů pohybu samostatně s každou platnou generací identifikačního klíče K_{ID}. Výrobce snímačů pohybu musí uložit veškerá šifrování párovacího klíče a veškerá šifrování sériového čísla do určeného snímače pohybu společně s příslušnými otevřenými textovými hodnotami a číslem (čísly) verze K_M a K_{ID} užívanými pro šifrování.

Poznámka: To předpokládá, že v posledním roce doby platnosti certifikátu ERCA budou vydány snímače pohybu se šifrovanými daty na základě tří různých generací K_M podle Obrázek 2.

CSM_117 Ve vztahu k procesu popsanému v CSM_107 výše: Protože délka párovacího klíče K_P musí být spojena s délkou K_M (viz CSM_100), musí být výrobce snímačů pohybu schopen generovat až tři různé párovací klíče (různých délek) pro jeden snímač pohybu v případě, že následující generace K_M mají různé délky. V takovém případě musí výrobce zaslat MSCA každý párovací klíč. MSCA musí zajistit, aby byl každý párovací klíč zašifrován se správnou generací hlavního klíče snímače pohybu, tj. tím, který má stejnou délku.

Poznámka: V případě, že se výrobce snímačů pohybu rozhodne generovat pro snímač pohybu druhé generace párovací klíč na bázi TDES (viz CSM_111), musí výrobce MSCA oznámit, že pro šifrování tohoto párovacího klíče je třeba použít hlavní klíč snímače pohybu na bázi TDES. Délka klíče TDES může být totiž stejná jako délka klíče AES, takže MSCA nemůže usuzovat podle samotné délky klíče.

CSM_118 Výrobce celků ve vozidle musí do každého celku ve vozidle vložit pouze jednu generaci K_{M-VU} společně s jeho číslem verze. Tato generace K_{M-VU} musí být spojena s certifikátem ERCA, na němž jsou založeny certifikáty VU.

Poznámky:

— Celek ve vozidle založený na certifikátu ERCA generace X musí obsahovat pouze K_{M-VU} generace *X*, i když je vydán po začátku doby platnosti certifikátu ERCA generace *X+1*. To je znázorněno na Obrázek 2.

— VU generace *X* nemůže být párován se snímačem pohybu generace *X-1*.

— Protože karty dílny mají dobu platnosti jednoho roku, důsledkem CSM_113 – CSM_118 je, že všechny karty dílny obsahují v okamžiku, kdy je vydán první VU obsahující nový K_{M-VU}, již nový K_{M-WC}. Tento VU je proto vždy schopen vypočítat nový K_M. Do té doby bude navíc většina nových snímačů pohybu také obsahovat šifrovaná data na bázi nového K_M.

9.2.2 *Klíče pro zabezpečení komunikace DSRC*

9.2.2.1 *Obecné informace*

CSM_119 Pravost a důvěrnost dat předávaných z celku ve vozidle řídicímu orgánu prostřednictvím kanálu vzdálené komunikace DSRC musí být zajištěny pomocí sady klíčů AES vyhrazených příslušným VU odvozených z jediného hlavního klíče DSRC, totiž KM_{DSRC}.

CSM_120 Hlavní klíč DSRC KM_{DSRC} musí být klíč AES, který je bezpečně generován, uložen a distribuován ERCA. Délka klíče může být 128, 192 nebo 256 bitů a musí být spojena s délkou evropského kořenového páru klíčů podle popisu v CSM_50.

CSM_121 ERCA musí certifikačním orgánům členských států na požádání bezpečným způsobem předat hlavní klíč DSRC, aby mohly odvozovat klíče DSRC vyhrazené příslušným VU a aby bylo zajištěno, že je hlavní klíč DSRC vložen do všech kontrolních karet a karet dílny vydaných v rámci jeho odpovědnosti.

CSM_122 ERCA musí každému hlavnímu klíči DSRC přidělit jedinečné číslo verze. ERCA musí MSCA sdělit číslo verze při zaslání hlavního klíče DSRC.

Poznámka: Číslo verze je užíváno pro rozlišování různých generací hlavního klíče DSRC, jak je podrobně vysvětleno v části 9.2.2.2.

CSM_123 Pro každý celek ve vozidle musí výrobce celku ve vozidle vytvořit jedinečné sériové číslo VU a na požádání je zaslat příslušnému certifikačnímu orgánu členského státu, aby mohl získat sadu dvou klíčů DSRC vyhrazených příslušným VU. Sériové číslo VU musí mít datový typ `VuSerialNumber` a pro kódování musí být použita zvláštní kódovací pravidla (DER) podle [ISO 8825-1].

CSM_124 Po přijetí žádosti o vydání klíčů DSRC vyhrazených příslušným VU musí MSCA odvodit dva klíče AES pro celek ve vozidle, označené K_VU_{DSRC}_ENC and K_VU_{DSRC}_MAC. Tyto klíče vyhrazené příslušným VU musí mít stejnou délku jako hlavní klíč DSRC. MSCA musí použít funkci odvození klíče definovanou v [RFC 5869]. Hašovací funkce, která je potřebná pro vytvoření instance funkce HMAC-Hash, musí být spojena s délkou hlavního klíče DSRC podle popisu v CSM_50. Funkce odvození klíče v [RFC 5869] se užívá takto:

Krok 1 (extrakce):

— *PRK* = HMAC-Hash (*salt, IKM*) kde *salt* je prázdný řetězec (empty string) *''* a *IKM* je KM_{DSRC}.

Krok 2 (expanze):

— *OKM* = *T(1)*, kde

T(1) = HMAC-Hash (*PRK, T(0)* || *info* || '01') s

— *T(0)* = an empty string (*''*)

— *info* = sériové číslo VU stanovené v CSM_123

— K_VU_{DSRC}_ENC = první *L* oktety *OKM* a

K_VU_{DSRC}_MAC = poslední *L* oktety *OKM*

kde *L* je požadovaná délka K_VU_{DSRC}_ENC a K_VU_{DSRC}_MAC v oktetech.

CSM_125 MSCA musí bezpečným způsobem předat K_VU_{DSRC}_ENC and K_VU_{DSRC}_MAC výrobci VU k vložení do určeného celku ve vozidle.

CSM_126 Při vydání musí mít celek ve vozidle ve své zabezpečené paměti uloženy K_VU_{DSRC}_ENC a K_VU_{DSRC}_MAC, aby mohl zaručit integritu, pravost a důvěrnost dat zasílaných prostřednictvím kanálu vzdálené komunikace. Celek ve vozidle musí mít rovněž uloženo číslo verze hlavního klíče DSRC používaného pro odvozování těchto klíčů vyhrazených příslušným VU.

CSM_127 Při vydání musí mít kontrolní karty a karty dílny ve své zabezpečené paměti uloženy KM_{DSRC}, aby mohly zaručit integritu a pravost dat zasílaných VU prostřednictvím kanálu vzdálené komunikace a dekódovat tato data. Kontrolní karty a karty dílny musí mít rovněž uložené číslo verze hlavního klíče DSRC.

Poznámka: Podle pokynů v části 9.2.2.2 musí být do jediné karty dílny nebo kontrolní karty prakticky možné vkládat více generací KM_{DSRC}.

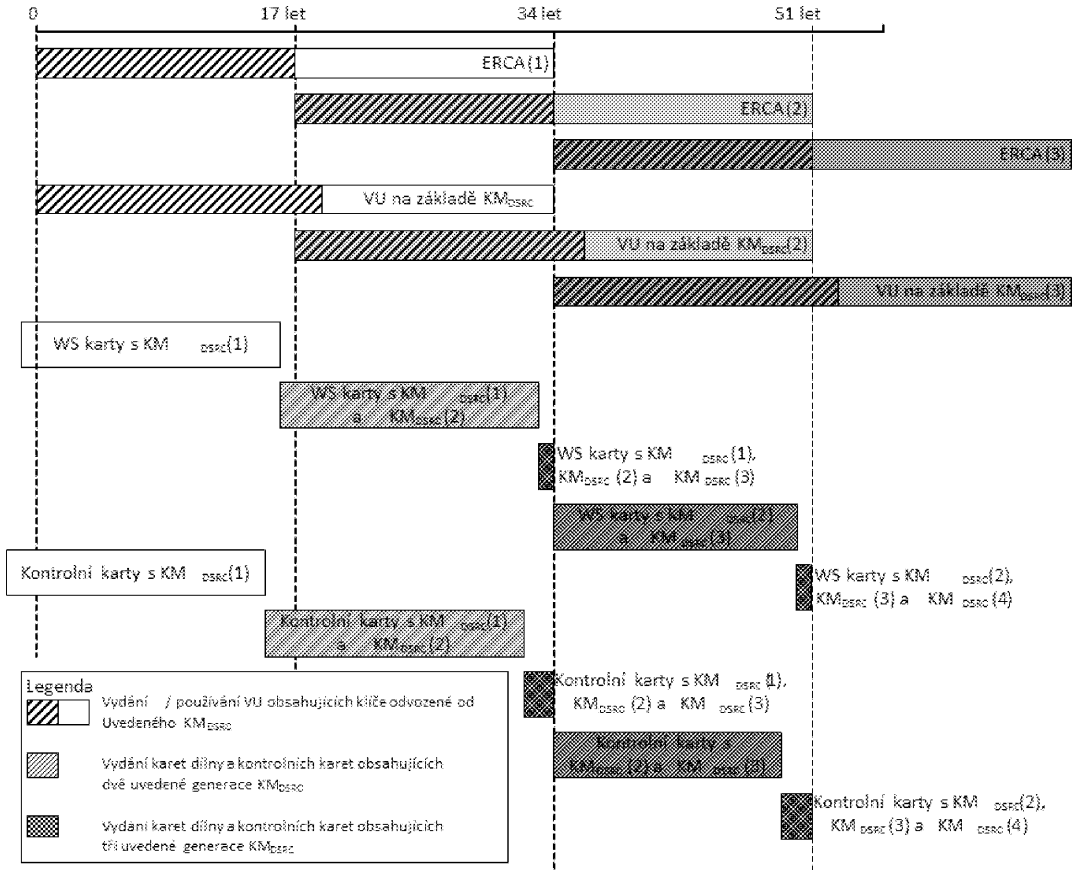
CSM_128 MSCA musí udržovat záznamy všech klíčů DSRC vyhrazených příslušným VU, které generoval, jejich čísla verze a identifikaci VU, pro které byla každá sada klíčů určena.

9.2.2.2 *Výměna hlavního klíče DSRC*

CSM_129 Každý hlavní klíč DSRC je přiřazen určité generaci kořenového páru klíčů ERCA. ERCA proto musí vyměnit hlavní klíč DSRC každých 17 let. Doba platnosti každé generace hlavního klíče DSRC musí začínat dva roky před vstupem přiřazeného kořenového páru klíčů ERCA v platnost a musí končit se skončením platnosti přiřazeného kořenového páru klíčů ERCA. To je znázorněno na Obrázek 3.

Obrázek 3

Vydávání a používání různých generací hlavního klíče DSRC v celcích ve vozidle, kartách dílny a kontrolních kartách



CSM_130 Nejméně dva roky před generováním nového evropského kořenového páru klíčů podle popisu v CSM_56 musí ERCA generovat nový hlavní klíč DSRC. Délka klíče DSRC musí být spojena s předpokládanou sílou nového evropského kořenového páru klíčů podle CSM_50. ERCA musí na požádání MSCA sdělit nový hlavní klíč DSRC společně s jeho číslem verze.

CSM_131 MSCA musí zajistit uložení všech platných generací $K_{M\text{-}WC}$ do každé kontrolní karty vydané v rámci jeho pravomoci společně s jejich čísly verze podle Obrázek 3.

Poznámka: To předpokládá, že v posledních dvou letech doby platnosti certifikátu ERCA budou kontrolní karty vydávány se třemi různými generacemi KM_{DSRC}, jak je znázorněno na Obrázek 3.

CSM_132 MSCA musí zajistit, aby všechny generace KM_{DSRC}, které byly platné nejméně rok a jsou stále platné, byly uloženy v každé kartě dílny vydané v rámci jeho pravomoci společně s jejich čísly verze jak je znázorněno na Obrázek 3.

Poznámka: To předpokládá, že v posledním roce doby platnosti certifikátu ERCA budou vydány karty dílny se třemi různými generacemi KM_{DSRC}, jak je znázorněno na Obrázek 3.

CSM_133 Výrobci celků ve vozidle musí do každého celku ve vozidle vložit pouze jednu sadu klíčů DSRC vyhrazených příslušným VU společně s jejich číslem verze. Tato sada klíčů musí být odvozena z generace KM_{DSRC} spojené s certifikátem ERCA, na němž jsou založeny certifikáty VU.

Poznámky:

— To předpokládá, že celek ve vozidle založený na certifikátu ERCA generace *X* musí obsahovat pouze K_VU_{DSRC}_ENC and K_VU_{DSRC}_MAC generace *X*, i když je VU vydán po začátku doby platnosti certifikátu ERCA generace *X+1*. To je znázorněno na Obrázek 3.

— Protože karty dílny mají dobu platnosti jeden rok a kontrolní karty dva roky, výsledkem CSM_131 – CSM_133 je, že všechny karty dílny a kontrolní karty obsahují nový hlavní klíč DSRC v okamžiku, kdy je vydán první VU obsahující klíče vyhrazené příslušným VU na základě tohoto hlavního klíče.

9.3. **Certifikáty**

9.3.1 *Obecné informace*

CSM_134 Všechny certifikáty v systému evropského inteligentního tachografu musí být samopopisné, kartou ověřitelné (CV) certifikáty podle [ISO 7816-4] a [ISO 7816-8].

CSM_135 Zvláštní kódovací pravidla (DER) podle [ISO 8825-1] musí být užívána pro kódování datových struktur ASN.1 i datových objektů (podle konkrétní aplikace) v certifikátech.

Poznámka: Toto kódování má za následek následující strukturu hodnoty délky tagu (TLV):

Tag: Tag je kódován v jednom nebo dvou oktetech a indikuje obsah.

Délka: Délka je kódována jako nepodepsané celé číslo v jednom, dvou nebo třech oktetech, což má za následek maximální délku 65 535 oktetů. Používá se minimální počet oktetů.

Hodnota: Hodnota je kódována v nula nebo více oktetech

9.3.2 *Obsah certifikátu*

CSM_136 Všechny certifikáty musí mít strukturu uvedenou v profilu certifikátu v Tabulka 4.

Tabulka 4

Profil certifikátu verze 1

Pole	ID pole	Tag	Délka (bajty)	Datový typ ASN.1 (viz dodatek 1)
Certifikát ECC	C	'7F 21'	var	
Tělo certifikátu ECC	B	'7F 4E'	var	

Pole	ID pole	Tag	Délka (bajty)	Datový typ ASN.1 (viz dodatek 1)
Identifikátor profilu certifikátu	CPI	'5F 29'	'01'	INTEGER(0..255)
Odkaz na certifikační orgán	CAR	'42'	'08'	KeyIdentifier
Autorizace držitele certifikátu	CHA	'5F 4C'	'07'	CertificateHolder Authorisation
Veřejný klíč	PK	'7F 49'	var	
Parametry domény	DP	'06'	var	OBJECT IDENTIFIER
Veřejný bod	PP	'86'	var	OCTET STRING
Odkaz na držitele certifikátu	CHR	'5F 20'	'08'	KeyIdentifier
Datum účinnosti certifikátu	CEfD	'5F 25'	'04'	TimeReal
Datum konce platnosti certifikátu	CExD	'5F 24'	'04'	TimeReal
Podpis certifikátu ECC	S	'5F 37'	var	OCTET STRING

Poznámka: ID pole se užívá v dalších částech tohoto dodatku pro označení jednotlivých polí certifikátu, např. X.CAR je odkaz na certifikační orgán uvedený v certifikátu uživatele X.

9.3.2.1 Identifikátor profilu certifikátu

CSM_137 Certifikáty musí používat identifikátor profilu certifikátu pro označení používaného profilu certifikátu. Verze 1 podle Tabulka 4 musí být označena hodnotou '00'.

9.3.2.2 Odkaz na certifikační orgán

CSM_138 Odkaz na certifikační orgán se užívá pro identifikaci veřejného klíče užívaného pro ověření podpisu certifikátu. Odkaz na certifikační orgán proto musí být stejný jako odkaz na držitele certifikátu v certifikátu příslušné certifikační autority.

CSM_139 Kořenový certifikát ERCA musí být samočinně podepsaný, tj. odkaz na certifikační orgán a odkaz na držitele certifikátu musí být v certifikátu stejné.

CSM_140 Pro spojovací certifikát ERCA musí být odkaz na držitele certifikátu stejný jako CHR nového kořenového certifikátu ERCA. Odkaz na certifikační orgán pro spojovací certifikát musí být stejný jako CHR předchozího kořenového certifikátu ERCA.

9.3.2.3 Autorizace držitele certifikátu

CSM_141 Oprávnění držitele certifikátu se užívá pro identifikaci typu certifikátu. Obsahuje šest nejdůležitějších bajtů ID aplikace tachografu kaskádově spojených s typem zařízení, pro něž je certifikát určen.

9.3.2.4 Veřejný klíč

Veřejný klíč obsahuje dva datové prvky: standardní parametry domény užívané s veřejným klíčem v certifikátu a hodnotu veřejného bodu.

CSM_142 Datový prvek parametry domény musí obsahovat jeden z identifikátorů objektu uvedených v Tabulka 1 pro označení odkazu na sadu standardních parametrů domény.

CSM_143 Datový prvek veřejný bod musí obsahovat veřejný bod. Veřejné body eliptických křivek musí být konvertovány na oktetové řetězce podle [TR-03111]. Musí být použit nekomprimovaný kódovací formát. Při získávání bodu eliptické křivky z jeho kódovaného formátu musí být vždy provedeny validace podle [TR-03111].

9.3.2.5 Odkaz na držitele certifikátu

CSM_144 Odkaz na držitele certifikátu je identifikátor pro veřejný klíč poskytovaný v certifikátu. Užívá se pro označení tohoto veřejného klíče v jiných certifikátech.

CSM_145 Pro certifikáty karet a certifikáty vnějších zařízení GNSS musí mít odkaz na držitele certifikátu datový typ `ExtendedSerialNumber` uvedený v dodatku 1.

CSM_146 Pro celky ve vozidle výrobce při podání žádosti o certifikát může nebo nemusí znát specifické sériové číslo výrobce VU, pro nějž je tento certifikát a příslušný soukromý klíč určen. V prvním případě musí mít odkaz na držitele certifikátu datový typ `ExtendedSerialNumber` podle dodatku 1. Ve druhém případě musí mít odkaz na držitele certifikátu datový typ `CertificateRequestID` podle dodatku 1.

CSM_147 Pro certifikáty ERCA a MSCA musí mít odkaz na držitele certifikátu datový typ `CertificationAuthorityKID` podle dodatku 1.

9.3.2.6 Datum účinnosti certifikátu

CSM_148 Datum účinnosti certifikátu musí označovat počáteční datum a délku doby platnosti certifikátu. Datum účinnosti certifikátu musí být datem generování certifikátu.

9.3.2.7 Datum konce platnosti certifikátu

CSM_149 Datum konce platnosti certifikátu musí označovat konečné datum a délku doby platnosti certifikátu.

9.3.2.8 Podpis certifikátu

CSM_150 Podpis certifikátu musí být vytvořen na kódovaném těle certifikátu, včetně tagu a délky těla certifikátu. Podpisový algoritmus musí být ECDSA podle [DSS], který používá hašovací algoritmus spojený s velikostí klíče podepisujícího orgánu podle CSM_50. Formát podpisu musí být otevřený podle [TR-03111].

9.3.3 *Podání žádosti o certifikát*

CSM_151 Při podání žádosti o certifikát musí žádající strana zaslat svému certifikačnímu orgánu tyto údaje:

— identifikátor profilu požadovaného certifikátu,

— odkaz na certifikační orgán, který se má použít při podpisu certifikátu,

— veřejný klíč, který má být podepsán.

CSM_152 Kromě údajů v CSM_151 musí MSCA zaslat ERCA v žádosti o certifikát tyto údaje, které ERCA umožní vytvořit odkaz na držitele certifikátu nového certifikátu MSCA:

— číselný kód státu certifikační autority (datový typ `NationNumeric` stanovený v dodatku 1),

— alfanumerický kód státu certifikační autority (datový typ `NationAlpha` stanovený v dodatku 1),

— jednobajtové sériové číslo pro rozlišení různých klíčů certifikační autority v případě výměny klíčů,

— dvoubajtové pole obsahující doplňkové informace příslušné certifikační autority.

CSM_153 Kromě údajů v CSM_151 musí výrobce zařízení zaslat MSCA v žádosti o certifikát tyto údaje, které MSCA umožní vytvořit odkaz na držitele nového certifikátu zařízení:

— identifikátor výrobce typu 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 vrátí MSCA, do určeného zařízení.

CSM_154 Pokud jde o VU, výrobce při podání žádosti o certifikát může a nemusí znát specifické sériové číslo výrobce VU, pro nějž je tento certifikát a příslušný soukromý klíč určen. Je-li toto číslo známo, musí výrobce VU zaslat sériové číslo MSCA. Není-li známo, musí výrobce jedinečně označit každou žádost o certifikát a toto sériové číslo žádosti o certifikát zaslat MSCA. Výsledný certifikát potom obsahuje sériové číslo žádosti o certifikát. Po vložení certifikátu do specifického VU musí výrobce sdělit MSCA spojení mezi sériovým číslem žádosti o certifikát a označením VU.

10. VZÁJEMNÉ OVĚŘOVÁNÍ PRAVOSTI A BEZPEČNÉ PŘEDÁVÁNÍ ZPRÁV VU A KARTY

10.1. **Obecné informace**

CSM_155 Bezpečná komunikace na vysoké úrovni mezi celkem ve vozidle a kartou tachografu je založena na těchto krocích:

— Za prvé, každá strana musí druhé straně prokázat, že vlastní platný certifikát veřejného klíče podepsaný certifikačním orgánem členského státu. Certifikát veřejného klíče MSCA musí být navíc podepsán Evropským úřadem kořenových certifikátů. Tento krok se nazývá ověřením řetězce certifikátů a je podrobně popsán v části 10.2.

— Za druhé, celek ve vozidle musí kartě prokázat, že vlastní soukromý klíč odpovídající veřejnému klíči příslušného certifikátu. Učiní tak podpisem náhodného čísla zaslaného kartou. Karta ověří podpis náhodného čísla. Je-li toto ověření úspěšné, je ověřena pravost VU. Tento krok se nazývá ověření pravosti VU a je podrobně popsán v části 10.3.

— Za třetí, obě strany nezávisle vypočítají dva klíče relace AES pomocí algoritmu odsouhlasení asymetrického klíče. Pomocí jednoho z těchto klíčů relace karta vytvoří kód ověřování zprávy (MAC) pro určitá data zaslaná z VU. VU ověří MAC. Je-li toto ověření úspěšné, je ověřena pravost karty. Tento krok se nazývá ověření pravosti karty a je podrobně popsán v části 10.4.

— Za čtvrté, VU a karta musí užívat odsouhlasené klíče relace pro zajištění důvěrnosti, integrity a pravosti všech vyměňovaných zpráv. Tento proces se nazývá bezpečné předávání práv a je podrobně popsán v části 10.5.

CSM_156 Mechanismus popsaný v CSM_155 musí být aktivován celkem ve vozidle při každém vložení karty do některého z jeho slotů.

10.2. **Vzájemné ověření řetězce certifikátů**

10.2.1 *Ověření řetězce certifikátů karty celkem ve vozidle*

CSM_157 Celky ve vozidle musí pro ověření řetězce certifikátů karty tachografu užívat protokol popsaný na Obrázek 4.

Poznámky k Obrázek 4:

— Certifikáty a veřejné klíče karty uvedené na obrázku se používají pro vzájemné ověřování pravosti. V části 9.1.5 jsou označeny jako Card_MA.

— Certifikáty a veřejné klíče Card.CA uvedené na obrázku se používají pro podpis certifikátů karet a jsou uvedeny v CAR certifikátu karty. V bodě 9.1.3 jsou označeny jako MSCA_Card.

— Certifikát Card.CA.EUR uvedený na obrázku je evropský kořenový certifikát, který je uveden v CAR certifikátu Card.CA.

— Certifikát Card.Link uvedený na obrázku je případný spojovací certifikát karty. Jak je uvedeno v části 9.1.2, jedná se o spojovací certifikát pro nový evropský kořenový pár klíčů vytvořený ERCA a podepsaný předchozím evropským soukromým klíčem.

— Certifikát Card.Link.EUR je evropský kořenový certifikát, který je uveden v CAR certifikátu Card.Link.

CSM_158 Jak je uvedeno v Obrázek 4, ověření řetězce certifikátů karty se zahájí po vložení karty. Celek ve vozidle přečte z EF ICC odkaz na držitele karty (`cardExtendedSerialNumber`). VU musí zkontrolovat, zda kartu zná, tj. zda řetězec certifikátů karty úspěšně ověřil v minulosti a uložil jej pro budoucí potřebu. Pokud ano a certifikát karty je dosud platný, pokračuje proces ověřením řetězce certifikátů VU. V opačném případě VU postupně z karty přečte certifikát MSCA_Card užívaný pro ověření certifikátu karty, certifikát Card.CA. EUR užívaný pro ověření certifikátu MSCA_Card a případně spojovací certifikát, dokud nenalezne certifikát, který zná nebo který může ověřit. Pokud takový certifikát nalezne, VU tento certifikát použije pro ověření příslušných certifikátů karty, které z karty přečetl. Je-li tento krok úspěšný, pokračuje proces ověřením řetězce certifikátů VU. Není-li úspěšný, VU kartu ignoruje.

Poznámka: Existují tři způsoby, jak může VU znát certifikát Card.CA.EUR:

— certifikát Card.CA.EUR je stejný certifikát jako vlastní certifikát EUR ve VU,

— Card.CA.EUR certifikát byl vydán dříve než vlastní certifikát EUR ve VU a VU tento certifikát obsahoval již při vydání (viz CSM_81),

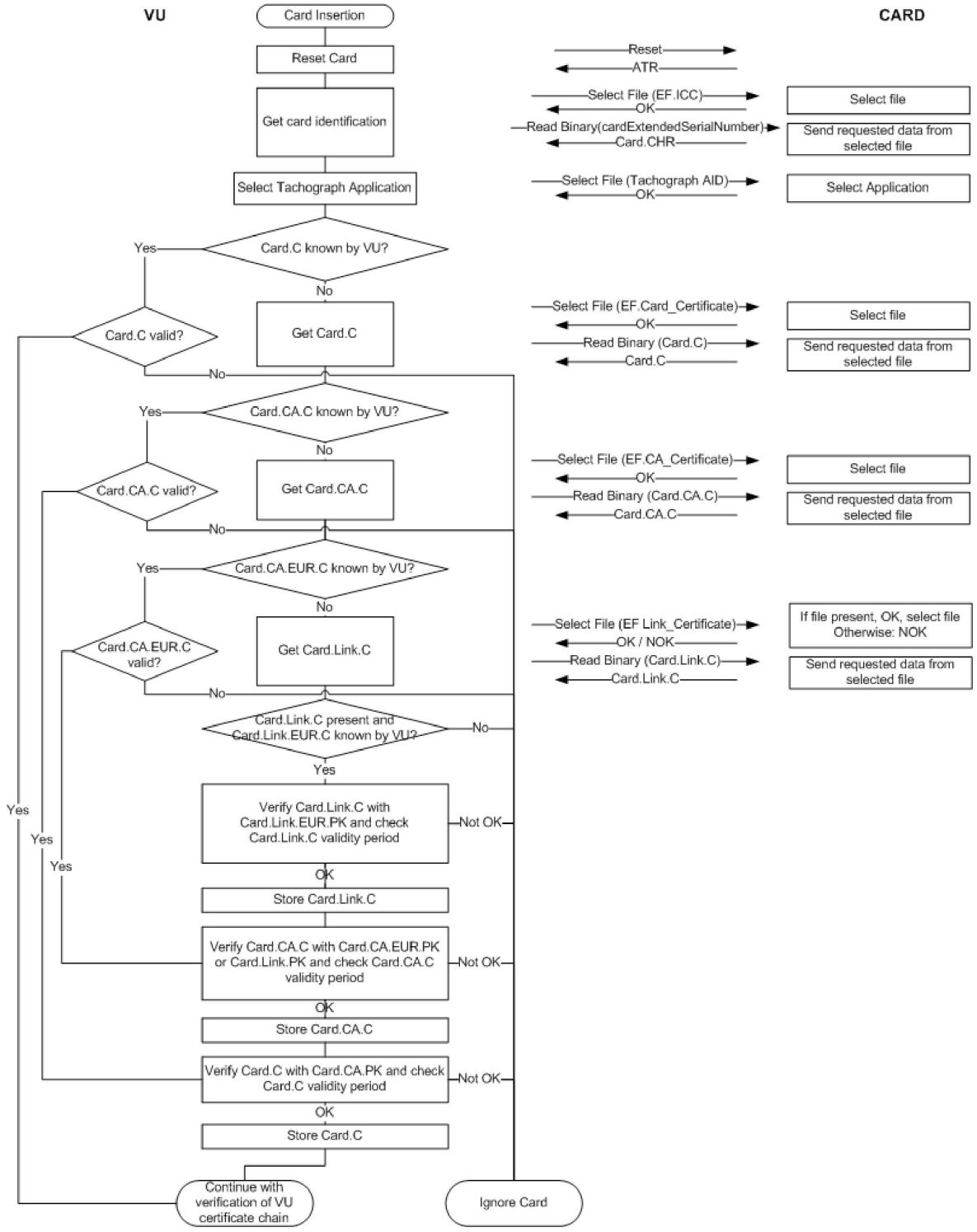
— Card:CA.EUR certifikát byl vydán až po vlastním certifikátu EUR ve VU a VU v minulosti přijal spojovací certifikát z jiné karty tachografu, ověřil jej a uložil pro budoucí potřebu.

CSM_159 Jak je uvedeno v Obrázek 4, jakmile VU prokáže pravost a platnost dříve neznámého certifikátu, může tento certifikát uložit pro budoucí potřebu, aby nemusel pravost tohoto certifikátu ověřovat znovu, až bude VU opět předložen. Místo uložení celého certifikátu může VU uložit pouze obsah těla certifikátu, jak je uvedeno v části 9.3.2.

CSM_160 VU musí ověřit aktuální platnost každého certifikátu přečteného z karty nebo uloženého do své paměti a musí zamítnout certifikáty se skončenou platností. Pro ověření aktuální platnosti certifikátu předloženého kartou musí VU užít své vnitřní hodiny.

Obrázek 4

Protokol pro ověření řetězce certifikátů karty celkem ve vozidle

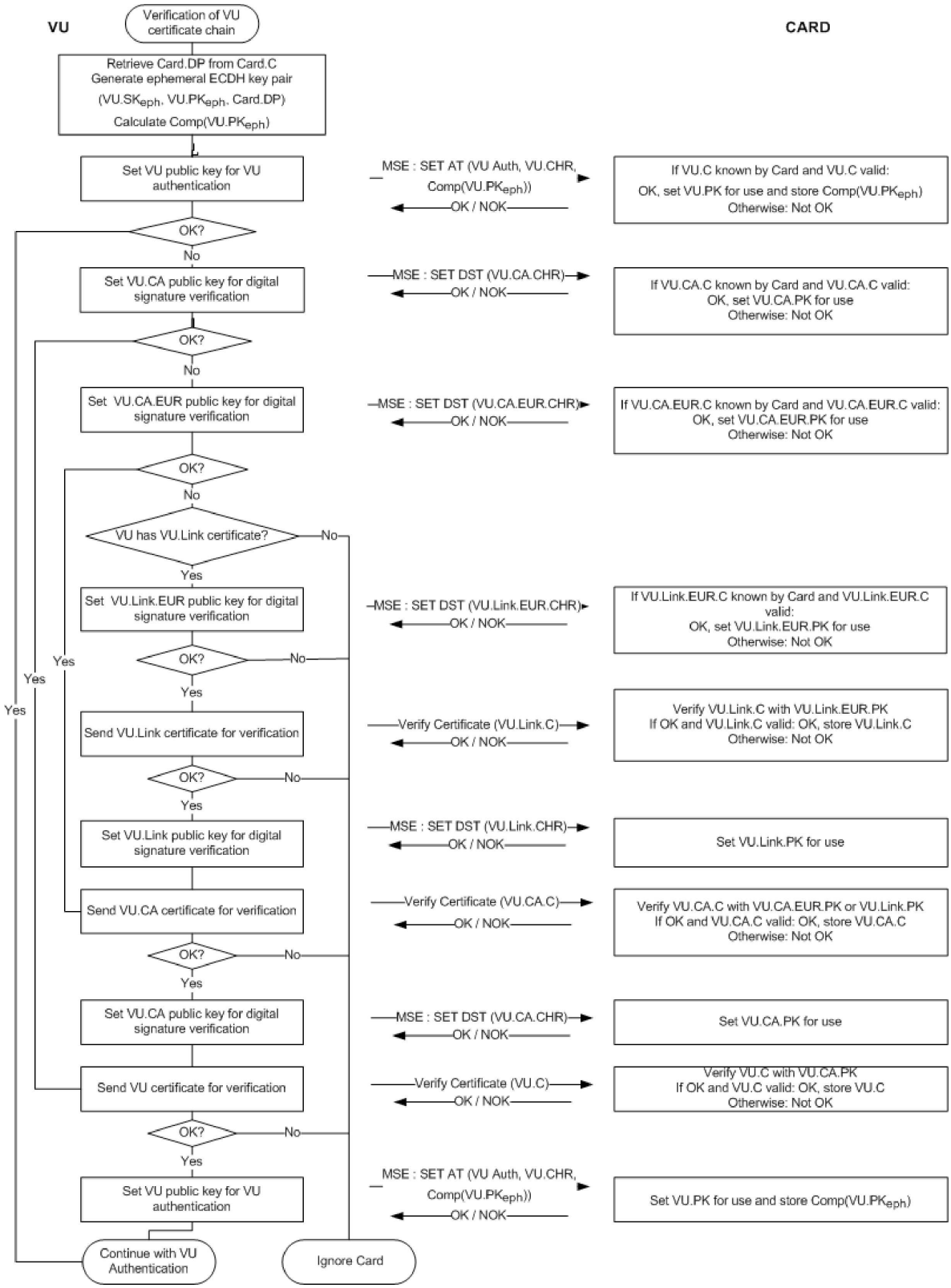


10.2.2 *Ověření řetězce certifikátů VU kartou*

CSM_161 Karty tachografu musí pro ověření řetězce certifikátů VU užívat protokol popsaný na Obrázek 5.

Obrázek 5

Protokol pro ověření řetězce certifikátů karty celkem ve vozidle



Poznámky k Obrázek 5:

— Certifikáty a veřejné klíče VU uvedené na obrázku se používají pro vzájemné ověřování pravosti. V části 9.1.4 jsou označeny jako VU_MA.

— Certifikáty a veřejné klíče VU.CA uvedené na obrázku se používají pro podpis certifikátů VU a vnějších zařízení GNSS. V části 9.1.3 jsou označeny jako MSCA_VU-EGF.

— Certifikát VU.CA.EUR uvedený na obrázku je evropský kořenový certifikát, který je uveden v CAR certifikátu VU.CA.

— Certifikát VU.Link uvedený na obrázku je případný spojovací certifikát VU. Jak je uvedeno v části 9.1.2, jedná se o spojovací certifikát pro nový evropský kořenový pár klíčů vytvořený ERCA a podepsaný předchozím evropským soukromým klíčem.

— Certifikát VU.Link.EUR je evropský kořenový certifikát, který je uveden v CAR certifikátu VU.Link.

CSM_162 Jak je uvedeno v Obrázek 5, ověření řetězce certifikátů celku ve vozidle se zahájí v okamžiku, kdy se celek ve vozidle pokouší nastavit vlastní veřejný klíč pro používání v kartě tachografu. Pokud se to podaří, znamená to, že karta v minulosti úspěšně ověřila řetězec certifikátů VU a uložila certifikát VU pro budoucí potřebu. V tomto případě se certifikát VU nastaví pro použití a proces pokračuje ověřením pravosti VU. Pokud karta certifikát VU nezná, VU postupně předloží certifikát VU.CA užívaný pro ověření certifikátu VU, certifikát VU.CA.EUR užívaný pro ověření certifikátu VU.CA a případně spojovací certifikát, aby tak byl nalezen certifikát, který karta zná. Je-li takový certifikát nalezen, karta tento certifikát použije pro ověření příslušných certifikátů VU, které jí jsou předloženy. Je-li tento krok úspěšný, VU nakonec nastaví svůj veřejný klíč pro užití v kartě tachografu. Není-li úspěšný, VU kartu ignoruje.

Poznámka: Existují tři způsoby, jak může karta poznat certifikát VU.CA.EUR:

— certifikát VU.CA.EUR je stejný certifikát jako vlastní certifikát EUR karty,

— certifikát VU.CA.EUR byl vydán dříve než vlastní certifikát EUR karty a karta tento certifikát obsahovala již při vydání (viz CSM_91),

— certifikát VU.CA.EUR byl vydán až po vlastním certifikátu EUR karty a karta v minulosti přijala spojovací certifikát z jiného celku ve vozidle, ověřila jej a uložila pro budoucí potřebu.

CSM_163 VU použije příkaz MSE: Set AT pro nastavení svého veřejného klíče pro užití v kartě tachografu. Jak je uvedeno v dodatku 2, tento příkaz obsahuje označení kryptografického mechanismu, který bude použit se stanoveným klíčem. Tímto mechanismem je „Ověřování pravosti VU pomocí algoritmu ECDSA ve spojení s hašovacím algoritmem spojeným s velikostí klíče páru klíčů VU_MA celku ve vozidle, jak je uvedeno v CSM_50“.

CSM_164 Příkaz MSE: Set AT rovněž obsahuje označení přechodného páru klíčů, který VU použije při odsouhlasení klíče relace (viz část 10.4). Před zasláním příkazu MSE: Set AT proto VU vygeneruje přechodný pár klíčů ECC. Pro generování přechodného páru klíčů VU použije standardní parametry domény uvedené v certifikátu karty. Přechodný pár klíčů je označen jako ($VU.SK_{eph}$, $VU.PK_{eph}$, Card.DP). VU použije souřadnici x přechodného veřejného bodu ECDH jako označení klíče; toto se nazývá komprimované zastoupení veřejného klíče a označuje se jako $Comp(VU.PK_{eph})$.

CSM_165 Je-li příkaz MSE: Set AT úspěšný, karta nastaví uvedený VU.PK pro následující použití během ověřování pravosti vozidla a přechodně uloží $Comp(VU.PK_{eph})$. Jsou-li před odsouhlasením klíče relace zaslány dva nebo více úspěšných příkazů MSE: Set AT, karta uloží pouze poslední přijatý $Comp(VU.PK_{eph})$.

CSM_166 Karta musí ověřit dočasnou platnost všech certifikátů, které VU předloží nebo na které odkazuje při uložení do paměti karty, a musí zamítnout certifikáty se skončenou platností.

CSM_167 Pro ověření dočasné platnosti certifikátu předloženého celkem ve vozidle musí každá karta tachografu interně ukládat určitá data představující aktuální čas. Tato data nesmí být celkem ve vozidle přímo aktualizovatelná. Při vydání musí být aktuální čas karty nastaven na datum účinnosti certifikátu Card_MA karty. Karta svůj aktuální čas aktualizuje, je-li datum účinnosti certifikátu s původním platným zdrojem času předloženého celkem ve vozidle pozdější než aktuální čas karty. V tomto případě karta nastaví svůj aktuální čas na datum účinnosti tohoto certifikátu. Karta jako platný zdroj času přijme pouze tyto certifikáty:

— spojovací certifikáty ERCA druhé generace,

— certifikáty MSCA druhé generace,

— certifikáty VU druhé generace vydané stejnou zemí jako vlastní certifikát(y) karty.

Poznámka: Poslední požadavek předpokládá, že karta musí být schopna rozeznat CAR certifikátu VU, tj. certifikát MSCA_VU-EGF. Ten nebude stejný jako CAR jejího vlastního certifikátu, kterým je certifikát MSCA_Card.

CSM_168 Jak je uvedeno v Obrázek 5, jakmile karta ověří pravost a platnost dříve neznámého certifikátu, může tento certifikát uložit pro budoucí potřebu, aby nemusela pravost tohoto certifikátu ověřovat znovu, až bude kartě opět předložen. Místo uložení celého certifikátu může karta uložit pouze obsah těla certifikátu, jak je uvedeno v části 9.3.2.

10.3. **Ověření pravosti VU**

CSM_169 Celky ve vozidle a karty musí používat protokol ověřování pravosti VU uvedený na Obr. 6 pro prokázání pravosti VU vůči kartě. Ověřování pravosti VU umožňuje kartě tachografu jednoznačně ověřit důvěryhodnost VU. K tomuto účelu VU použije svůj soukromý klíč k podpisu výzvy generované kartou.

CSM_170 Kromě samotného podpisu výzvy karty musí VU do podpisu vložit odkaz na držitele karty zjištěný z certifikátu karty.

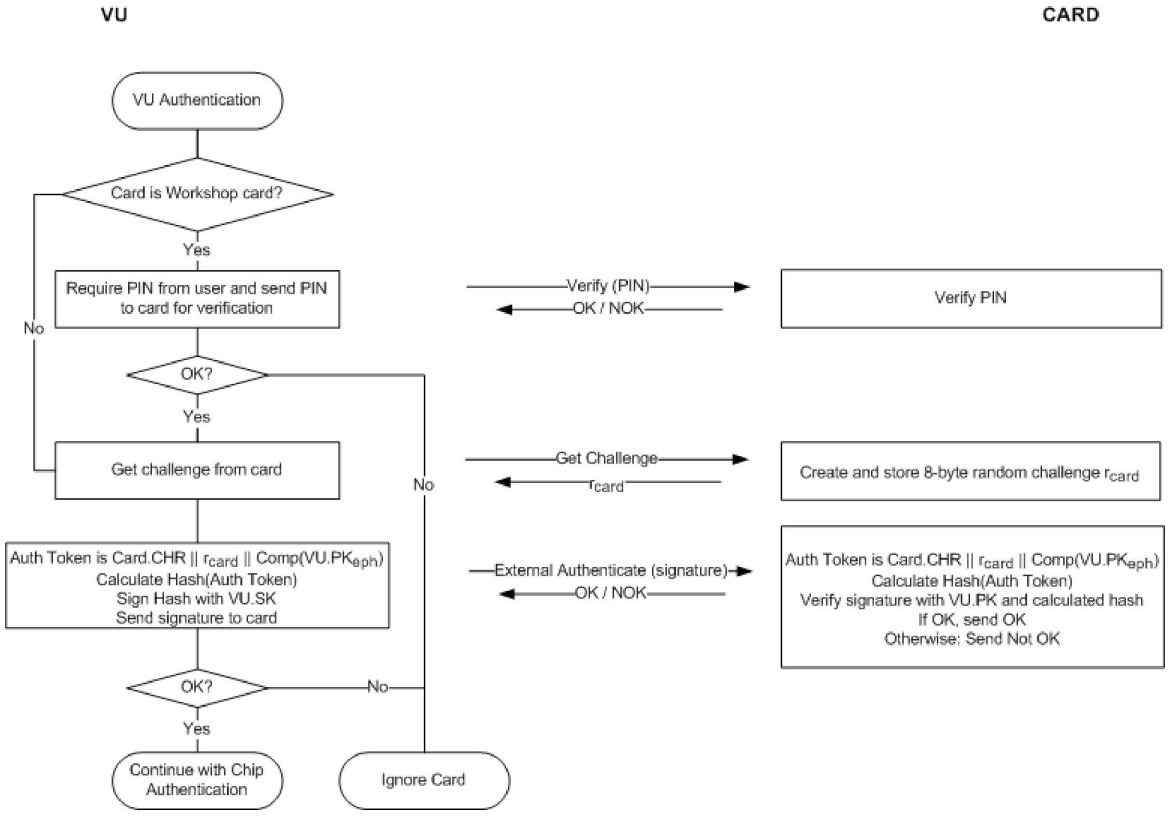
Poznámka: Tento postup zajišťuje, že karta, které VU prokazuje svou pravost, je stejná karta, jejíž řetězec certifikátů VU dříve ověřil.

CSM_171 VU musí rovněž do podpisu vložit identifikátor přechodného veřejného klíče Comp(VU.PK_{eph}), který bude VU používat pro zajištění bezpečného předávání zpráv během procesu ověřování pravosti čipu stanoveného v části 10.4.

Poznámka: Tento postup zajišťuje, že VU, se kterým karta komunikuje během relace bezpečného předávání zpráv, je ten VU, jehož pravost byla ověřena kartou.

Obr. 6

Protokol ověřování pravosti VU



CSM_172 Pokud během ověřování pravosti VU celek ve vozidle odešle vícenásobné příkazy GET CHALLENGE, karta vždy vrátí novou osmibajtovou náhodnou výzvu, ale uloží pouze poslední výzvu.

CSM_173 Podpisový algoritmus užívaný celkem ve vozidle pro ověřování pravosti VU musí být ECDSA podle pokynů v [DSS], který používá hašovací algoritmus spojený s velikostí klíče páru klíčů VU_MA celku ve vozidle podle CSM_50. Formát podpisu musí být otevřený podle [TR-03111]. VU zašle výsledný podpis kartě.

CSM_174 Po přijetí podpisu VU v příkazu EXTERNAL AUTHENTICATE musí karta

— vypočítat ověřovací token kaskádovým spojením Card.CHR, výzvu karty r_{card} a identifikátor přechodného veřejného klíče Comp($VU.PK_{eph}$) celku ve vozidle,

— vypočítat hash pro ověřovací token pomocí hašovacího algoritmu spojeného s velikostí klíče páru klíčů VU_MA celku ve vozidle podle CSM_50,

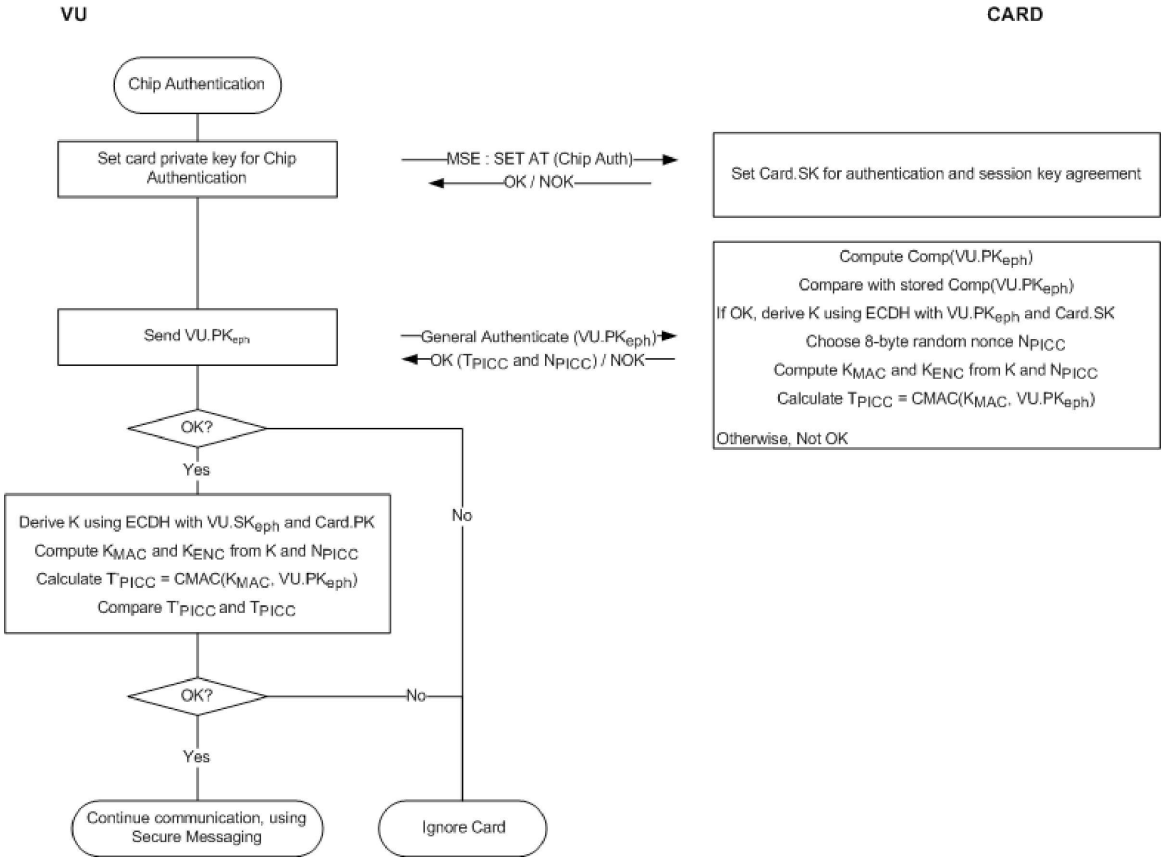
— ověřit podpis VU pomocí algoritmu ECDSA ve spojení s VU.PK a vypočítanou hash.

10.4. Ověření pravosti čipu a odsouhlasení klíče relace

CSM_175 Celky ve vozidle a karty musí užívat protokol ověřování pravosti čipu uvedený na **Obr. 7** pro ověření pravosti karty vůči VU. Ověření pravosti čipu umožňuje celku ve vozidle jednoznačně ověřit důvěryhodnost karty.

Obr. 7

Ověření pravosti čipu a odsouhlasení klíče relace



CSM_176 VU a karta musí provést tyto kroky:

1. Celek ve vozidle zahájí proces ověření pravosti čipu zasláním příkazu MSE: Set AT, který znamená „Ověření pravosti čipu pomocí algoritmu ECDH pro vytvoření délky klíče relace AES spojené s velikostí klíče páru klíčů Card_MA karty, jak je uvedeno v CSM_50“. VU určí velikost klíče páru klíčů karty z certifikátu karty.

2. VU zašle kartě veřejný bod $VU.PK_{eph}$ svého přechodného páru klíčů. 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.

3. Karta vypočítá $Comp(VU.PK_{eph})$ z $VU.PK_{eph}$ a porovná jej s uloženou hodnotou $Comp(VU.PK_{eph})$.

4. Pomocí algoritmu ECDH ve spojení se statickým soukromým klíčem karty a přechodným veřejným klíčem VU karta vypočítá tajnou hodnotu K.

5. Karta zvolí náhodnou 8bajtovou hodnotu nonce N_{PICC} a použije ji pro odvození dvou klíčů relace AES K_{MAC} a K_{ENC} z hodnoty K. Viz CSM_179.

6. Pomocí K_{MAC} karta vypočítá ověřovací token pro identifikátor přechodného veřejného klíče VU: $T_{PICC} = CMAC(K_{MAC}, VU.PK_{eph})$. Karta zašle N_{PICC} a T_{PICC} celku ve vozidle.

7. Pomocí algoritmu ECDH ve spojení se statickým veřejným klíčem karty a přechodným soukromým klíčem VU celek ve vozidle vypočítá stejnou tajnou hodnotu K jako karta v kroku 4.

8. VU odvodí klíče relace K_{MAC} a K_{ENC} z K a N_{PICC}; viz CSM_179.

9. VU ověří značku prokázání pravosti T_{PICC}.

CSM_177 V kroku 3 výše musí karta vypočítat Comp(VU.PKeph) jako souřadnici x veřejného bodu ve VU. PKeph.

CSM_178 V krocích 4 a 7 výše musí karta a celek ve vozidle použít algoritmus ECKA-EG stanovený v [TR-03111].

CSM_179 V krocích 5 a 8 výše musí karta a celek ve vozidle použít funkci odvození klíče pro klíče relace AES stanovené v [TR-03111] s touto přesností a změnami:

— Hodnota čítače musí být '00 00 00 01' pro K_{ENC} a '00 00 00 02' pro K_{MAC}.

— Musí být použita volitelná hodnota nonce *r* odpovídající hodnotě N_{PICC}.

— Pro odvození 128-bitových klíčů AES musí být použit hašovací algoritmus SHA-256.

— Pro odvození 192-bitových klíčů AES musí být použit hašovací algoritmus SHA-384.

— Pro odvození 256-bitových klíčů AES musí být použit hašovací algoritmus SHA-512.

Délka klíčů relace (tj. délka, při níž je hash přerušen) musí být spojena s velikostí páru klíčů Card_MA podle CSM_50.

CSM_180 V krocích 6 a 9 výše musí karta a celek ve vozidle použít algoritmus AES v režimu CMAC podle [SP 800-38B]. Délka T_{PICC} musí být spojena s délkou klíčů relace AES podle CSM_50.

10.5. **Bezpečné předávání zpráv**

10.5.1 *Obecné informace*

CSM_181 Všechny příkazy a odpovědi vyměňované mezi celkem ve vozidle a kartou tachografu po úspěšném ověření pravosti čipu a do skončení relace musí být chráněny bezpečným předáváním zpráv.

CSM_182 S výjimkou čtení ze souboru s podmínkou přístupu SM-R-ENC-MAC-G2 (viz dodatek 2, část 4) musí být bezpečné předávání zpráv užíváno pouze v režimu ověřování pravosti. V tomto režimu je kryptografický kontrolní součet (MAC) přidáván ke všem příkazům a odpovědím pro zajištění pravosti a integrity zpráv.

CSM_183 Při čtení dat ze souboru s podmínkou přístupu SM-R-ENC-MAC-G2 musí být bezpečné předávání zpráv používáno v režimu šifrování a následného prokazování pravosti, tj. data odezvy jsou nejprve šifrována pro zajištění důvěrnosti zprávy a následně je vypočítán MAC pro formátovaná šifrovaná data pro zajištění pravosti a integrity.

CSM_184 Bezpečné předávání zpráv musí užívat AES podle [AES] s klíči relace K_{MAC} a K_{ENC}, které byly odsouhlaseny během ověřování pravosti čipu.

CSM_185 Pro zabránění opakovaným útokům musí být používáno nepodepsané celé číslo jako čítač odeslané posloupnosti (SSC). Velikost SSC musí být stejná jako velikost bloku AES, tj. 128 bitů. SSC musí být ve formátu MSB-first. Čítač odeslané posloupnosti musí být při zahájení bezpečného předávání zpráv nastaven na nulu (tj. '00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00'). SSC musí být zvýšen před každým generováním příkazu nebo odezvy APDU, tj. jestliže je počáteční hodnota SSC v relaci SM 0, bude v prvním příkazu hodnota SSC 1. Hodnota SSC pro první odpověď bude 2.

CSM_186 Pro šifrování zpráv musí být užíván klíč K_{ENC} s AES v operačním módu řetězení šifrového textu (CBC) podle [ISO 10116] s vloženým parametrem m = 1 a inicializačním vektorem SV = E(K_{ENC}, SSC), tj. aktuální hodnota čítače odeslané posloupnosti šifrovaná pomocí K_{ENC}.

CSM_187 Pro ověření pravosti zpráv musí být užíván klíč K_{MAC} s AES v módu CMAC podle [SP 800-38B]. Délka MAC musí být spojena s délkou klíčů relace AES podle CSM_50. Čítač odeslané posloupnosti se do MAC vloží před datagram, který má být ověřen.

10.5.2 *Struktura bezpečné zprávy*

CSM_188 Bezpečné předávání zpráv musí užívat pouze datové objekty bezpečného předávání zpráv (viz [ISO 7816-4]) uvedené v Tabulka 5. V každé zprávě musí být tyto datové objekty použity v pořadí uvedeném v této tabulce.

Tabulka 5

Datové objekty bezpečného předávání zpráv

Název datového objektu	Tag	Přítomnost (Z)ávazná, (P)odmíněná nebo (N)epřípustná v	
		Příkazy	Odezvy
Otevřená hodnota nekódovaná v BER-TLV	'81'	C	C
Otevřená hodnota kódovaná v BER-TLV, ale neobsahující SM DO	'B3'	C	C
Indikátor doplňkového obsahu následovaný šifrovaným záznamem, otevřenou hodnotou nekódovanou v BER-TLV	'87'	C	C
Chráněné Le	'97'	C	F
Stav zpracování	'99'	F	M
Kryptografický kontrolní součet	'8E'	M	M

Poznámka: Jak je uvedeno v dodatku 2, mohou karty tachografu podporovat příkaz READ BINARY a UPDATE BINARY s lichým bajtem INS ('B1' resp. 'D7'). Tyto varianty příkazů jsou požadovány pro čtení a aktualizaci souborů s více než 32 768 bajty. V případě užití takové varianty se datový objekt s tagem 'B3' použije místo objektu s tagem '81'. Více informací v dodatku 2.

CSM_189 Všechny datové objekty SM musí být kódovány v DER TLV podle [ISO 8825-1]. Toto kódování má za následek následující strukturu hodnoty délky tagu (TLV):

Tag: Tag je kódován v jednom nebo dvou oktetech a indikuje obsah.

Délka: Délka je kódována jako nepodepsané celé číslo v jednom, dvou nebo třech oktetech, což má za následek maximální délku 65 535 oktetů. Používá se minimální počet oktetů.

Hodnota: Hodnota je kódována v nula nebo více oktetech

CSM_190 APDU chráněné bezpečným předáváním zpráv musí být vytvořeny takto:

— Záhlaví příkazu se zahrne do výpočtu MAC, proto se pro druh bajtu CLA užije hodnota '0C'.

— Jak je uvedeno v dodatku 2, musí být všechny bajty INS sudé s možnou výjimkou lichých bajtů INS pro příkazy READ BINARY a UPDATE BINARY.

— Aktuální hodnota Lc se po použití bezpečného zpracování zpráv změní na Lc'.

— Datové pole musí obsahovat datové objekty SM.

— V chráněném příkazu APDU musí být nový bajt Le nastaven na hodnotu '00'. V případě potřeby se do datového pole zařadí datový objekt '97', který vyjadřuje původní hodnotu Le.

CSM_191 Všechny datové objekty určené k šifrování musí být podle [ISO 7816-4] doplněny indikátorem doplňkového obsahu '01'. Pro výpočet MAC se každý datový objekt v APDU rovněž samostatně 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:

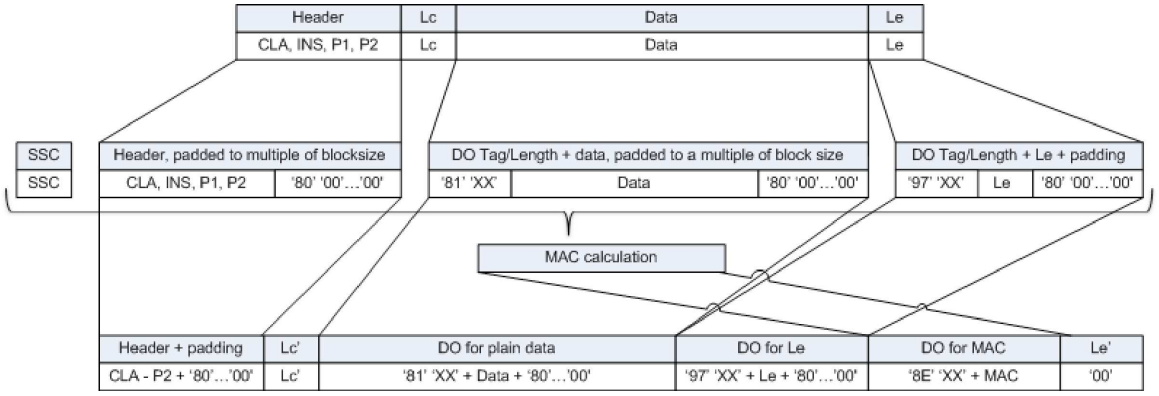
Případ 1 nebo 3:	DO '99' || DO '8E' || SW1SW2
Případ 2 nebo 4 (sudý bajt INS) se šifrováním:	DO '81' || DO '99' || DO '8E' || SW1SW2
Případ 2 nebo 4 (sudý bajt INS) bez šifrování:	DO '87' || DO '99' || DO '8E' || SW1SW2
Případ 2 nebo 4 (lichý bajt INS) bez šifrování:	DO 'B3' || DO '99' || DO '8E' || 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 příkaz APDU případu 4 s ověřenou pravostí, Obrázek 9 znázorňuje odpověď APDU případu 2/případu 4 s prokázanou pravostí a Obrázek 10 znázorňuje odpověď APDU případu 2/případu 4 se šifrováním a ověřenou pravostí.

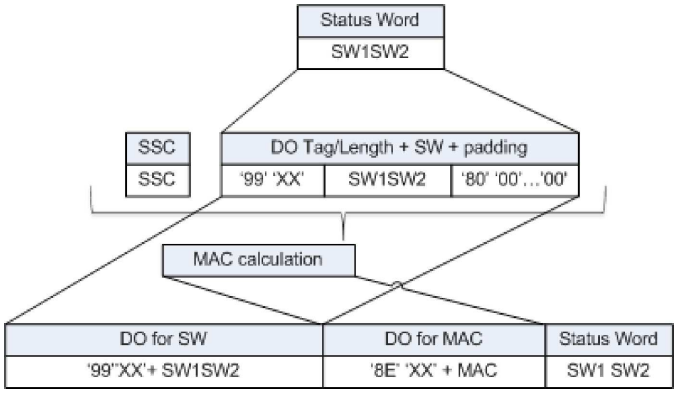
Obrázek 8

Transformace příkazu APDU případu 4 s ověřenou pravostí



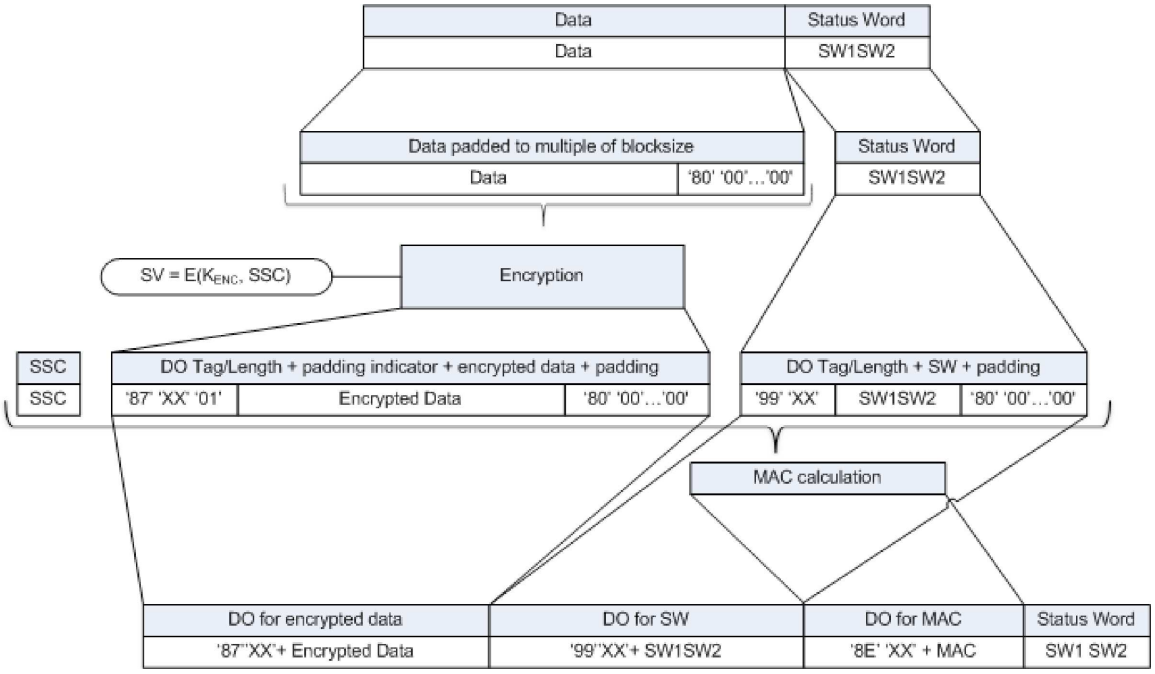
Obrázek 9

Transformace odpovědi APDU případu 1 / případu 3 s ověřenou pravostí



Obrázek 10

Transformace odpovědi APDU případu 2 / případu 4 se šifrování a prokázanou pravostí



10.5.3 *Přerušení relace bezpečného předávání zpráv*

CSM_192 Celek ve vozidle přeruší aktuální relaci bezpečného předávání zpráv pouze v případě, že je splněna některá z těchto podmínek:

— přijme otevřenou odpověď APDU,

— detekuje chybu bezpečného předávání zpráv v odpovědi 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 je nesprávná, struktura TLV je nesprávná nebo indikátor doplnění v tagu '87' se nerovná '01'.

— karta odešle bajt statusu, který označuje detekování chyby SM (viz CSM_194),

— je dosaženo mezního počtu příkazů a příslušných odpovědí v rámci aktuální relace. Pro příslušný VU tuto mezní hodnotu stanoví jeho výrobce s ohledem na bezpečnostní požadavky použitého hardwaru s maximální hodnotou 240 příkazů a příslušných odpovědí SM na relaci.

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 zvolí aplikaci na kartě,

— 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.

CSM_194 Na chybu SM reaguje karta tachografu takto:

— Pokud v příkazu APDU chybí některé očekávané datové objekty bezpečného předávání zpráv, pořadí datových objektů je nesprávné nebo jsou zařazeny neznámé datové objekty, odpoví karta tachografu stavovými bajty '69 87'.

— Pokud je některý datový objekt bezpečného předávání zpráv v příkazu APDU nesprávný, odpoví karta tachografu bajty statusu '69 88'.

V takovém případě musí být bajty statusu znovu odeslány bez použití bezpečného předávání zpráv.

CSM_195 Pokud je relace bezpečného předávání zpráv mezi VU a kartou tachografu přerušena, VU a karta tachografu musí

— bezpečně zlikvidovat uložené klíče relace,

— okamžitě navázat novou relaci bezpečného předávání zpráv podle částí 10.2 – 10.5.

CSM_196 Pokud se z jakéhokoli důvodu VU rozhodne znovu zahájit vzájemné ověřování pravosti vůči vložené kartě, musí být tento proces zahájen ověřením řetězce certifikátů karty podle části 10.2 a pokračovat v souladu s částmi 10.2 – 10.5.

11. PÁROVÁNÍ VU – VNĚJŠÍ ZAŘÍZENÍ GNSS, VZÁJEMNÉ OVĚŘOVÁNÍ PRAVOSTI A BEZPEČNÉ PŘEDÁVÁNÍ ZPRÁV

11.1. **Obecné informace**

CSM_197 Zařízení GNSS používané VU pro určování jeho polohy může být interní (tj. vestavěné do krytu VU a neoddělitelné), nebo se může jednat o externí modul. V prvním případě není třeba standardizovat vnitřní komunikaci mezi zařízením GNSS a VU a požadavky podle této kapitoly se nepoužijí. Ve druhém případě musí být komunikace mezi VU a vnějším zařízením GNSS standardizována a chráněna podle ustanovení této kapitoly.

CSM_198 Bezpečná komunikace mezi celkem ve vozidle a vnějším zařízením GNSS probíhá stejně jako bezpečná komunikace mezi celkem ve vozidle a kartou tachografu, přičemž úlohu karty přebírá vnější zařízení GNSS (EGF). EGF musí splňovat všechny požadavky uvedené v kapitole 10 pro karty tachografu při zohlednění odchylek, vysvětlení a doplňků uvedených v této kapitole. Zejména vzájemné ověření řetězců certifikátů, ověření pravosti VU a ověření pravosti čipu se musí provádět podle pokynů v částech 11.3 and 11.4.

CSM_199 Komunikace mezi celkem ve vozidle a EGF se liší od komunikace mezi celkem ve vozidle a kartou v tom, že celek ve vozidle a EGF se musí před tím, než si budou moci během normálního provozu vyměňovat data na bázi GNSS, spárovat v dílně. Proces párování je popsán v části 11.2.

CSM_200 Pro komunikaci mezi celkem ve vozidle a EGF musí být užívány příkazy a odezvy APDU podle [ISO 7816-4] a [ISO 7816-8]. Přesná struktura těchto APDU je stanovena v dodatku 2 této přílohy.

11.2. **Párování VU a externího zařízení GNSS**

CSM_201 Celek ve vozidle a EGF ve vozidle musí být spárovány v dílně. Během normálního provozu mohou komunikovat pouze celek ve vozidle a EGF, které byly spárovány.

CSM_202 Párování celku ve vozidle a EGF je možné pouze v případě, že celek ve vozidle je v kalibračním módu. Párování musí být zahájeno celkem ve vozidle.

CSM_203 Dílna může kdykoli znovu spárovat celek ve vozidle s jiným EGF nebo stejným EGF. Během nového párování musí VU ve své paměti bezpečně zlikvidovat stávající certifikát EGF_MA a uložit certifikát EGF_MA vnějšího zařízení GNSS, s nímž má být párováno.

CSM_204 Dílna může kdykoli znovu spojit vnější zařízení GNSS s jiným VU nebo stejným VU. Během nového párování musí EGF ve své paměti bezpečně zlikvidovat stávající certifikát VU_MA a uložit certifikát VU_MA celku ve vozidle, s nímž má být párováno.

11.3. **Vzájemné ověření řetězce certifikátů**

11.3.1 *Obecné informace*

CSM_205 Vzájemné ověření řetězce certifikátů mezi VU a EGF se provede pouze během párování VU a EGF v dílně. Během normálního provozu spárovaného VU a EGF nejsou ověřovány žádné certifikáty. VU a EGF musí naopak důvěřovat certifikátům, které uložily během párování a po ověření dočasné platnosti těchto certifikátů. VU a EGF nesmí důvěřovat žádným jiným certifikátům z důvodu ochrany komunikace VU – EGF během normálního provozu.

11.3.2 *Během párování VU – EGF*

CSM_206 Během párování s EGF musí celek ve vozidle užívat protokol popsaný na Obrázek 4 (části 10.2.1) pro ověření řetězce certifikátů vnějšího zařízení GNSS.

Poznámky k Obrázek 4 v této souvislosti:

— Řízení komunikace je mimo rozsah tohoto dodatku. EGF však není inteligentní karta, a proto VU pravděpodobně nebude odesílat příkaz resetu pro obnovení komunikace a nebude přijímat ATR.

— Certifikáty a veřejné klíče karet uvedené na obrázku lze považovat za certifikáty a veřejné klíče EGF pro vzájemné ověřování pravosti. V části 9.1.6 jsou označeny jako EGF_MA.

— Certifikáty a veřejné klíče Card.CA uvedené na obrázku lze považovat za certifikáty a veřejné klíče MSCA pro podpis certifikátů EGF. V části 9.1.3 jsou označeny jako MSCA_VU-EGF.

— Certifikát Card.CA.EUR uvedený na obrázku lze považovat za evropský kořenový certifikát, který je uveden v CAR certifikátu MSCA_VU-EGF.

— Certifikát Card.Link uvedený na obrázku lze považovat za spojovací certifikát EGF, je-li přítomen. Jak je uvedeno v části 9.1.2, jedná se o spojovací certifikát pro nový evropský kořenový pár klíčů vytvořený ERCA a podepsaný předchozím evropským soukromým klíčem.

— Certifikát Card.Link.EUR je evropský kořenový certifikát, který je uveden v CAR certifikátu Card.Link.

— Místo `cardExtendedSerialNumber` musí VU z EF ICC načíst `sensorGNSSserialNumber`.

— Místo výběru AID tachografu musí VU zvolit AID EGF.

— Příkaz „Ignore Card“ se považuje za příkaz „Ignore EGF“.

CSM_207 Jakmile celek ve vozidle ověří certifikát EGF_MA, uloží jej pro užití během normálního provozu; viz bod 11.3.3.

CSM_208 Během párování s VU musí vnější jednotka GNSS používat protokol uvedený na Obrázek 5 (části 10.2.2) pro ověření řetězců certifikátů VU.

Poznámky k Obrázek 5 v této souvislosti:

— VU musí vygenerovat nový přechodný pár klíčů pomocí parametrů domény v certifikátu EGF.

— Certifikáty a veřejné klíče VU uvedené na obrázku se používají pro vzájemné ověřování pravosti. V části 9.1.4 jsou označeny jako VU_MA.

— Certifikáty a veřejné klíče VU.CA uvedené na obrázku se používají pro podpis certifikátů VU a vnějších zařízení GNSS. V části 9.1.3 jsou označeny jako MSCA_VU-EGF.

— Certifikát VU.CA.EUR uvedený na obrázku je evropský kořenový certifikát, který je uveden v CAR certifikátu VU.CA.

— Certifikát VU.Link uvedený na obrázku je spojovací certifikát VU, je-li přítomen. Jak je uvedeno v části 9.1.2, jedná se o spojovací certifikát pro nový evropský kořenový pár klíčů vytvořený ERCA a podepsaný předchozím evropským soukromým klíčem.

— Certifikát VU.Link.EUR je evropský kořenový certifikát, který je uveden v CAR certifikátu VU. Link.

CSM_209 Odchylně od požadavku CSM_167 musí EGF užívat pro ověření dočasné platnosti všech předložených certifikátů čas GNSS.

CSM_210 Jakmile vnější jednotka GNSS ověří certifikát VU_MA, musí jej uložit pro užití během normálního provozu; viz bod 11.3.3.

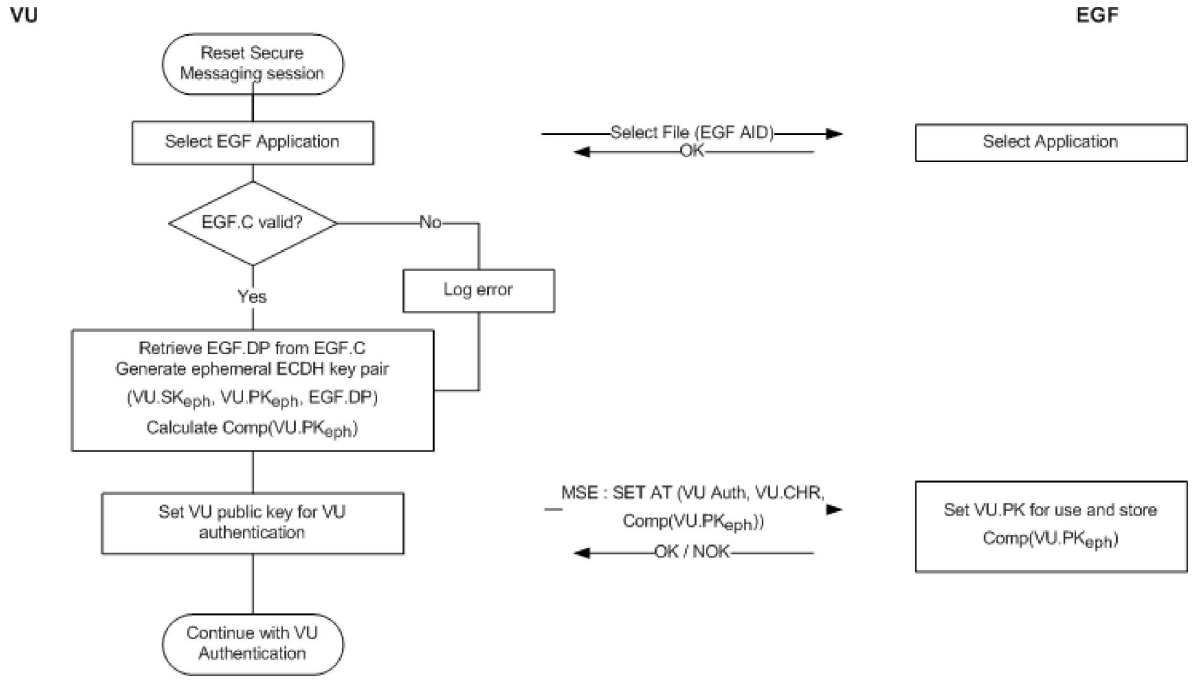
11.3.3 *Během normálního provozu*

CSM_211 Během normálního provozu musí celek ve vozidle a EGF užívat protokol uvedený na Obrázek 11 pro ověření dočasné platnosti uložených certifikátů EGF_MA a VU_MA a pro nastavení veřejného klíče VU_MA pro následné ověření pravosti VU. Během normálního provozu se žádné další vzájemné ověření řetězců certifikátů neprovádí.

Všimněte si, že Obrázek 11 v zásadě obsahuje první kroky uvedené na Obrázek 4 a Obrázek 5. Protože EGF není inteligentní karta, opět platí, že VU pravděpodobně nebude odesílat příkaz resetu pro zahájení komunikace a nebude přijímat ATR. Tento postup je v každém případě mimo rozsah tohoto dodatku.

Obrázek 11

Vzájemné ověření dočasné platnosti certifikátu během normálního provozu VU – EGF



CSM_212 Jak je uvedeno na Obrázek 11, celek ve vozidle zaznamená chybu, pokud certifikát EGF_MA již není platný. Vzájemné ověřování pravosti, odsouhlasení klíče a následná komunikace prostřednictvím bezpečného předávání zpráv však pokračuje normálně.

11.4. Ověřování pravosti VU„ ověřování pravosti čipu a odsouhlasení klíče relace

CSM_213 Ověřování pravosti VU, ověřování pravosti čipu a odsouhlasení klíče relace mezi VU a EGF se provádí během párování a při každém obnovení relace bezpečného předávání zpráv během normálního provozu. VU a EGF musí provádět postupy popsané v částech 10.3 a 10.4. Platí všechny požadavky uvedené v těchto částech.

11.5. Bezpečné předávání zpráv

CSM_214 Všechny příkazy a odezvy vyměňované mezi celkem ve vozidle a vnějším zařízením GNSS po úspěšném ověření pravosti čipu a do skončení relace musí být chráněny bezpečným předáváním zpráv pouze v módu ověřování pravosti. Platí všechny požadavky v bodě 10.5.

CSM_215 Při přerušení relace bezpečného předávání zpráv mezi VU a EGF musí VU okamžitě vytvořit novou relaci bezpečného předávání zpráv, jak je uvedeno v části 11.3.3 a 11.4.

12. PÁROVÁNÍ A KOMUNIKACE VU – SNÍMAČ POHYBU

12.1. **Obecné informace**

CSM_216 Celek ve vozidle a snímač pohybu musí během párování a za normálního provozu komunikovat pomocí protokolu rozhraní uvedeného v [ISO 16844-3] se změnami uvedenými v této kapitole a v části 9.2.1.

Poznámka: Čtenáři této kapitoly by měli být seznámeni s obsahem [ISO 16844-3].

12.2. **Párování VU – snímač pohybu pomocí různých generací klíčů**

Jak je uvedeno v části 9.2.1, hlavní klíč snímače pohybu a všechny související klíče jsou pravidelně vyměňovány. To znamená, že v kartách dílny jsou současně až tři klíče AEC K_{M-WC} pro snímač pohybu (následných generací klíče). Podobně mohou být ve snímačích pohybu až tři různé druhy šifrování dat na bázi AES (podle následných generací hlavního klíče snímače pohybu K_M). Celek ve vozidle obsahuje pouze jeden klíč K_{M-VU} pro snímač pohybu.

CSM_217 VU druhé generace a snímač pohybu druhé generace musí být párovány takto (viz tabulka 6 v [ISO 16844-3]):

1. Karta dílny druhé generace je vložena do VU a VU je spojen se snímačem pohybu.

2. VU čte všechny dostupné klíče K_{M-WC} z karty dílny, kontroluje jejich čísla verze klíče a zvolí to, které odpovídá číslu verze klíče VU K_{M-VU}. Není-li odpovídající klíč K_{M-WC} na kartě dílny, VU přeruší párovací proces a držiteli karty dílny zobrazí příslušné chybové hlášení.

3. VU vypočítá hlavní klíč snímače pohybu K_M z K_{M-VU} a K_{M-WC} a identifikační klíč K_{ID} zK_M, jak je uvedeno v části 9.2.1.

4. VU odešle snímači pohybu pokyn pro zahájení párovacího procesu, jak je uvedeno v [ISO 16844-3], a zašifruje sériové číslo, které získá ze snímače pohybu s identifikačním klíčem K_{ID}. VU vrátí snímači pohybu zašifrované sériové číslo.

5. Snímač pohybu porovná zašifrované sériové číslo postupně se všemi zašifrovanými sériovými čísly, která jsou v něm uložena. Nalezne-li shodu, je pravost VU ověřena. Snímač pohybu zaznamená generaci K_{ID} používaného VU a vrátí vyhovující zašifrovanou verzi svého párovacího klíče; tj. šifrování, které bylo vytvořeno pomocí stejné generace KM.

6. VU dešifruje párovací klíč pomocí K_M, generuje klíč relace K_S, zašifruje jej s párovacím klíčem a výsledek odešle do snímače pohybu. Snímač pohybu K_S dekóduje.

7. VU sestaví párovací informaci podle [ISO 16844-3], zašifruje informaci s párovacím klíčem a výsledek odešle do snímače pohybu. Snímač pohybu párovací informaci dekóduje.

8. Snímač pohybu zašifruje přijatou párovací informaci s přijatým K_S a vrátí ji VU. Ten ověří, zda je tato párovací informace stejná informace, jakou snímači pohybu odeslal v předchozím kroku. Pokud ano, znamená to, že snímač pohybu použil stejný K_S jako VU, a proto v kroku 5 odeslal svůj párovací klíč zašifrovaný se správnou generací K_M. Tím je pravost snímače pohybu ověřena.

Kroky 2 a 5 se liší od standardního procesu v [ISO 16844-3]; ostatní kroky jsou standardní.

Příklad: Předpokládejme, že k párování dojde v prvním roce platnosti certifikátu ERCA (3); viz Obrázek 2 v bodě 9.2.1.2. Kromě toho:

— předpokládejme, že snímač pohybu byl vydán v posledním roce platnosti certifikátu ERCA (1). Bude proto obsahovat tyto klíče a data:

  — $N_s[1]$: své sériové číslo šifrované s generací 1 K_{ID},

  — $N_s[2]$: své sériové číslo šifrované s generací 2 K_{ID},

  — $N_s[3]$: své sériové číslo šifrované s generací 3 K_{ID},

  — $K_P[1]$: svůj párovací klíč generace 1 ([1]), šifrovaný s generací 1 K_M,

  — $K_P[2]$: svůj párovací klíč generace 2, šifrovaný s generací 2 K_M,

  — $K_P[3]$: svůj párovací klíč generace 3, šifrovaný s generací 3 K_M,

— předpokládejme, že karta dílny byla vydána v prvním roce platnosti certifikátu ERCA (3). Bude proto obsahovat generaci 2 a generaci 3 klíče $K_{M\text{-}WC}$.

— předpokládejme, že VU je generace 2, obsahující generaci 2 klíče $K_{M\text{-}VU}$.

V tomto případě proběhnou v krocích 2 – 5 tyto operace:

— Krok 2: VU přečte klíče $K_{M\text{-}WC}$ generace 2 a generace 3 z karty dílny a zkontroluje jejich čísla verze.

— Krok 3: VU spojí klíč $K_{M\text{-}WC}$ generace 2 se svým $K_{M\text{-}VU}$ a vypočítá K_M a K_{ID}.

— Krok 4: VU zašifruje sériové číslo, které přijme ze snímače pohybu, s klíčem K_{ID}.

— Krok 5: Snímač pohybu porovná přijatá data s $N_s[1]$ a nezjistí shodu. Potom porovná data s $N_s[2]$ a zjistí shodu. Dojde k závěru, že VU je generace 2, a proto odešle zpět $K_P[2]$.

12.3. **Párování a komunikace VU – snímač pohybu pomocí AES**

CSM_218 Jak je uvedeno v Tabulka 3 v části 9.2.1, všechny klíče použité v párování celku ve vozidle (druhé generace) a snímače pohybu a v následné komunikaci jsou klíče AES, a nikoli klíče TDES dvojité délky podle [ISO 16844-3]. Tyto klíče AES mohou mít délku 128, 192 nebo 256 bitů. Protože velikost bloku AES je 16 bajtů, musí být délka šifrované zprávy násobkem 16 bajtů na rozdíl od 8 bajtů pro TDES. Některé z těchto zpráv budou navíc použity pro přenos klíčů AES, jejichž délka může být 128, 192 nebo 256 bitů. Proto se počet datových bajtů na instrukci v tabulce 5 [ISO 16844-3] změní, jak je uvedeno v Tabulka 6:

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

([1]) Párovací klíče generace 1, generace 2 a generace 3 mohou být ve skutečnosti stejný klíč nebo mohou být třemi různými klíči s různými délkami, jak je uvedeno v CSM_117.

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
11	odpověď	Data ověření pravosti + obsah souboru	16 nebo 32, podle souboru	16 nebo 32, podle souboru	16 / 32	16 / 32	16 / 32
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

CSM_219 Párovací informace, které jsou zaslány v instrukcích 43 (žádost VU) a 50 (odpověď MoS), musí být sestaveny, jak je uvedeno v části 7.6.10 [ISO 16844-3], s tou výjimkou, že ve schématu šifrování pro párování se místo algoritmu TDES použije algoritmus AES, což vede ke dvěma šifrováním AES a doplňování podle CSM_220 se upraví tak, aby byla dodržena délka bloku AES. Klíč K'_P použitý pro toto šifrování musí být generován takto:

— v případě párovacího klíče K_P s délkou 16 bajtů: $K'_P = K_P \text{ XOR } (N_s||N_s)$

— v případě párovacího klíče K_P s délkou 24 bajtů: $K'_P = K_P \text{ XOR } (N_s||N_s||N_s)$

— v případě párovacího klíče K_P s délkou 32 bajtů: $K'_P = K_P \text{ XOR } (N_s||N_s||N_s||N_s)$

kde N_s je 8-bajtové sériové číslo snímače pohybu.

CSM_220 V případě, že délka otevřeného textu (s použitím klíče AES) není násobkem 16 bajtů, použije se metoda doplňování 2 stanovená v [ISO 9797-1].

Poznámka: V [ISO 16844-3] je počet bajtů otevřeného textu vždy násobkem 8, proto při použití TDES není doplňování nutné. Tato část tohoto dodatku nemění definici dat a zpráv v [ISO 16844-3], proto je třeba použít metodu doplňování.

CSM_221 Pro instrukci 11 a v případě, že musí být šifrován více než jeden blok, se použije mód řetězení šifrového textu podle [ISO 10116] s vloženým parametrem *m* = 1. Použitý IV je:

— pro instrukci 11: 8-bajtový blok ověření pravosti uvedený v části 7.6.3.3 [ISO 16844-3], doplněný pomocí metody doplňování 2 podle [ISO 9797-1]; viz rovněž část 7.6.5 a 7.6.6 [ISO 16844-3],

— pro všechny ostatní instrukce, v nichž je přesunuto více než 16 bajtů, jak je uvedeno v Tabulka 6: '00' {16}, tj. šestnáct bajtů s binární hodnotou 0.

Poznámka: Jak je uvedeno v části 7.6.5 a 7.6.6 [ISO 16844-3], když MoS šifruje datové soubory pro zařazení do instrukce 11, je blok prokázání pravosti:

— použit jako inicializační vektor pro šifrování datových souborů v módu CBC,

— zašifrován a zařazen jako první blok do dat, která jsou odeslána do VU.

12.4. **Párování VU – snímač pohybu pro různé generace zařízení**

CSM_222 Jak je uvedeno v části 9.2.1, snímač pohybu druhé generace může obsahovat šifrování párovacích dat na bázi TDES (podle části A tohoto dodatku), které umožňuje párování snímače pohybu s VU první generace. V tomto případě musí být VU první generace a snímač pohybu druhé generace párovány podle části A tohoto dodatku a podle [ISO 16844-3]. Pro párovací proces lze použít kartu dílny první nebo druhé generace.

Poznámky:

— Nelze párovat VU druhé generace a snímač pohybu první generace.

— Pro párování VU druhé generace a snímače pohybu nelze použít kartu dílny první generace.

13. BEZPEČNOST VZDÁLENÉ KOMUNIKACE PROSTŘEDNICTVÍM DSRC

13.1. **Obecné informace**

Jak je uvedeno v dodatku 14, VU pravidelně generuje data vzdáleného sledování tachografu (RTM) a odesílá tato data (internímu nebo externímu) zařízení vzdálené komunikace (RCF). Zařízení vzdálené komunikace je odpovědné za odesílání těchto dat přes rozhraní DSRC podle dodatku 14 do vzdáleného dotazovacího zařízení. Dodatek 1 stanoví, že data RTM jsou kaskádovým spojením:

šifrovaného vytížení tachografu šifrování otevřeného přenosu dat tachografu,

bezpečnostních dat DSRC uvedených níže.

Datový formát otevřeného přenosu dat tachografu je uveden v dodatku 1 a dále popsán v dodatku 14. Tato část popisuje strukturu bezpečnostních dat DSRC; formální specifikace jsou uvedeny v dodatku 1.

CSM_223 Otevřený text `tachographPayload` předávaný z VU do zařízení vzdálené komunikace (je-li RCF vůči VU externí jednotkou) nebo z VU do vzdáleného dotazovacího zařízení přes rozhraní DSRC (je-li RCF vůči VU interní jednotkou) musí být chráněna v módu šifrování a následného ověření pravosti, tj. přenášená data tachografu jsou nejprve šifrována pro zajištění důvěrnosti zprávy a následně je vypočítán MAC pro zajištění pravosti a integrity.

CSM_224 Bezpečnostní data DSRC musí obsahovat kaskádové spojení následujících datových prvků v níže uvedeném pořadí; viz také Obr. 12:

Aktuální datum čas	aktuální datum a čas VU (datový typ `TimeReal`),
Čítač	3-bajtový čítač, viz CSM_225

Sériové číslo VU	sériové číslo VU (datový typ `VuSerialNumber`),
Číslo verze hlavního klíče DSRC	1-bajtové číslo verze hlavního klíče DSRC, z něhož se odvozují klíče DSRC pro příslušné VU, viz část 9.2.2.
MAC	MAC vypočítaný ze všech předchozích bajtů v datech RTM.

CSM_225 3-bajtový čítač v bezpečnostních datech DSRC musí být ve formátu MSB-first. Když VU po uvedení do provozu poprvé vypočítá sadu dat RTM, nastaví hodnotu čítače na 0. Před každým výpočtem nové sady dat RTM zvýší VU hodnotu dat čítače o 1.

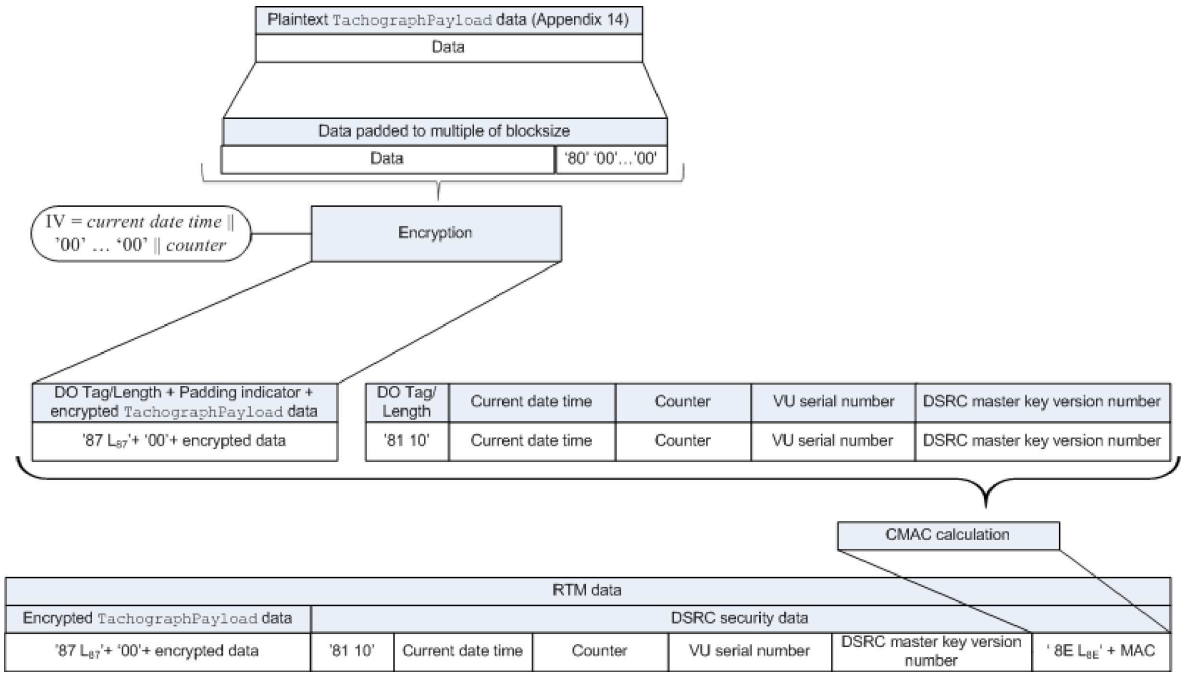
13.2. Šifrování přenosu dat tachografu a generování MAC

CSM_226 V případě otevřeného datového prvku s datovým typem `TachographPayload` podle dodatku 14 musí VU tato data šifrovat, jak je uvedeno v Obr. 12: Klíč DSRC celku ve vozidle pro šifrování K_VU_{DSRC}_ENC (viz bod 9.2.2) musí být použit s AES v operačním módu řetězení šifrového textu (CBC) podle [ISO 10116] s vloženým parametrem *m* = 1. Inicializační vektor musí odpovídat hodnotě *IV = aktuální datum čas || '00 00 00 00 00 00 00 00' || čítač, kde aktuální datum čas* a *čítač* jsou uvedeny v CSM_224. Šifrovaná data musí být doplněna pomocí metody 2 podle [ISO 9797-1].

CSM_227 VU musí vypočítat MAC v bezpečnostních datech DSRC, jak je uvedeno v Obr. 12: MAC se vypočte pro všechny předchozí bajty v datech RTM až do čísla verze hlavního klíče DSRC včetně i včetně tagů a délek datových objektů. VU použije svůj klíč DSRC pro ověření pravosti K_VU_{DSRC}_MAC (viz část 9.2.2) s algoritmem AES v módu CMAC podle [SP 800-38B]. Délka MAC musí být spojena s délkou klíčů DSRC příslušných VU, jak je uvedeno v CSM_50.

Obr. 12

Šifrování přenosu dat tachografu a generování MAC



13.3. **Ověření a dešifrování přenosu dat tachografu**

CSM_228 Když vzdálené dotazovací zařízení přijme data RTM z VU, musí veškerá data RTM odeslat do kontrolní karty v datovém poli příkazu PROCESS DSRC MESSAGE, jak je uvedeno v dodatku 2. Pak:

1. Kontrolní karta zkontroluje číslo verze hlavního klíče DSRC v bezpečnostních datech DSRC. Pokud kontrolní karta nezná uvedený hlavní klíč DSRC, oznámí chybu uvedenou v dodatku 2 a přeruší proces.

2. Kontrolní karta použije uvedený hlavní klíč DSRC ve spojení se sériovým číslem VU 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.

3. Kontrolní karta použije K_VU_{DSRC}_MAC pro ověření MAC v bezpečnostních datech DSRC, jak je uvedeno v CSM_227. Je-li MAC nesprávný, kontrolní karta oznámí chybu uvedenou v dodatku 2 a přeruší proces.

4. Kontrolní karta použije K_VU_{DSRC}_ENC pro dešifrování šifrovaného přenosu dat tachografu, jak je uvedeno v CSM_226. Kontrolní karta musí odstranit doplnění a vrátit dešifrovaná přenášená data tachografu vzdálenému dotazovacímu zařízení.

CSM_229 Pro zabránění opakovaným útokům musí vzdálené dotazovací zařízení zkontrolovat aktuálnost dat RTM ověřením, zda se *aktuální datum čas* v bezpečnostních datech DSRC příliš neodchyluje od aktuálního času vzdáleného dotazovacího zařízení.

Poznámky:

— To vyžaduje, aby mělo vzdálené dotazovací zařízení přesný a spolehlivý zdroj času.

— Protože dodatek 14 požaduje, aby VU každých 60 sekund vypočítal novou sadu dat RTM a hodiny VU se smějí odlišovat o 1 minutu od skutečného času, je spodní hranice aktuálnosti dat RTM 2 minuty. Požadovaná aktuálnost rovněž závisí na přesnosti hodin vzdáleného dotazovacího zařízení.

CSM_230 Když dílna ověří správnou funkci DSRC celku ve vozidle, musí veškerá přijatá data RTM odeslat z VU do karty dílny v datovém poli příkazu PROCESS DSRC MESSAGE, jak je uvedeno v dodatku 2. Dílna karty musí provést kontroly a postupy uvedené v CSM_228.

14. PODEPISOVÁNÍ STAŽENÝCH DAT A OVĚŘOVÁNÍ PODPISŮ

14.1. **Obecné informace**

CSM_231 Inteligentní vyhrazené zařízení (IDE) musí uložit data přijatá z VU nebo karty během jedné relace stahování v jednom fyzickém datovém souboru. Data mohou být uložena na ESM (externí paměťové médium). Tento soubor obsahuje digitální podpisy bloků dat, jak je uvedeno v dodatku 7. Tento soubor musí rovněž obsahovat tyto certifikáty (viz část 9.1):

— v případě stahování VU:

  — certifikát VU_Sign,

  — certifikát MSCA_VU-EGF obsahující veřejný klíč pro ověření certifikátu VU_Sign,

— v případě stahování karty:

— certifikát Card_Sign,

— certifikát MSCA_Card obsahující veřejný klíč pro ověření certifikátu Card_Sign.

CSM_232 IDE musí rovněž zlikvidovat

— v případě, že používá kontrolní kartu pro ověření podpisu podle Obrázek 13: spojovací certifikát spojující poslední certifikát EUR s certifikátem EUR, jehož doba platnosti jej přímo předchází, pokud existuje,

— v případě, že ověřuje samotný podpis: všechny platné evropské kořenové certifikáty.

Poznámka: Metoda, kterou IDE používá pro získání těchto certifikátů, není v tomto dodatku stanovena.

14.2. **Generování podpisu**

CSM_233 Podpisový algoritmus pro vytváření digitálních podpisů stahovaných dat musí být ECDSA podle [DSS] s použitím hašovacího algoritmu spojeného s velikostí klíče VU nebo karty, jak je uvedeno v CSM_50. Formát podpisu musí být otevřený podle [TR-03111].

14.3. **Ověření podpisu**

CSM_234 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 Obrázek 13. 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].

Poznámky k Obrázek 13:

— zařízení, které podepisovalo analyzovaná data, je označeno EQT,

— certifikáty a veřejné klíče EQT uvedené na obrázku se používají pro podpis, tj. VU_Sign nebo Card_Sign,

— certifikáty a veřejné klíče EQT.CA uvedené na obrázku se používají pro podpis certifikátů VU nebo karty,

— certifikát EQT.CA.EUR uvedený na obrázku je evropský kořenový certifikát, který je uveden v CAR certifikátu EQT.CA,

— certifikát EQT.Link uvedený na obrázku je případný spojovací certifikát EQT. Jak je uvedeno v části 9.1.2, jedná se o spojovací certifikát pro nový evropský kořenový pár klíčů vytvořený ERCA a podepsaný předchozím evropským soukromým klíčem,

— certifikát EQT.Link.EUR je evropský kořenový certifikát, který je uveden v CAR certifikátu EQT. Link.

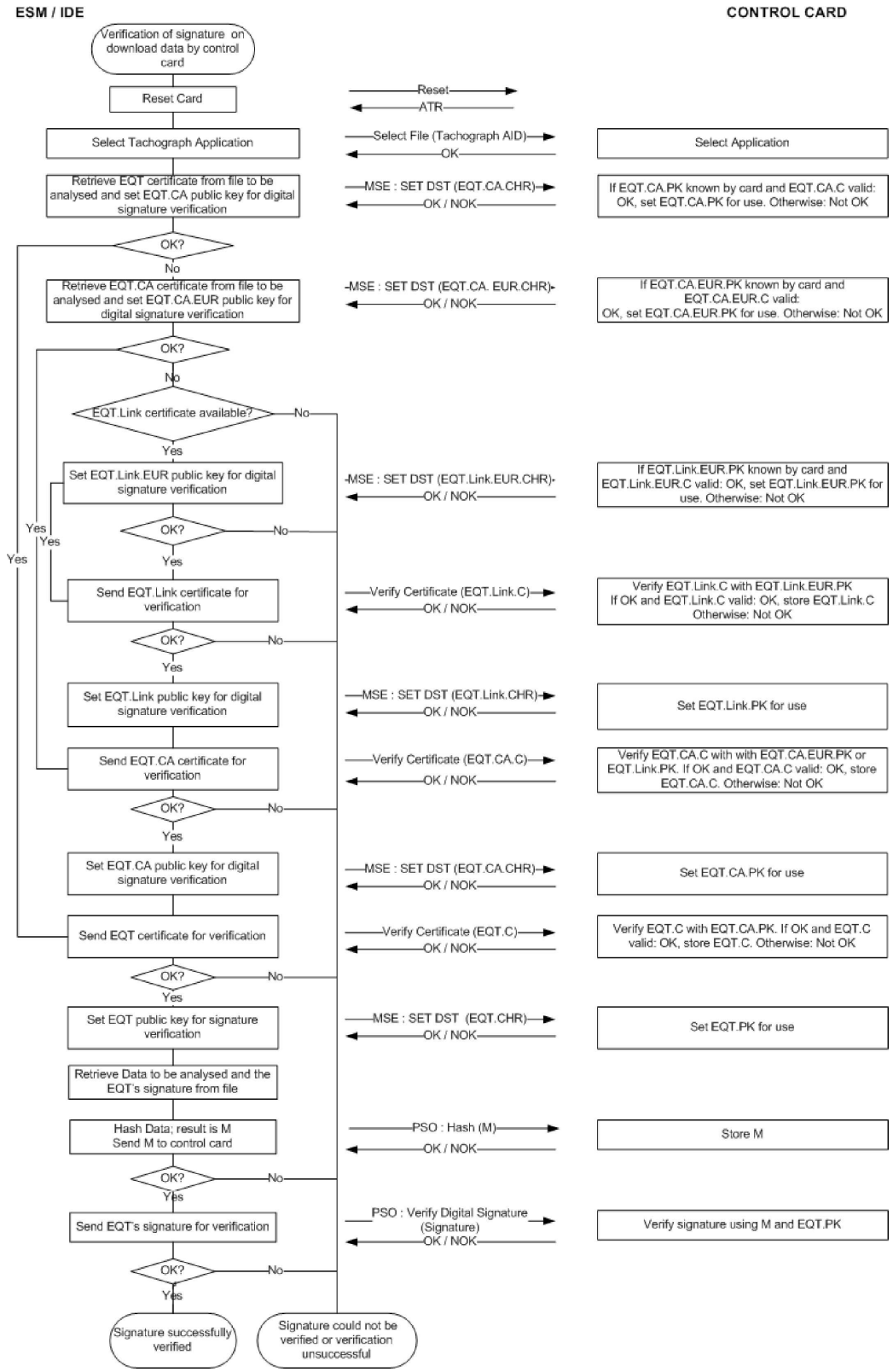
CSM_235 Pro výpočet hash M odeslané do kontrolní karty v PSO: příkaz hash, IDE musí používat hašovací algoritmus spojený s velikostí klíče VU nebo karty, ze kterých jsou stahována data, jak je uvedeno v CSM_50.

CSM_236 Pro ověření podpisu EQT musí kontrolní karta postupovat podle podpisového schématu uvedeného v [DSS].

Poznámka: Tento dokument nestanoví žádné opatření pro případ, kdy nelze ověřit podpis staženého datového souboru nebo je ověření neúspěšné.

Obrázek 13

Protokol pro ověření podpisu staženého datového souboru



Dodatek 12

URČOVÁNÍ POLOHY NA ZÁKLADĚ GLOBÁLNÍHO DRUŽICOVÉHO NAVIGAČNÍHO SYSTÉMU (GNSS)

OBSAH

1. ÚVOD

Tento dodatek stanoví technické požadavky na údaje GNSS používané celkem ve vozidle, včetně protokolů, které je třeba implementovat k zajištění zabezpečeného a správného přenosu dat s informacemi o poloze.

Hlavními články nařízení (EU) č. 165/2014 určujícími tyto požadavky jsou: článek 8 „Zaznamenávání polohy vozidla v určitých místech během denní pracovní doby“, článek 10 „Rozhraní s inteligentními dopravními systémy“ a článek 11 „Podrobná ustanovení pro inteligentní tachografy“.

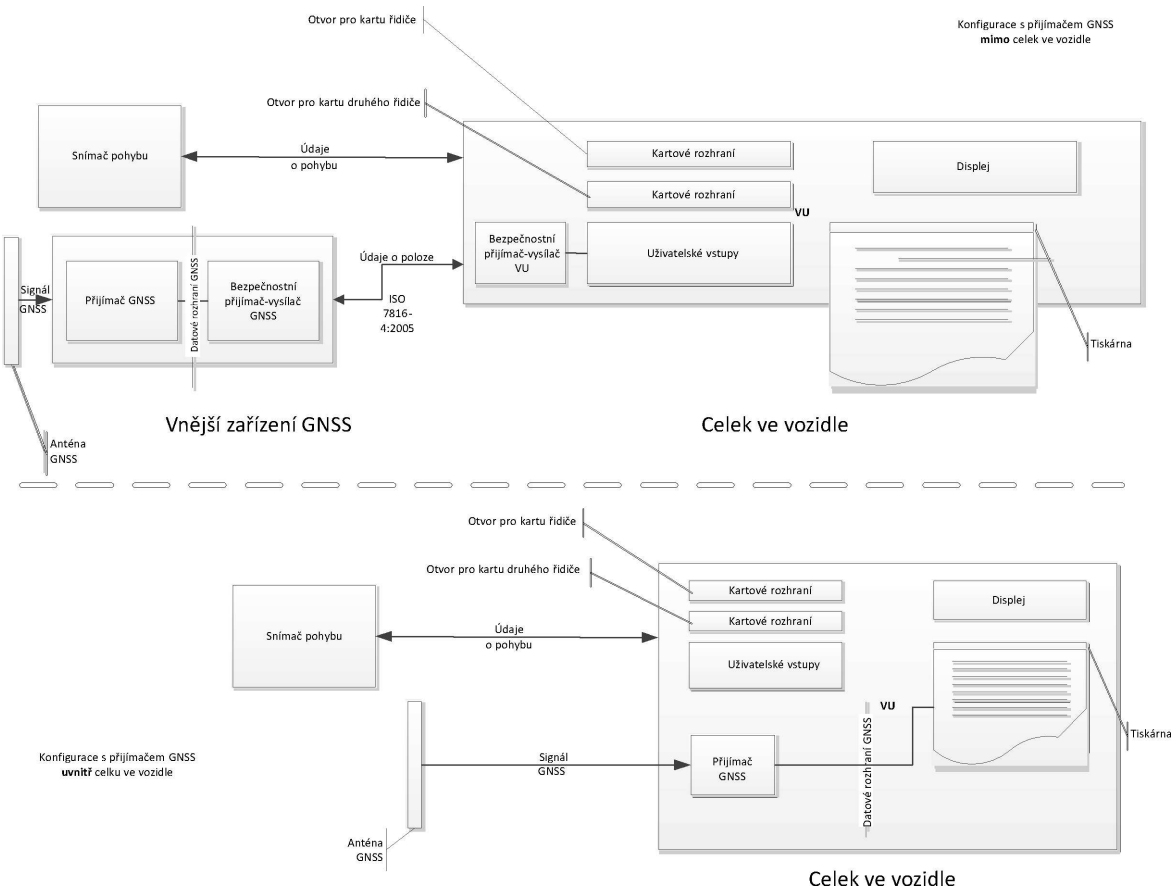
1.1 **Oblast působnosti**

GNS_1 Za účelem provádění článku 8 shromažďuje celek ve vozidle údaje o poloze nejméně z jednoho globálního družicového navigačního systému.

Celek ve vozidle může, ale nemusí být vybaven vnějším zařízením GNSS, jak popisuje obrázek 1:

Obrázek 1

Různé konfigurace přijímače GNSS



1.2 **Zkratky a notace**

V tomto dodatku jsou použity tyto zkratky:

DOP parametr přesnosti (*Dilution of Precision*)

EGF elementární soubor zařízení GNSS (*Elementary file GNSS Facility*)

EGNOS Evropská služba pro pokrytí geostacionární navigací (*European Geostationary Navigation Overlay Service*)

GNSS globální družicový navigační systém (*Global Navigation Satellite System*)

GSA GPS DOP a aktivní družice (*GPS DOP and active satellites*)

HDOP parametr horizontální přesnosti (*Horizontal Dilution of Precision*)

ICD kontrolní dokument rozhraní (*Interface Control Document*)

NMEA Národní asociace pro námořní elektroniku (*National Marine Electronics Association*)

PDOP parametr přesnosti polohy (*Position Dilution of Precision*)

RMC doporučená minimální specifická data (*Recommended Minimum Specific*)

SIS signál v kosmu (*Signal in Space*)

VDOP parametr vertikální přesnosti (*Vertical Dilution of Precision*)

VU celek ve vozidle (*Vehicle Unit*)

2. SPECIFIKACE PŘIJÍMAČE GNSS

Bez ohledu na konfiguraci inteligentního tachografu s vnějším zařízením GNSS nebo bez něj je poskytování přesných a spolehlivých informací o poloze základním prvkem účinného fungování inteligentního tachografu. Proto je přiměřené požadovat jeho slučitelnost se službami poskytovanými v rámci programů Galileo a EGNOS podle nařízení Evropského parlamentu a Rady (EU) č. 1285/2013 ([1]). Systém zavedený v rámci programu Galileo je nezávislým globálním družicovým navigačním systémem a systém zavedený v rámci programu EGNOS je regionálním družicovým navigačním systémem zvyšujícím kvalitu signálu systému GPS (*Global Positioning System*).

GNS_2 Výrobci zajistí, aby přijímače GNSS v inteligentních tachografech byly slučitelné se službami určování polohy poskytovanými systémy Galileo a EGNOS. Výrobci mohou rovněž navíc zvolit kompatibilitu s dalšími družicovými navigačními systémy.

GNS_3 Přijímač GNSS musí být schopen podporovat ověření pravosti v rámci otevřené služby systému Galileo, až bude systém Galileo takovou službu poskytovat a výrobci přijímačů GNSS ji budou podporovat. Nicméně u inteligentních tachografů uvedených na trh dříve, než budou uvedené podmínky splněny, a nepodporujících ověření pravosti v rámci otevřené služby systému Galileo nebude vyžadována modernizace.

3. VĚTY NMEA

Tato část popisuje věty NMEA používané při provozu inteligentního tachografu. Tato část platí pro konfiguraci inteligentního tachografu s vnějším zařízením GNSS i bez něj.

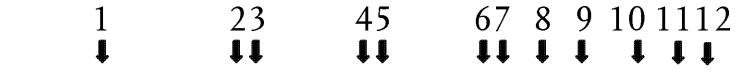
GNS_4 Údaje o poloze jsou založeny na větě NMEA s doporučenými minimálními specifickými daty GNSS (RMC), která obsahuje údaje o poloze (zeměpisná šířka, délka), čas ve formátu UTC (hhmmss.ss) a rychlost vůči zemskému povrchu v uzlech, jakož i další hodnoty.

Věta RMC má tento formát (podle standardu NMEA V4.1):

([1]) Nařízení Evropského parlamentu a Rady (EU) č. 1285/2013 ze dne 11. prosince 2013 o zřízení evropských systémů družicové navigace a jejich využití a o zrušení nařízení Rady (ES) č. 876/2002 a nařízení Evropského parlamentu a Rady (ES) č. 683/2008 (Úř. věst. L 347, 20.12.2013, s. 1).

Obrázek 2

Struktura věty RMC



1) Čas (UTC)
2) Status, A = platná poloha, V = varování
3) Zeměpisná šířka
4) N nebo S
5) eměpisná délka
6) E nebo W
7) Rychlost vůči zemskému povrchu v uzlech
8) Kurz pohybu ve stupních
9) Datum, ddmmyy
10) Magnetická deklinace ve stupních
11) E nebo W
12) Kontrolní součet

Status udává, zda je signál GNSS dostupný. Dokud nemá status hodnotu A, nelze přijímané údaje (např. čas nebo zeměpisnou šířku a délku) používat v celku ve vozidle pro zaznamenávání polohy vozidla.

Rozlišení polohy je založeno na výše popsaném formátu věty RMC. První část polí č. 3 a 5 (první dvě čísla) 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).

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 GPS, Glonass, Galileo, Beidou nebo rozšiřující družicový systém (SBAS).

Obrázek 3

Struktura věty GSA

1) Režim výběru
2) Režim
3) ID prvního satelitu použitého pro určení polohy
4) D druhého satelitu použitého pro určení polohy
...
14) ID dvanáctého satelitu použitého pro určení polohy
15) PDOP v metrech
16) HDOP v metrech
17) VDOP v metrech
18) ID systému GNSS
19) Kontrolní součet

kde režim (2) uvádí, zda je určení polohy (fix) nedostupné (režim=1), dostupné pro 2D (režim=2), nebo dostupné pro 3D (režim=3).

GNS_6 Věta GSA se ukládá s číslem záznamu '06'.

GNS_7 Maximální velikost vět NMEA (např. RMC, GSA nebo dalších), kterou lze použít pro určení velikosti v příkazu čtení záznamu, je 85 bajtů (viz tabulka 1).

4. CELEK VE VOZIDLE S VNĚJŠÍM ZAŘÍZENÍM GNSS

4.1 **Konfigurace**

4.1.1 *Hlavní součásti a rozhraní*

V této konfiguraci je přijímač GNSS součástí vnějšího zařízení GNSS.

GNS_8 Vnější zařízení GNSS musí být napájeno zvláštním vozidlovým rozhraním.

GNS_9 Vnější zařízení GNSS obsahuje tyto součásti (viz obrázek 4):

a) komerční přijímač GNSS pro poskytování údajů o poloze prostřednictvím datového rozhraní GNSS. Datovým rozhraním GNSS může být například standard NMEA V4.10, kde přijímač GNSS funguje jako vysílač a předává věty NMEA bezpečnostnímu přijímači-vysílači GNSS s frekvencí 1 Hz, pokud jde o předem definovanou sadu vět NMEA, která musí zahrnovat přinejmenším věty RMC a GSA. Implementace datového rozhraní GNSS je volbou výrobce vnějšího zařízení GNSS;

b) jednotku přijímače-vysílače (bezpečnostní přijímač-vysílač GNSS) podporující normu ISO/IEC 7816-4:2013 (viz část 4.2.1) pro komunikaci s celkem ve vozidle a podporu datového rozhraní GNSS s přijímačem GNSS. Jednotka je vybavena pamětí pro ukládání identifikačních údajů přijímače GNSS a vnějšího zařízení GNSS;

c) systém krytí s funkcí detekce nedovolené manipulace, který zapouzdřuje jak přijímač GNSS, tak bezpečnostní přijímač-vysílač GNSS. Funkce detekce nedovolené manipulace implementuje bezpečnostní ochranná opatření požadovaná v profilu ochrany inteligentního tachografu;

d) anténu GNSS instalovanou na vozidle a připojenou k přijímači GNSS skrz systém krytí.

GNS_10 Vnější zařízení GNSS má přinejmenším tato vnější rozhraní:

a) rozhraní pro anténu GNSS instalovanou na nákladním vozidle, je-li použita externí anténa;

b) rozhraní s celkem ve vozidle.

GNS_11 V celku ve vozidle je protistranou zabezpečené komunikace s bezpečnostním přijímačem-vysílačem GNSS bezpečnostní přijímač-vysílač VU, který musí podporovat normu ISO/IEC 7816-4:2013, pokud jde o připojení k vnějšímu zařízení GNSS.

GNS_12 Pokud jde o fyzickou vrstvu komunikace s vnějším zařízením GNSS, musí celek ve vozidle podporovat normu ISO/IEC 7816-12:2005 nebo jiný standard, který podporuje normu ISO/IEC 7816-4:2013 (viz část 4.2.1).

4.1.2 *Stav vnějšího zařízení GNSS po dokončení výroby*

GNS_13 Vnější zařízení GNSS při opuštění továrny uchovává v paměti bezpečnostního přijímače-vysílače GNSS nezávislé na napájení tyto hodnoty:

— pár klíčů EGF_MA a příslušný certifikát,

— certifikát MSCA_VU-EGF obsahující veřejný klíč MSCA_VU-EGF.PK používaný pro ověření certifikátu EGF_MA,

— certifikát EUR obsahující veřejný klíč EUR.PK používaný pro ověření certifikátu MSCA_VU-EGF,

— certifikát EUR, jehož doba platnosti přímo předchází době platnosti certifikátu EUR používaného pro ověření certifikátu MSCA_VU-EGF, pokud existuje,

— spojovací certifikát spojující tyto dva certifikáty EUR, pokud existuje,

— rozšířené sériové číslo vnějšího zařízení GNSS,

— identifikátor operačního systému zařízení GNSS,

— číslo schválení typu vnějšího zařízení GNSS,

— identifikátor bezpečnostní komponenty vnějšího modulu GNSS.

4.2 **Komunikace mezi vnějším zařízením GNSS a celkem ve vozidle**

4.2.1 *Komunikační protokol*

GNS_14 Komunikační protokol mezi vnějším zařízením GNSS a celkem ve vozidle podporuje tři funkce:

1. shromažďování a distribuci údajů GNSS (např. polohy, časování, rychlosti);
2. shromažďování konfiguračních dat vnějšího zařízení GNSS;
3. protokol správy na podporu vazby, vzájemného ověření pravosti a dohody na klíči relace mezi vnějším zařízením GNSS a celkem ve vozidle.

GNS_15 Komunikační protokol je založen na normě ISO/IEC 7816-4:2013, přičemž bezpečnostní přijímač-vysílač VU má nadřazenou roli („master“) a bezpečnostní přijímač-vysílač GNSS má podřízenou roli („slave“). Fyzické spojení mezi vnějším zařízením GNSS a celkem ve vozidle je založeno na normě ISO/IEC 7816-12:2005 nebo na jiném standardu, který podporuje normu ISO/IEC 7816-4:2013.

GNS_16 V komunikačním protokolu nejsou podporována rozšířená pole délky.

GNS_17 Komunikační protokol dle ISO 7816 (jak -4:2013, tak -12:2005) mezi vnějším zařízením GNSS a VU je nastaven na T=1.

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), adresářovým 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.

GNS_19 Bezpečnostní přijímač-vysílač GNSS ukládá údaje přicházející z přijímače GNSS a konfiguraci v souboru EF.EGF. Jde o lineární soubor se záznamy proměnné délky a s identifikátorem rovným ‘2F2F’ v hexadecimálním formátu.

GNS_20 Bezpečnostní přijímač-vysílač GNSS používá pro ukládání dat paměť schopnou 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 uvádí tabulka 1. Je třeba připomenout, že existují čtyři věty GSA pro čtyři družicové systémy a rozšiřující družicový systém (SBAS).

GNS_21 Strukturu souborů uvádí tabulka 1. Podmínky přístupu (ALW, NEV, SM-MAC) viz dodatek 2 kapitolu 3.5.

Tabulka 1

Struktura souborů

		Podmínky přístupu		
Soubor	ID souboru	Čtení	Aktualizace	Šifrování
MF	3F00			
EF.ICC	0002	ALW	NEV (by VU)	Ne
DF GNSS Facility	0501	ALW	NEV	Ne
EF EGF_MACertificate	C100	ALW	NEV	Ne
EF CA_Certificate	C108	ALW	NEV	Ne
EF Link_Certificate	C109	ALW	NEV	Ne
EF.EGF	2F2F	SM-MAC	NEV (by VU)	Ne

Soubor / datový prvek	Č. záznamu	Velikost (bajty)		Výchozí hodnoty
		Min	Max	
MF		552	1 031	
EF.ICC				
sensorGNSSSerialNumber		8	8	
DF GNSS Facility		*612*	*1 023*	
EF EGF_MACertificate		*204*	*341*	
EGFCertificate		204	341	{00..00}
EF CA_Certificate		*204*	*341*	
MemberStateCertificate		204	341	{00..00}
EF Link_Certificate		*204*	*341*	
LinkCertificate		204	341	{00..00}
EF.EGF				
Věta RMC NMEA	‘01’	85	85	
1. věta GSA NMEA	‘02’	85	85	
2. věta GSA NMEA	‘03’	85	85	

Soubor / datový prvek	Č. záznamu	Velikost (bajty)		Výchozí hodnoty
		Min	Max	
3. věta GSA NMEA	'04'	85	85	
4. věta GSA NMEA	'05'	85	85	
5. věta GSA NMEA	'06'	85	85	
Rozšířené sériové číslo vnějšího zařízení GNSS definované v dodatku 1 jako SensorGNSSSerialNumber	'07'	8	8	
Identifikátor operačního systému bezpečnostního přijímače-vysílače GNSS definovaný v dodatku 1 jako SensorOSIdentifier	'08'	2	2	
Číslo schválení typu vnějšího zařízení GNSS definované v dodatku 1 jako SensorExternalGNSSApprovalNumber	'09'	16	16	
Identifikátor bezpečnostní komponenty vnějšího zařízení GNSS definovaný v dodatku 1 jako SensorExternalGNSSSCIdentifier	'10'	8	8	
RFU – rezervováno pro budoucí použití	od '11' do 'FD'			

4.2.2 *Zabezpečený přenos údajů GNSS*

GNS_22 Zabezpečený přenos údajů GNSS o poloze je povolen pouze za těchto podmínek:

1. byl dokončen proces vytvoření vazby popsaný v dodatku 11. Společné bezpečnostní mechanismy;

2. bylo provedeno periodické vzájemné ověření pravosti a dohoda na klíči relace mezi celkem ve vozidlem a vnějším zařízením GNSS, rovněž popsané v dodatku 11. Společné bezpečnostní mechanismy, s uvedenou frekvencí.

GNS_23 Každých T sekund, kde T je hodnota menší než nebo rovná 10, pokud neprobíhá vazba nebo vzájemné ověření pravosti a dohoda na klíči relace, si celek ve vozidle vyžádá od vnějšího zařízení GNSS údaje o poloze podle tohoto postupu:

1. Celek ve vozidle si od vnějšího zařízení GNSS vyžádá údaje o poloze společně s parametrem přesnosti (z věty GSA NMEA). Bezpečnostní přijímač-vysílač VU použije příkaz SELECT a READ RECORD(S) podle ISO/IEC 7816-4:2013 v režimu bezpečného předávání zpráv pouze s ověřením pravosti podle popisu v dodatku 11 části 11.5 s identifikátorem souboru '2F2F' a číslem RECORD rovným '01' pro větu RMC NMEA a '02', '03', '04', '05', '06' pro větu GSA NMEA.

2. Poslední přijaté údaje o poloze jsou uloženy v EF s identifikátorem '2F2F' a záznamy, které popisuje tabulka 1, v bezpečnostním přijímači-vysílači GNSS, s tím, jak bezpečnostní přijímač-vysílač GNSS přijímá data NMEA z přijímače GNSS prostřednictvím datového rozhraní GNSS s frekvencí nejméně 1 Hz.

3. Bezpečnostní přijímač-vysílač GNSS odešle bezpečnostnímu přijímači-vysílači VU odpověď prostřednictvím zprávy s odpovědí APDU v režimu bezpečného předávání zpráv pouze s ověřením pravosti podle popisu v dodatku 11 části 11.5.

4. Bezpečnostní přijímač-vysílač VU ověří pravost a integritu přijaté odpovědi. V případě pozitivního výsledku jsou údaje o poloze předány procesoru VU prostřednictvím datového rozhraní GNSS.

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 průměrnou hodnotu z dostupných družicových systémů (tj. je-li poloha k dispozici).

6. Procesor VU uloží přijaté a zpracované informace, např. zeměpisnou šířku, délku, čas a rychlost, do celku ve vozidle ve formátu stanoveném v dodatku 1 – Datový slovník jako údaje GeoCoordinates, společně s hodnotou HDOP vypočítanou jako minimum z hodnot HDOP získaných z dostupných systémů GNSS.

4.2.3 *Struktura příkazu Read Record*

Tato část podrobně popisuje strukturu příkazu *Read Record*. Je doplněno bezpečné předávání zpráv (režim pouze s ověřením pravosti) podle popisu v dodatku 11 – Společné bezpečnostní mechanismy.

GNS_24 Příkaz podporuje režim bezpečného předávání zpráv pouze s ověřením pravosti, viz dodatek 11.

GNS_25 Zpráva s příkazem

Bajt	Délka	Hodnota	Popis
CLA	1	'0Ch'	Požadavek na bezpečné předávání zpráv
INS	1	'B2h'	Read Record
P1	1	'XXh'	Číslo záznamu ('00' odkazuje na aktuální záznam)
P2	1	'04h'	Čtení záznamu s číslem záznamu uvedeným v P1
Le	1	'XXh'	Očekávaná délka dat. Počet bajtů ke čtení.

GNS_26 Záznam, na který odkazuje P1, se stává aktuálním záznamem.

Bajt	Délka	Hodnota	Popis
#1-#X	X	'XX..XXh'	Přečtená data
SW	2	'XXXXh'	Stavová slova (SW1, SW2)

— Je-li příkaz úspěšný, bezpečnostní přijímač-vysílač GNSS vrátí '**9000**'.

— Není-li aktuální soubor uspořádán do záznamů, bezpečnostní přijímač-vysílač GNSS vrátí '**6981**'.

— Je-li příkaz použit s parametrem P1 = '00', ale žádný EF není aktuální, bezpečnostní přijímač-vysílač GNSS vrátí '**6986**' (příkaz není povolen).

— Není-li záznam nalezen, bezpečnostní přijímač-vysílač GNSS vrátí '**6A 83**'.

— Pokud vnější zařízení GNSS zjistilo nedovolenou manipulaci, vrátí stavová slova '**66 90**'.

GNS_27 Bezpečnostní přijímač-vysílač GNSS podporuje tyto příkazy tachografu druhé generace specifikované v dodatku 2:

Příkaz	Odkaz
Select	Dodatek 2 kapitola 3.5.1
Read Binary	Dodatek 2 kapitola 3.5.2
Get Challenge	Dodatek 2 kapitola 3.5.4
PSO: Verify Certificate	Dodatek 2 kapitola 3.5.7
External Authenticate	Dodatek 2 kapitola 3.5.9
General Authenticate	Dodatek 2 kapitola 3.5.10
MSE:SET	Dodatek 2 kapitola 3.5.11

4.3 **Vazba, vzájemné ověření pravosti a dohoda na klíči relace mezi vnějším zařízením GNSS a celkem ve vozidle**

Vazba, vzájemné ověření pravosti a dohoda na klíči relace mezi vnějším zařízením GNSS a celkem ve vozidle jsou popsány v dodatku 11 – Společné bezpečnostní mechanismy, kapitole 11.

4.4 **Zpracování chyb**

Tato část popisuje, jak jsou v celku ve vozidle zpracovávány a zaznamenávány potenciální chybové stavy vnějšího zařízení GNSS.

4.4.1 *Chyba komunikace s vnějším zařízením GNSS*

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 '53'H *External GNSS communication fault* (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 popisuje část 4.2.

4.4.2 *Narušení fyzické integrity vnějšího zařízení GNSS*

GNS_29 Při narušení vnějšího zařízení GNSS bezpečnostní přijímač-vysílač GNSS vymaže veškerý obsah své paměti, včetně kryptografického materiálu. Jak je popsáno v bodech GNS_25 a GNS_26, VU detekuje nedovolenou manipulaci, je-li status odpovědi '6690'. Celek ve vozidle poté generuje událost typu EventFaultType enum '*55'H Tamper detection of GNSS* (detekce nedovolené manipulace s GNSS).

4.4.3 *Chybí informace o poloze z přijímače GNSS*

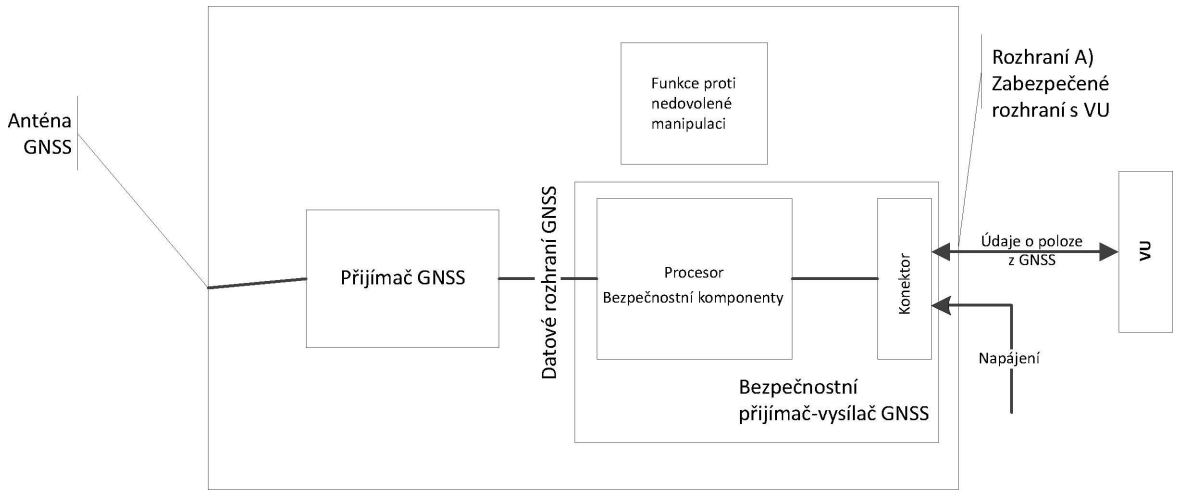
GNS_30 Pokud bezpečnostní přijímač-vysílač GNSS neobdrží data z přijímače GNSS nepřetržitě po dobu delší než 3 hodiny, bezpečnostní přijímač-vysílač GNSS generuje zprávu s odpovědí na příkaz READ RECORD s číslem RECORD rovným '01' a s datovým polem obsahujícím 12 bajtů, které mají všechny hodnotu 0xFF. Po přijetí zprávy s odpovědí s touto hodnotou datového pole VU generuje a zaznamená událost typu EventFaultType enum '52'H *external GNSS receiver fault* (závada vnějšího zařízení 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.

4.4.4 *Skončení platnosti certifikátu vnějšího zařízení GNSS*

GNS_31 Pokud celek ve vozidle zjistí, že certifikát EGF používaný pro vzájemné ověření pravosti již není platný, VU generuje a zaznamená závadu záznamového zařízení typu EventFaultType enum *'56'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.

Obrázek 4

Schéma vnějšího zařízení GNSS



5. CELEK VE VOZIDLE BEZ VNĚJŠÍHO ZAŘÍZENÍ GNSS

5.1 Konfigurace

V této konfiguraci je přijímač GNSS uvnitř celku ve vozidle, jak popisuje obrázek 1.

GNS_32 Přijímač GNSS funguje jako vysílač a předává věty NMEA procesoru VU, který funguje jako přijímač, s frekvencí 1/10 Hz nebo vyšší, pokud jde o předem definovanou sadu vět NMEA, která musí zahrnovat přinejmenším věty RMC a GSA.

GNS_33 K celku ve vozidle je připojena externí anténa GNSS instalovaná na vozidle nebo interní anténa GNSS.

5.2 Zpracování chyb

5.2.1 *Chybí informace o poloze z přijímače GNSS*

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 '51'H *Internal GNSS receiver fault* (závada interního 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.

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). Tato událost se zaznamená společně s hodnotou vnitřních hodin celku ve vozidle a je spojena s automatickým nastavením času. Po vyvolání události nesouladu času VU nekontroluje časový nesoulad po dobu následujících 12 hodin. Tato událost se nevyvolá v případech, kdy během posledních 30 dnů přijímač GNSS nedetekoval žádný platný signál GNSS. Jakmile jsou však znovu k dispozici údaje o poloze z přijímače GNSS, provede se automatické nastavení času.

7. NESOULAD ÚDAJŮ O POHYBU VOZIDLA

GNS_35 VU generuje a zaznamená událost „Nesoulad údajů o pohybu vozidla“ (viz požadavek 84 v této příloze) s časovým razítkem s aktuálním časem, pokud jsou informace o pohybu vozidla vypočtené ze snímače pohybu v konfliktu s informacemi o pohybu vozidla vypočtenými z vnitřního přijímače GNSS nebo vnějšího zařízení GNSS. Pro účely detekce těchto konfliktů se použije medián rozdílů rychlostí mezi těmito dvěma zdroji, jak je specifikováno níže:

— každých maximálně 10 sekund se vypočte absolutní hodnota rozdílu rychlosti vozidla odhadnuté z GNSS a rychlosti odhadnuté ze snímače pohybu,

— k výpočtu mediánu se použijí všechny vypočtené hodnoty v časovém okně zahrnujícím posledních pět minut pohybu,

— medián se vypočte jako průměr z 80 % hodnot, které zůstanou po eliminaci hodnot, jež jsou v absolutní hodnotě nejvyšší.

Událost „Nesoulad údajů o pohybu vozidla“ se vyvolá, pokud je medián po dobu pěti nepřerušených minut pohybu vozidla vyšší než 10 km/h. Volitelně lze použít další nezávislé zdroje detekce pohybu vozidla, aby byla detekce neoprávněných manipulací s tachografem spolehlivější. (*Poznámka:* použití mediánu za posledních 5 minut má za cíl omezit riziko plynoucí z odlehlých a přechodných hodnot.) Tato událost se nevyvolá za těchto podmínek: a) během převozu lodí / převozu vlakem, b) pokud nejsou k dispozici údaje o poloze z přijímače GNSS a c) v kalibračním režimu.

Dodatek 13

ROZHRANÍ ITS

OBSAH

1. ÚVOD

Tento dodatek stanoví koncepci a postupy pro implementaci rozhraní s inteligentními dopravními systémy (ITS) podle článku 10 nařízení (EU) č. 165/2014 (dále jen *nařízení*).

Nařízení stanoví, že tachografy vozidel mohou být vybaveny standardizovaným rozhraním umožňujícím, aby údaje zaznamenané či vytvořené tachografem byly v provozním režimu používány vnějším zařízením, jsou-li splněny tyto podmínky:

a) rozhraní nemá vliv na pravost a integritu údajů tachografu;

b) rozhraní vyhovuje podrobným ustanovením uvedeným v článku 11;

c) vnější zařízení připojené k rozhraní má přístup k osobním údajům, včetně údajů o zeměpisné poloze, pouze po prokazatelném souhlasu řidiče, k němuž se tyto údaje vztahují.

2. OBLAST PŮSOBNOSTI

Tento dodatek stanoví, jak aplikace ve vnějších zařízeních mohou prostřednictvím připojení Bluetooth® získávat data (dále též *údaje*) z tachografu.

Údaje dostupné prostřednictvím tohoto rozhraní jsou popsány v příloze 1 tohoto dokumentu. Toto rozhraní nebrání implementaci dalších rozhraní (např. prostřednictvím sběrnice CAN) pro přenos dat z celku ve vozidle do jiných procesorových jednotek vozidla.

Tento dodatek specifikuje:

— *údaje* dostupné prostřednictvím rozhraní ITS,

— profil Bluetooth® používaný pro přenos dat,

— postupy dotazování a stahování a posloupnost operací,

— mechanismus párování mezi tachografem a vnějším zařízením,

— mechanismus poskytnutí souhlasu, který je k dispozici řidiči.

Pro upřesnění, tato příloha 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 10 Společné bezpečnostní mechanismy]),

— protokoly Bluetooth® používané rozhraním ITS.

2.1 **Zkratky, definice a notace**

Pro účely tohoto dodatku se použijí tyto zkratky a definice:

komunikace	výměna informací/dat mezi nadřízenou („master“) jednotkou (tj. tachografy) a vnější jednotkou prostřednictvím rozhraní ITS přes připojení Bluetooth®
údaje	sady dat specifikované v příloze 1
nařízení	nařízení Evropského parlamentu a Rady (EU) č. 165/2014 ze dne 4. února 2014 o tachografech v silniční dopravě, o zrušení nařízení Rady (EHS) č. 3821/85 o záznamovém zařízení v silniční dopravě a o změně nařízení Evropského parlamentu a Rady (ES) č. 561/2006 o harmonizaci některých předpisů v sociální oblasti týkajících se silniční dopravy
BR	základní rychlost přenosu dat (*Basic Rate*)
EDR	zvýšená rychlost přenosu dat (*Enhanced Data Rata*)
GNSS	globální družicový navigační systém (*Global Navigation Satellite System*)
IRK	klíč k rozlišení totožnosti (*Identity Resolution Key*)
ITS	inteligentní dopravní systém (*Intelligent Transport System*)
LE	nízká spotřeba energie (*Low Energy*)
PIN	kód PIN (*Personal Identification Number*)
PUC	osobní odblokovací kód (*Personal Unblocking Code*)
SID	identifikátor služby (*Service Identifier*)
SPP	profil sériového portu (*Serial Port Profile*)
SSP	bezpečné jednoduché párování (*Secure Simple Pairing*)
TRTP	parametr požadavku na přenos (*Transfer Request Parameter*)
TREP	parametr odpovědi na požadavek na přenos (*Transfer Response Parameter*)
VU	celek ve vozidle (*Vehicle Unit*)

3. NAŘÍZENÍ A NORMY, NA KTERÉ SE ODKAZUJE

Specifikace definované v tomto dodatku se odvolávají na níže uvedená nařízení a normy nebo jejich části a závisí na nich. Příslušné normy nebo jejich ustanovení jsou specifikovány v ustanoveních tohoto dodatku. V případě rozporu mají přednost ustanovení tohoto dodatku.

Nařízení a normy, na které se odkazuje v tomto dodatku, jsou:

— nařízení Evropského parlamentu a Rady (EU) č. 165/2014 ze dne 4. února 2014 o tachografech v silniční dopravě, o zrušení nařízení Rady (EHS) č. 3821/85 o záznamovém zařízení v silniční dopravě a o změně nařízení Evropského parlamentu a Rady (ES) č. 561/2006 o harmonizaci některých předpisů v sociální oblasti týkajících se silniční dopravy,

— nařízení Evropského parlamentu a Rady (ES) č. 561/2006 ze dne 15. března 2006 o harmonizaci některých předpisů v sociální oblasti týkajících se silniční dopravy, o změně nařízení Rady (EHS) č. 3821/85 a (ES) č. 2135/98 a o zrušení nařízení Rady (EHS) č. 3820/85,

— ISO 16844-4: *Road vehicles – Tachograph systems – Part 4: Can interface*,

— ISO 16844-7: *Road vehicles – Tachograph systems – Part 7: Parameters*,

— Bluetooth® – *Serial Port Profile – V1.2*,

— Bluetooth® – *Core Version 4.2*,

— protokol NMEA 0183 V4.1.

4. PRINCIPY ČINNOSTI ROZHRANÍ

4.1 **Předpoklady přenosu dat prostřednictvím rozhraní ITS**

Celek ve vozidle je odpovědný za aktualizaci a uchovávání údajů, které mají být uloženy ve VU, bez jakékoli účasti rozhraní ITS. Způsob, jakým je tohoto cíle dosaženo, je vnitřní funkcí VU specifikovanou jinde v nařízení, a není specifikován v tomto dodatku.

4.1.1 *Údaje poskytované prostřednictvím rozhraní ITS*

Celek ve vozidle je odpovědný za aktualizaci údajů, které budou k dispozici prostřednictvím rozhraní ITS, s četností určenou v rámci postupů VU bez jakékoli účasti rozhraní ITS. Z údajů VU se vychází při naplnění a aktualizaci *údajů* a způsob, jakým je tohoto cíle dosaženo, je specifikován jinde v *nařízení*, nebo pokud taková specifikace neexistuje, je funkcí konstrukce výrobku a není specifikován v tomto dodatku.

4.1.2 *Obsah údajů*

Obsah *údajů* je specifikován v příloze 1 tohoto dodatku.

4.1.3 *Aplikace ITS*

Aplikace ITS používají údaje zpřístupněné prostřednictvím rozhraní ITS např. pro optimalizaci správy činností řidiče při současném dodržení nařízení, pro zjišťování možných závad tachografu nebo pro využití údajů GNSS. Specifikace aplikací nespadá do oblasti působnosti tohoto dodatku.

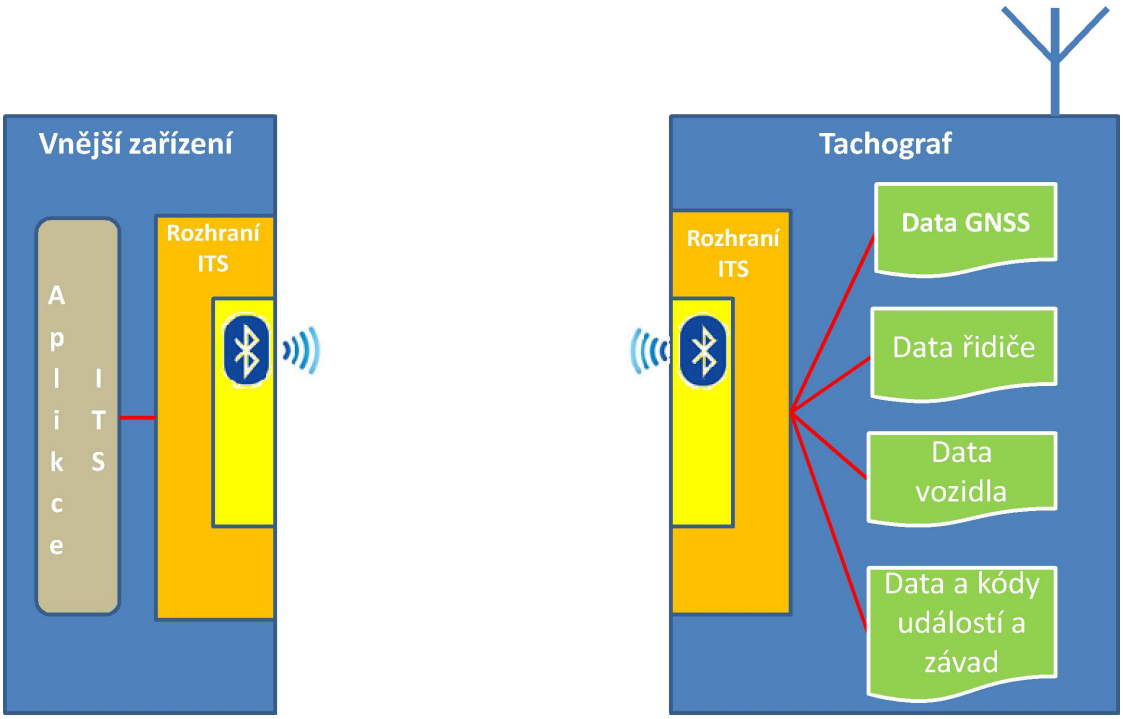
4.2 **Komunikační technologie**

Výměna *údajů* prostřednictvím rozhraní ITS je realizována pomocí rozhraní Bluetooth® kompatibilního s verzí 4.2 nebo novější. Bluetooth® pracuje v bezlicenčním průmyslovém, vědeckém a zdravotnickém pásmu (ISM) na frekvenci 2,4 až 2,485 GHz. Bluetooth® 4.2 nabízí vylepšené mechanismy zajištění soukromí a bezpečnosti a zvyšuje rychlost a spolehlivost přenosu dat. Pro účely této specifikace se používá rádiové spojení Bluetooth® třídy 2 s dosahem až 10 metrů. Více informací o technologii Bluetooth® 4.2 je k dispozici na adrese www.bluetooth.com (https://www.bluetooth.org/en-us/specification/adopted-specifications?_ga=1.215147412.2083380574.1435305676).

Komunikace se s komunikačním zařízením naváže poté, co autorizované zařízení dokončí proces párování. Protože Bluetooth® používá k řízení toho, kdy a kam mohou zařízení odesílat data, model „master/slave“, bude nadřízenou („master“) jednotkou tachograf a podřízenou („slave“) jednotkou vnější zařízení.

Dostane-li se vnější zařízení poprvé do dosahu VU, lze iniciovat proces párování Bluetooth® (viz rovněž přílohu 2). Zařízení sdílejí svoje adresy, názvy, profily a společný tajný klíč, který 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 10 Společné bezpečnostní mechanismy.

Obecný princip komunikace je popsán na následujícím obrázku.



Pro přenos dat z celku ve vozidle do vnějšího zařízení se používá profil SPP (*Serial Port Profile*).

4.3 **Autorizace pomocí kódu PIN**

Z bezpečnostních důvodů VU vyžaduje 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.

Po úspěšném zadání kódu PIN se zařízení zařadí na seznam povolených zařízení. Seznam povolených zařízení pojme nejméně 64 zařízení spárovaných s daným celkem ve vozidle.

Je-li třikrát za sebou poskytnut špatný kód PIN, je zařízení dočasně zařazeno na seznam zakázaných zařízení. Dokud je zařízení na seznamu zakázaných zařízení, každý další pokus z tohoto zařízení se odmítne. Je-li znovu třikrát za sebou poskytnut špatný kód PIN, prodlužuje se postupně doba zákazu (viz tabulku 1). Poskytnutím správného kódu PIN se obnoví výchozí doba zákazu a počet pokusů. Na obrázku 1 v příloze 2 je uvedeno schéma logické posloupnosti pokusu o ověření kódu PIN.

Tabulka 1

Doba zákazu v závislosti na počtu neúspěšných poskytnutí správného kódu PIN za sebou

Počet po sobě jdoucích neúspěchů	Doba zákazu
3	30 sekund
6	5 minut
9	1 hodina
12	24 hodin
15	trvale

Není-li správný kód PIN poskytnut patnáctkrát (5 × 3) za sebou, je jednotka ITS trvale zařazena na seznam zakázaných zařízení. Tento trvalý zákaz je možné zrušit pouze zadáním správného kódu PUC.

Kód PUC je složen z 8 číslic a poskytuje jej výrobce společně s celkem ve vozidle. Je-li desetkrát za sebou zadán špatný kód PUC, je jednotka ITS zařazena na seznam zakázaných zařízení nezrušitelně.

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.

Zařízení jsou na seznamu povolených zařízení uchovávána, dokud je uživatel ručně neodstraní (např. přes rozhraní člověk-stroj VU nebo jinými prostředky). Ze seznamu povolených zařízení tak lze odstraňovat ztracené nebo odcizené jednotky ITS. Ze seznamu povolených zařízení ve VU se rovněž automaticky odstraní jednotky ITS, které jsou mimo dosah spojení Bluetooth po dobu delší než 24 hodin. Při opětovném navázání komunikace musí tyto jednotky znovu poskytnout správný kód PIN.

Formát zpráv mezi rozhraním VU a samotným VU není stanoven, ale ponechán na rozhodnutí výrobce. Dotyčný výrobce však musí zajistit dodržování formátu zpráv mezi jednotkou ITS a rozhraním VU (viz specifikace v notaci ASN.1).

Všechny požadavky na údaje jsou proto před jakýmkoli dalším zpracováním podrobeny řádné kontrole pověření odesílatele. Na obrázku 2 přílohy 2 je uvedeno schéma logické posloupnosti tohoto postupu. Jakékoli zařízení uvedené na seznamu zakázaných zařízení je automaticky odmítnuto, zařízení neuvedené na žádném seznamu obdrží žádost o PIN, kterou musí splnit před novým odesláním požadavku na údaje.

4.4 **Formát zpráv**

Všechny zprávy vyměňované mezi jednotkou ITS a rozhraním VU mají formát struktury sestávající ze tří částí: Hlavička se skládá z bajtu cíle (TGT), bajtu zdroje (SRC) a bajtu délky (LEN).

Datové pole se skládá z bajtu identifikátoru služby (SID) a proměnného počtu datových bajtů (maximálně 255).

Bajt kontrolního součtu je jednobajtový součet modulo 256 všech bajtů zprávy kromě samotného CS.

Zpráva je ve tvaru Big Endian.

Tabulka 2

Obecný formát zpráv

Hlavička			Datové pole					Kontrolní součet
TGT	SRC	LEN	SID	TRTP	CC	CM	DATA	CS
3 bajty			Max. 255 bajtů					1 bajt

Hlavička

TGT a SRC: ID zařízení, které je cílem (TGT) a zdrojem (SRC) zprávy. Rozhraní VU má standardní ID „EE“. Toto ID nelze změnit. Jednotka ITS používá standardní ID „A0“ pro svou první zprávu v rámci komunikační relace. Rozhraní VU potom jednotce ITS přiřadí jedinečné ID a informuje ji o tomto ID pro budoucí zprávy v rámci relace.

Bajt LEN zohledňuje pouze část „DATA“ datového pole (viz tabulku 2), první 4 bajty jsou implicitní.

Rozhraní VU ověří pravost odesílatele zprávy křížovou kontrolou vlastního seznamu IDList s daty Bluetooth, při níž zkontroluje, zda je jednotka ITS, která je v seznamu s poskytnutým ID, aktuálně v dosahu připojení Bluetooth.

Datové pole

Kromě SID datové pole rovněž obsahuje další parametry: parametr požadavku na přenos (TRTP) a bajty čítačů.

Jsou-li data, která je třeba přenést, 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.

Pokud se CC a CM nepoužívají, mají hodnotu 0xFF.

Například následující zpráva:

HLAVIČKA	SID	TRTP	CC	CM	DATA	CS
3 bajty	Delší než 255 bajtů					1 bajt

se přenese jako:

HLAVIČKA	SID	TRTP	01	n	DATA	CS
3 bajty	255 bajty					1 bajt

HLAVIČKA	SID	TRTP	02	n	DATA	CS
3 bajty	255 bajty					1 bajt

…

HLAVIČKA	SID	TRTP	N	N	DATA	CS
3 bajty	Max. 255 bajtů					1 bajt

Tabulka 3 obsahuje zprávy, které si mohou VU a jednotka ITS vyměňovat. Obsah jednotlivých parametrů je uveden v hexadecimálním formátu. V tabulce nejsou z důvodu přehlednosti uvedeny CC a CM, viz kompletní formát výše.

Tabulka 3

Podrobný obsah zpráv

Zpráva	Hlavička			DATA			Kontrolní součet
	TGT	SRC	LEN	SID	TRTP	DATA	
RequestPIN	*ITSID*	EE	00	01	FF		
SendITSID	*ITSID*	EE	01	02	FF	*ITSID*	
SendPIN	EE	*ITSID*	04	03	FF	4*INTEGER (0..9)	
PairingResult	*ITSID*	EE	01	04	FF	BOOLEAN (T/F)	
SendPUC	EE	*ITSID*	08	05	FF	8*INTEGER (0..9)	
BanLiftingResult	*ITSID*	EE	01	06	FF	BOOLEAN (T/F)	
RequestRejected	*ITSID*	EE	08	07	FF	Time	
RequestData							
standardTachData	EE	*ITSID*	01	08	01		
personalTachData	EE	*ITSID*	01	08	02		
gnssData	EE	*ITSID*	01	08	03		
standardEventData	EE	*ITSID*	01	08	04		
personalEventData	EE	*ITSID*	01	08	05		
standardFaultData	EE	*ITSID*	01	08	06		
manufacturerData	EE	*ITSID*	01	08	07		

Zpráva	Hlavička			DATA			Kontrolní součet
	TGT	SRC	LEN	SID	TRTP	DATA	
ResquestAccepted	*ITSID*	EE	Len	09	TREP	Data	
DataUnavailable							
No data available	*ITSID*	EE	02	0A	TREP	10	
Personal data not shared	*ITSID*	EE	02	0A	TREP	11	
NegativeAnswer							
General reject	*ITSID*	EE	02	0B	SID Req	10	
Service not supported	*ITSID*	EE	02	0B	SID Req	11	
Sub function not supported	*ITSID*	EE	02	0B	SID Req	12	
Incorrect message length	*ITSID*	EE	02	0B	SID Req	13	
Conditions not correct or request sequence error	*ITSID*	EE	02	0B	SID Req	22	
Request out of range	*ITSID*	EE	02	0B	SID Req	31	
Response pending	*ITSID*	EE	02	0B	SID Req	78	
ITSID Mismatch	*ITSID*	EE	02	0B	SID Req	FC	
ITSID Not Found	*ITSID*	EE	02	0B	SID Req	FB	

RequestPIN (SID 01)

Tuto zprávu vyšle rozhraní VU, pokud jednotka ITS, která není zařazena do seznamu zakázaných zařízení ani do seznamu povolených zařízení, odesílá jakýkoli požadavek na údaje.

SendITSID (SID 02)

Tuto zprávu vyšle rozhraní VU, kdykoli nové zařízení odesílá požadavek. Toto zařízení použije výchozí ID „A0“, než je mu přiděleno jedinečné ID pro komunikační relaci.

SendPIN (SID 03)

Tuto zprávu vyšle jednotka ITS, aby byla rozhraním VU zařazena do seznamu povolených zařízení. Obsahem této zprávy je kód 4 hodnot INTEGER od 0 do 9.

PairingResult (SID 04)

Tuto zprávu vyšle rozhraní VU, aby informovalo jednotku ITS, zda odeslala správný kód PIN. Obsahem této zprávy je hodnota BOOLEAN „True“, pokud byl kód PIN správný, nebo „False“ v opačném případě.

SendPUC (SID 05)

Tuto zprávu vyšle jednotka ITS, aby rozhraní VU zrušilo sankci zařazení do seznamu zakázaných zařízení. Obsahem této zprávy je kód 8 hodnot INTEGER od 0 do 9.

BanLiftingResult (SID 06)

Tuto zprávu vyšle rozhraní VU, aby informovalo jednotku ITS, zda odeslala správný kód PUC. Obsahem této zprávy je hodnota BOOLEAN „True“, pokud byl kód PUC správný, nebo „False“ v opačném případě.

RequestRejected (SID 07)

Tuto zprávu vyšle rozhraní VU jako odpověď na jakoukoli zprávu od jednotky ITS zařazené do seznamu zakázaných zařízení kromě „SendPUC“. Zpráva obsahuje zbývající čas, po který je jednotka ITS zařazena do seznamu zakázaných zařízení, ve formátu sekvence „Time“ podle přílohy 3.

RequestData (SID 08)

Tuto zprávu pro zpřístupnění údajů vyšle jednotka ITS. Jednobajtový parametr TRTP označuje typ požadovaných údajů. Existuje několik typů údajů:

— standardTachData (TRTP 01): údaje dostupné z tachografu a klasifikované jako neosobní,

— personalTachData (TRTP 02): údaje dostupné z tachografu a klasifikované jako osobní,

— gnssData (TRTP 03): údaje GNSS, vždy osobní,

— standardEventData (TRTP 04): údaje zaznamenaných událostí klasifikované jako neosobní,

— personalEventData (TRTP 05): údaje zaznamenaných událostí klasifikované jako osobní,

— standardFaultData (TRTP 06): zaznamenané závady klasifikované jako neosobní,

— manufacturerData (TRTP 07): údaje zpřístupněné výrobcem.

Více informací o obsahu jednotlivých typů údajů viz přílohu 3 tohoto dodatku.

Více informací o formátu a obsahu údajů GNSS viz dodatek 12.

Více informací o kódu údajů událostí a závadách viz přílohy IB a IC.

RequestAccepted (SID 09)

Tuto zprávu vyšle rozhraní VU, pokud zpráva „RequestData“ od jednotky ITS byla akceptována. Tato zpráva obsahuje jednobajtový parametr TREP, což je bajt TRTP příslušné zprávy RequestData, a všechny údaje požadovaného typu.

DataUnavailable (SID 0A)

Tuto zprávu vyšle rozhraní VU, pokud z nějakého důvodu nelze odeslat požadovaná data jednotce ITS zařazené do seznamu povolených zařízení. Zpráva obsahuje jednobajtový parametr TREP, což je TRTP požadovaných údajů, a jednobajtový kód chyby podle tabulky 3. K dispozici jsou tyto kódy:

— *No data available* (data nejsou k dispozici) (10): Rozhraní VU nemůže z neurčených důvodů přistupovat k údajům VU.

— *Personal data not shared* (osobní údaje nesdíleny) (11): Jednotka ITS se pokouší získat osobní údaje, které nejsou sdíleny.

NegativeAnswer (SID 0B)

Tyto zprávy vysílá rozhraní VU, pokud požadavku nelze vyhovět z jiného důvodu, než je nedostupnost údajů. Tyto zprávy jsou zpravidla výsledkem špatného formátu požadavku (délka, SID, ITSID…), ale mohou mít i jiné příčiny. TRTP v datovém poli obsahuje SID požadavku. Datové pole obsahuje kód označující důvod negativní odpovědi. K dispozici jsou následující kódy:

— *General Reject* (obecné odmítnutí, kód: 10)

— Akci nelze provést z důvodu, který není uveden níže ani v části (doplnit číslo části *DataUnavailable*).

— *Service not supported* (služba nepodporována, kód: 11)

— Nesrozumitelné SID požadavku.

— *Sub function not supported* (podfunkce nepodporována, kód: 12)

— Nesrozumitelný parametr TRTP požadavku. Například může hodnota chybět nebo být mimo rozsah přípustných hodnot.

— *Incorrect message length* (chybná délka zprávy, kód: 13)

— Délka přijaté zprávy je chybná (neshoda mezi bajtem LEN a skutečnou délkou zprávy).

— *Conditions not correct or request sequence error* (chybné podmínky nebo chybná sekvence požadavků, kód: 22)

— Požadovaná služba není aktivní nebo je chybná posloupnost zpráv s požadavky.

— *Request out of range* (požadavek mimo rozsah, kód: 33)

— Záznam s parametry požadavku (datové pole) je neplatný.

— *Response pending* (odpověď se připravuje, kód: 78)

— Požadovanou akci nelze dokončit včas a VU není připraven přijmout další požadavek.

— *ITSID Mismatch* (neshoda *ITSID*, kód: FB)

— SRC *ITSID* neodpovídá příslušnému zařízení po porovnání s informacemi Bluetooth.

— *ITSID Not Found* (*ITSID* nenalezen, kód: FC)

— SRC *ITSID* není přidružen k žádnému zařízení.

Formát zpráv popsaných v tabulce 3 specifikují řádky 1 až 72 (**FormatMessageModule**) kódu ASN.1 v příloze 3. Více podrobností o obsahu zpráv je uvedeno níže.

4.5 **Souhlas řidiče**

Všechny dostupné údaje jsou klasifikovány jako standardní, nebo osobní. Osobní údaje jsou přístupné pouze v případě, že řidič poskytne souhlas s tím, že jeho osobní údaje z tachografu mohou opustit síť vozidla a být předány aplikacím třetích stran.

Souhlas řidiče se poskytuje, když je při prvním vložení příslušné karty řidiče nebo karty dílny, kterou celek ve vozidle aktuálně nezná, držitel karty vyzván, aby vyjádřil souhlas s předáváním osobních údajů souvisejících s tachografem prostřednictvím volitelného rozhraní ITS (viz rovněž přílohu 1C odstavec 3.6.2).

Stav souhlasu (povoleno/zamítnuto) je zaznamenán v paměti tachografu.

V případě více řidičů jsou s rozhraním ITS sdíleny pouze osobní údaje o řidičích, kteří poskytli souhlas. Jsou-li například ve vozidle dva řidiči a pouze první z nich souhlasil se sdílením svých osobních údajů, nesdílí se údaje, které se týkají druhého řidiče.

4.6 **Čtení standardních údajů**

Na obrázku 3 v příloze 2 jsou uvedena schémata logické posloupnosti platného požadavku na přístup ke standardním údajům odeslaného jednotkou ITS. Jednotka ITS je řádně uvedena na seznamu povolených zařízení a nepožaduje osobní údaje; žádné další ověřování není požadováno. Schémata vycházejí z předpokladu, že již byl proveden řádný postup uvedený na obrázku 2 přílohy 2. Mohou být považovány za šedé pole *REQUEST TREATMENT* na obrázku 2.

Z dostupných údajů se za standardní považují tyto:

— standardTachData (TRTP 01),

— StandardEventData (TRTP 04),

— standardFaultData (TRTP 06).

4.7 **Čtení osobních údajů**

Na obrázku 4 v příloze 2 jsou uvedena schémata logické posloupnosti zpracování požadavku na osobní údaje. Jak bylo uvedeno výše, rozhraní VU odešle osobní údaje pouze v případě, že řidič poskytl výslovný souhlas (viz rovněž bod 4.5). V opačném případě musí být požadavek automaticky odmítnut.

Z dostupných údajů se za osobní považují tyto:

— personalTachData (TRTP 02),

— gnssData (TRTP 03),

— personalEventData (TRTP 05),

— manufacturerData (TRTP 07).

4.8 **Čtení údajů událostí a závad**

Jednotky ITS mohou požadovat údaje o událostech zahrnující seznam všech neočekávaných událostí. Tyto údaje se považují za standardní nebo za osobní, viz přílohu 3. Obsah jednotlivých událostí je v souladu s dokumentací uvedenou v příloze 1 tohoto dodatku.

PŘÍLOHA 1

SEZNAM ÚDAJŮ DOSTUPNÝCH PROSTŘEDNICTVÍM ROZHRANÍ ITS

Data	Source	Data classification (personal/ not personal)
VehicleIdentificationNumber	Vehicle Unit	**not personal**
CalibrationDate	Vehicle Unit	**not personal**
TachographVehicleSpeed speed instant t	Vehicle Unit	personal
Driver1WorkingState Selector driver	Vehicle Unit	personal
Driver2WorkingState	Vehicle Unit	personal
DriveRecognize Speed Threshold detected	Vehicle Unit	**not personal**
Driver1TimeRelatedStates Weekly day time	Driver Card	personal
Driver2TimeRelatedStates	Driver Card	personal
DriverCardDriver1	Vehicle Unit	**not personal**
DriverCardDriver2	Vehicle Unit	**not personal**
OverSpeed	Vehicle Unit	personal
TimeDate	Vehicle Unit	**not personal**
HighResolutionTotalVehicleDistance	Vehicle Unit	**not personal**
ServiceComponentIdentification	Vehicle Unit	**not personal**
ServiceDelayCalendarTimeBased	Vehicle Unit	**not personal**
Driver1Identification	Driver Card	personal
Driver2Identification	Driver Card	personal
NextCalibrationDate	Vehicle Unit	**not personal**
Driver1ContinuousDrivingTime	Driver Card	personal
Driver2ContinuousDrivingTime	Driver Card	personal
Driver1CumulativeBreakTime	Driver Card	personal
Driver2CumulativeBreakTime	Driver Card	personal
Driver1CurrentDurationOfSelectedActivity	Driver Card	personal
Driver2CurrentDurationOfSelectedActivity	Driver Card	personal

Data	Source	Data classification (personal/ not personal)
SpeedAuthorised	Vehicle Unit	**not personal**
TachographCardSlot1	Driver Card	**not personal**
TachographCardSlot2	Driver Card	**not personal**
Driver1Name	Driver Card	personal
Driver2Name	Driver Card	personal
OutOfScopeCondition	Vehicle Unit	**not personal**
ModeOfOperation	Vehicle Unit	**not personal**
Driver1CumulatedDrivingTimePreviousAndCurrentWeek	Driver Card	personal
Driver2CumulatedDrivingTimePreviousAndCurrentWeek	Driver Card	personal
EngineSpeed	Vehicle Unit	personal
RegisteringMemberState	Vehicle Unit	**not personal**
VehicleRegistrationNumber	Vehicle Unit	**not personal**
Driver1EndOfLastDailyRestPeriod	Driver Card	personal
Driver2EndOfLastDailyRestPeriod	Driver Card	personal
Driver1EndOfLastWeeklyRestPeriod	Driver Card	personal
Driver2EndOfLastWeeklyRestPeriod	Driver Card	personal
Driver1EndOfSecondLastWeeklyRestPeriod	Driver Card	personal
Driver2EndOfSecondLastWeeklyRestPeriod	Driver Card	personal
Driver1CurrentDailyDrivingTime	Driver Card	personal
Driver2CurrentDailyDrivingTime	Driver Card	personal
Driver1CurrentWeeklyDrivingTime	Driver Card	personal
Driver2CurrentWeeklyDrivingTime	Driver Card	personal
Driver1TimeLeftUntilNewDailyRestPeriod	Driver Card	personal
Driver2TimeLeftUntilNewDailyRestPeriod	Driver Card	personal
Driver1CardExpiryDate	Driver Card	personal

Data	Source	Data classification (personal/ not personal)
Driver2CardExpiryDate	Driver Card	personal
Driver1CardNextMandatoryDownloadDate	Driver Card	personal
Driver2CardNextMandatoryDownloadDate	Driver Card	personal
TachographNextMandatoryDownloadDate	Vehicle Unit	**not personal**
Driver1TimeLeftUntilNewWeeklyRestPeriod	Driver Card	personal
Driver2TimeLeftUntilNewWeeklyRestPeriod	Driver Card	personal
Driver1NumberOfTimes9hDailyDrivingTimesExceeded	Driver Card	personal
Driver2NumberOfTimes9hDailyDrivingTimesExceeced	Driver Card	personal
Driver1CumulativeUninterruptedRestTime	Driver Card	personal
Driver2CumulativeUninterruptedRestTime	Driver Card	personal
Driver1MinimumDailyRest	Driver Card	personal
Driver2MinimumDailyRest	Driver Card	personal
Driver1MinimumWeeklyRest	Driver Card	personal
Driver2MinimumWeeklyRest	Driver Card	personal
Driver1MaximumDailyPeriod	Driver Card	personal
Driver2MaximumDailyPeriod	Driver Card	personal
Driver1MaximumDailyDrivingTime	Driver Card	personal
Driver2MaximumDailyDrivingTime	Driver Card	personal
Driver1NumberOfUsedReducedDailyRestPeriods	Driver Card	personal
Driver2NumberOfUsedReducedDailyRestPeriods	Driver Card	personal
Driver1RemainingCurrentDrivingTime	Driver Card	personal
Driver2RemainingCurrentDrivingTime	Driver Card	personal
GNSS position	Vehicle Unit	personal

2) PRŮBĚŽNÉ ÚDAJE GNSS DOSTUPNÉ PO SOUHLASU ŘIDIČE

Viz dodatek 12 – GNSS.

3) KÓDY UDÁLOSTÍ DOSTUPNÝCH BEZ SOUHLASU ŘIDIČE

Událost	Pravidla ukládání	Údaje, které se ukládají pro každou událost
Vložení neplatné karty	— 10 posledních událostí	— datum a čas události — typ, číslo, vydávající členský stát a generace karty (karet) vytvářející(ch) událost — počet podobných událostí v tentýž den
Konflikt karet	— 10 posledních událostí	— datum a čas začátku události — datum a čas konce události — typ, číslo, vydávající členský stát a generace dvou karet vytvářejících konflikt
Nesprávné uzavření poslední relace karty	— 10 posledních událostí	— datum a čas vložení karty — typ, číslo, vydávající členský stát a generace karty (karet) — poslední data relace přečtená z karty: — datum a čas vložení karty — VRN, členský stát registrace a generace VU
Přerušení napájení (2)	— nejdelší událost v každém z 10 posledních 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 konci události — počet podobných událostí v tentýž den
Chyba komunikace se zařízením pro dálkovou komunikaci	— nejdelší událost v každém z 10 posledních 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 konci události — počet podobných událostí v tentýž den
Chybí informace o poloze z přijímače GNSS	— nejdelší událost v každém z 10 posledních 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 konci události — počet podobných událostí v tentýž den
Chyba údajů o pohybu vozidla	— nejdelší událost v každém z 10 posledních 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 konci události — počet podobných událostí v tentýž den

Událost	Pravidla ukládání	Údaje, které se ukládají pro každou událost
Nesoulad údajů o pohybu vozidla	— nejdelší událost v každém z 10 posledních 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 konci události — počet podobných událostí v tentýž den
Pokus o narušení zabezpečení	10 posledních událostí pro každý typ události	— datum a čas začátku události — datum a čas konce události (je-li relevantní) — typ, číslo, vydávající členský stát a generace všech karet vložených na začátku a/nebo konci události — typ události
Časový konflikt	— nejdelší událost v každém z 10 posledních dnů výskytu — 5 nejdelších 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 konci události — počet podobných událostí v tentýž den

4) KÓDY UDÁLOSTÍ DOSTUPNÝCH SE SOUHLASEM ŘIDIČE

Událost	Pravidla ukládání	Údaje, které se ukládají pro každou událost
Řízení bez náležité karty	— nejdelší událost v každém z 10 posledních 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 konci události — počet podobných událostí v tentýž den
Vložení karty během řízení	— poslední událost v každém z 10 posledních dnů výskytu	— datum a čas události — typ, číslo, vydávající členský stát a generace karty (karet) — počet podobných událostí v tentýž den
Překročení povolené rychlosti (1)	— nejzávažnější událost v každém z 10 posledních dnů výskytu (tj. případ s nejvyšší průměrnou rychlostí) — 5 nejzávažnějších událostí za posledních 365 dnů — první událost, která nastala po poslední kalibraci	— datum a čas začátku události — datum a čas konce události — maximální rychlost změřená v průběhu události — aritmetický průměr rychlostí změřených v průběhu události — typ, číslo, vydávající členský stát a generace karty řidiče (v příslušných případech) — počet podobných událostí v tentýž den

5) KÓDY ÚDAJŮ ZÁVAD DOSTUPNÝCH BEZ SOUHLASU ŘIDIČE

Závada	Pravidla ukládání	Údaje, které se ukládají při závadě
Závada karty	— 10 posledních závad karty řidiče	— datum a čas začátku závady — datum a čas konce závady — typ, číslo, vydávající členský stát a generace karty (karet)
Závady záznamového zařízení	— 10 posledních závad pro každý typ závady — první závada po poslední kalibraci	— datum a čas začátku závady — datum a čas konce závady — typ závady — typ, číslo, vydávající členský stát a generace všech karet vložených na začátku a/nebo konci závady

Tato závada se aktivuje, pokud zařízení není v kalibračním režimu a nastane jakákoli z následujících poruch:

— interní závada celku ve vozidle,

— závada tiskárny,

— závada displeje,

— závada stahování,

— závada snímače,

— závada přijímače GNSS nebo vnějšího zařízení GNSS,

— závada zařízení pro dálkovou komunikaci.

6) UDÁLOSTI A ZÁVADY SPECIFICKÉ PRO VÝROBCE DOSTUPNÉ BEZ SOUHLASU ŘIDIČE

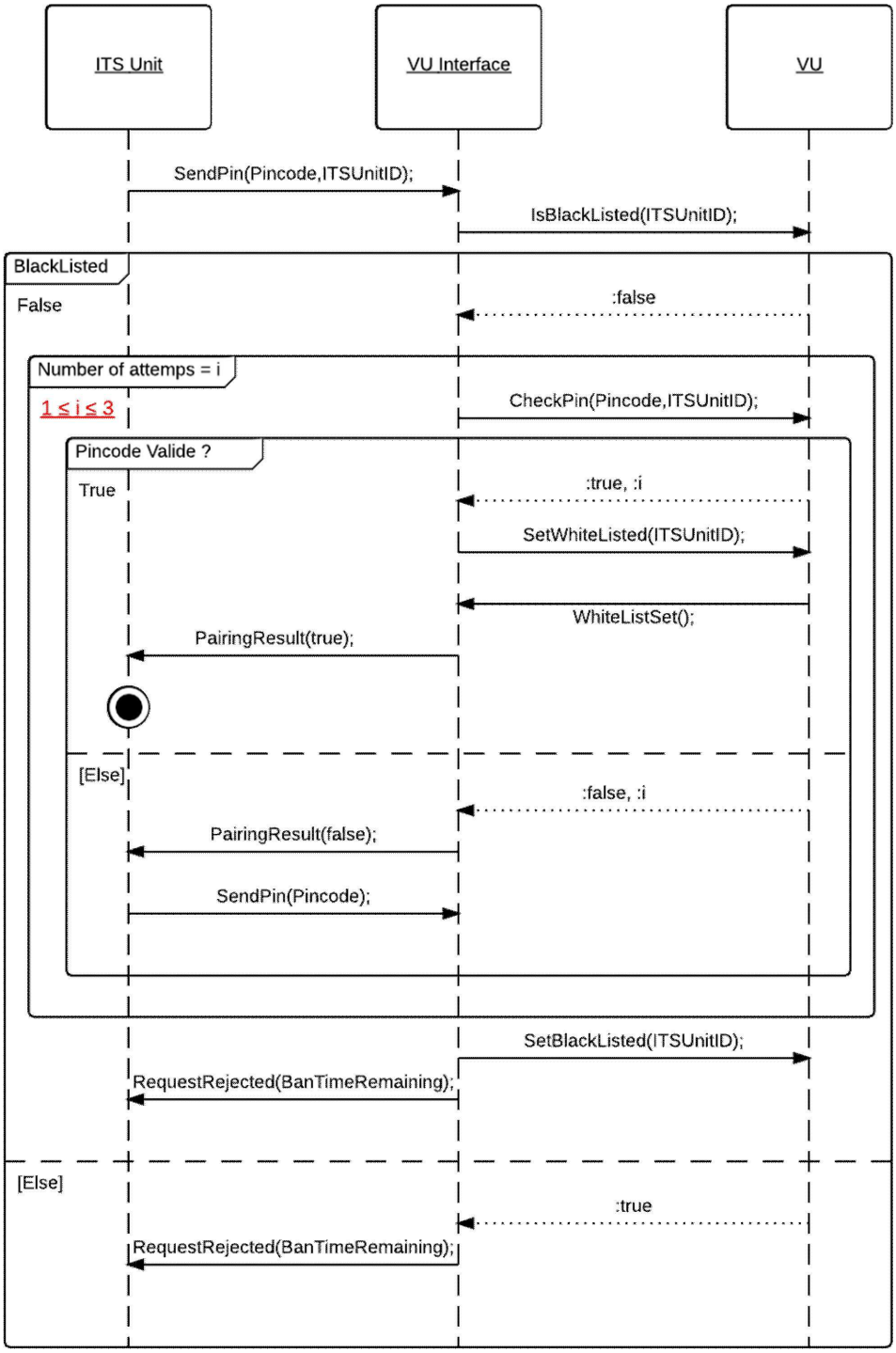
Událost nebo závada	Pravidla ukládání	Údaje, které se ukládají pro každou událost
Stanoví výrobce	Stanoví výrobce	Stanoví výrobce

PŘÍLOHA 2

SCHÉMATA LOGICKÉ POSLOUPNOSTI VÝMĚN ZPRÁV S JEDNOTKOU ITS

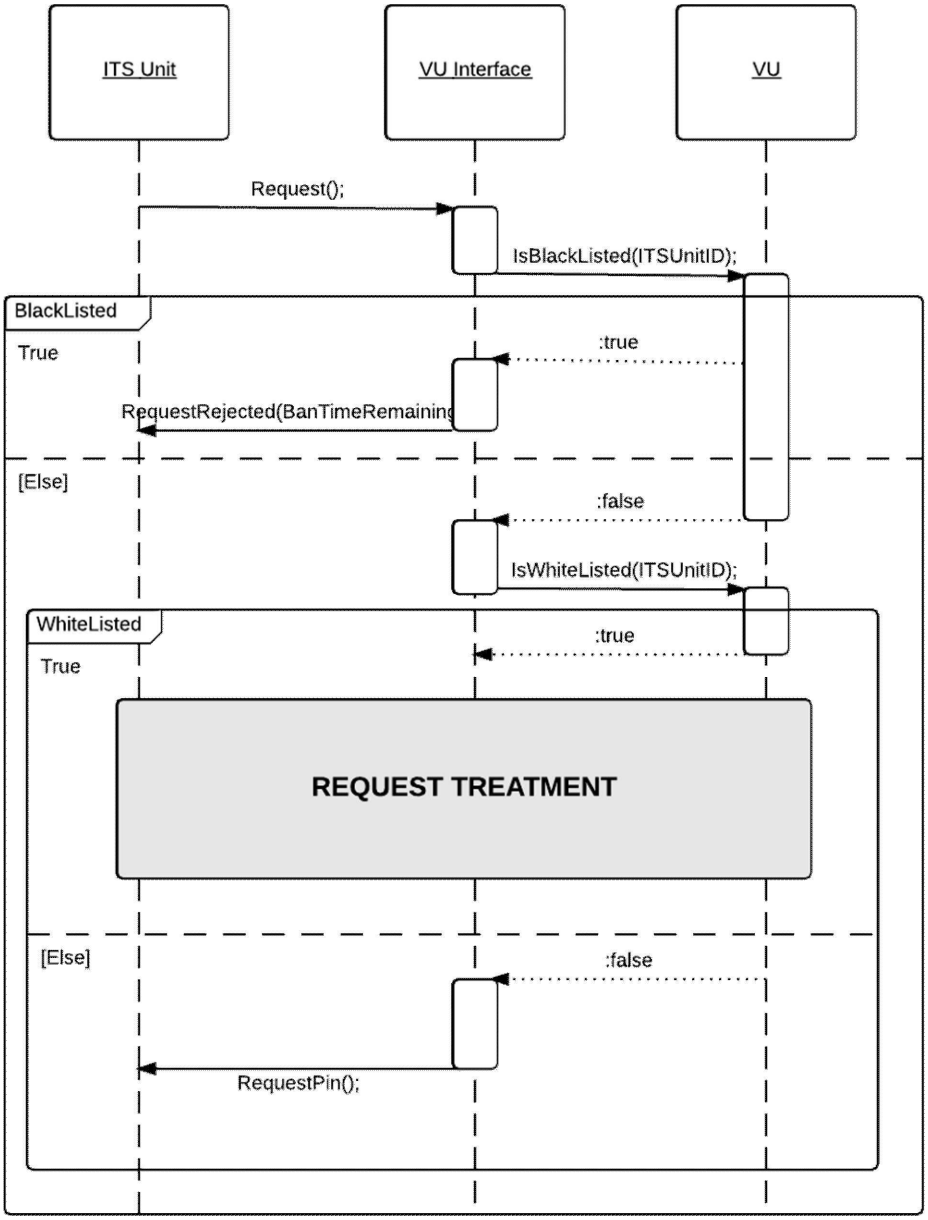
Obrázek 1

Schéma logické posloupnosti pokusu o ověření kódu PIN



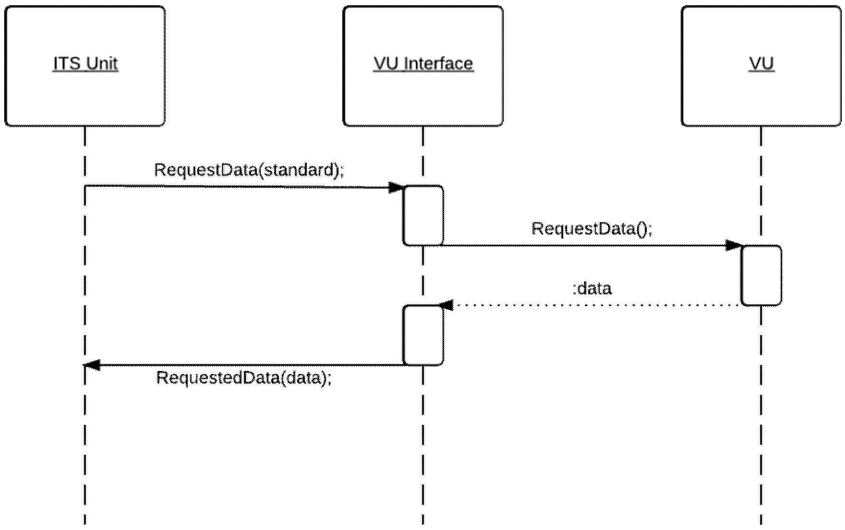
Obrázek 2

Schéma logické posloupnosti ověření autorizace jednotky ITS



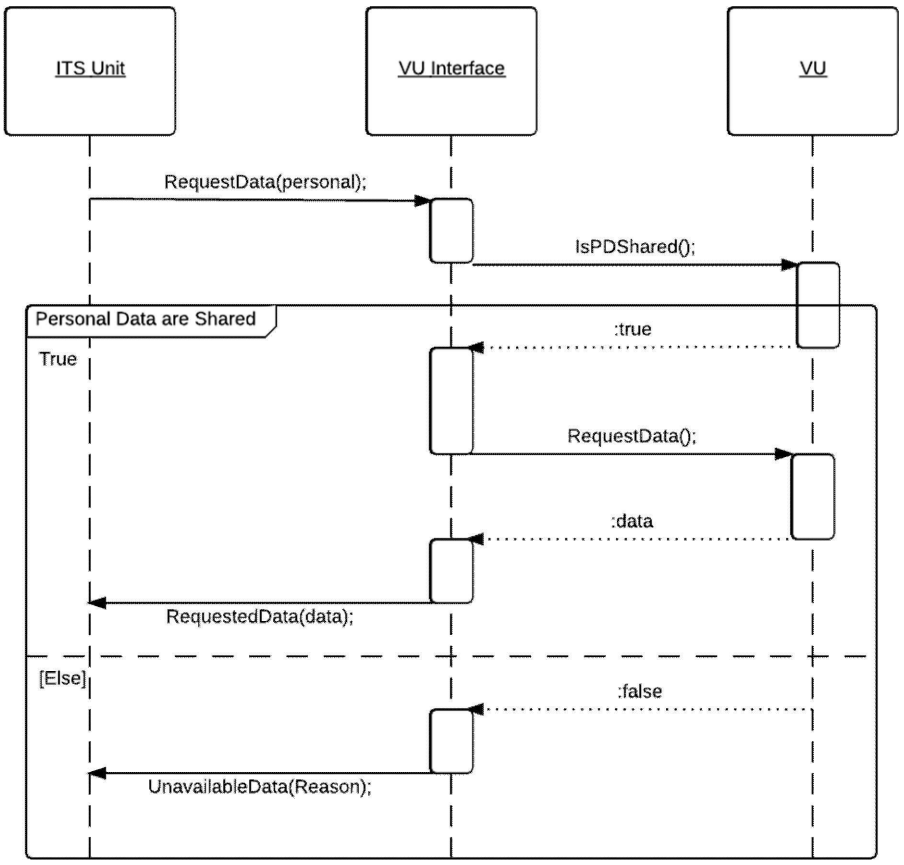
Obrázek 3

Schéma logické posloupnosti zpracování požadavku na údaje klasifikované jako neosobní (po zadání správného kódu PIN)



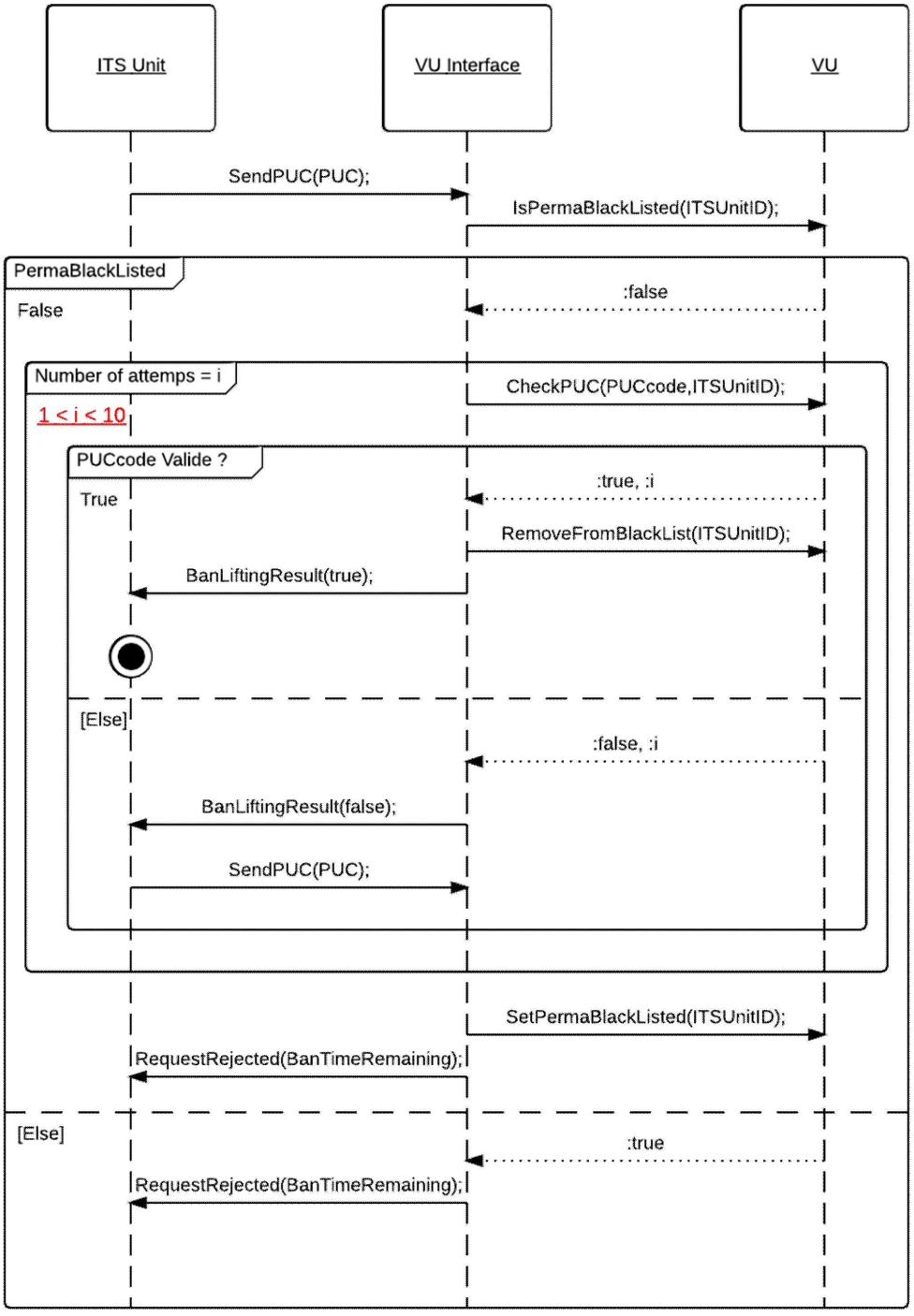
Obrázek 4

Schéma logické posloupnosti zpracování požadavku na údaje klasifikované jako osobní (po zadání správného kódu PIN)



Obrázek 5

Schéma logické posloupnosti pokusu o ověření PUC



PŘÍLOHA 3

SPECIFIKACE V NOTACI ASN.1

```
FormatMessageModule DEFINITIONS AUTOMATIC TAGS ::= BEGIN
EXPORTS ;
IMPORTS SendPIN, SendPUC, PairingResult, RequestPIN, RequestRejected,
        BanLiftingResult FROM PINPUCDataFieldsModule
        RequestAccepted,RequestData, DataUnavailable FROM
        RequestDataFieldsModule
        SendITSID, NegativeAnswer FROM OtherDataFieldsModule;

      CompleteMessage ::=SEQUENCE{
            header Header,
            data DataField,
            checksum Checksum
      }

      ----------------
      --HEADER TYPES--
      ----------------


      Header::=SEQUENCE{
            tgt IDList,
            src IDList,
            len BIT STRING (1..255)
      }

      vuID BIT STRING ::= 'EE'H
      IDList ::=CHOICE{
            vu BIT STRING (vuID),
            itsUnits SEQUENCE OF BIT STRING,
                  --Default hex Value:A0, redefined after first message exchange--
                  --Each ID will be linked to the Bluetooth ID of the device--
            ...
      }

      --------------------
      --DATAFIELDS TYPES--
      --------------------
      DataField ::=SEQUENCE{
            sid BIT STRING,
            trtp BIT STRING,
            subMBytes SubMessageBytes,
            dataField Content,
            ...
      }

      SubMessageBytes ::= SEQUENCE{
            currentSubM BIT STRING,
            totalSubM BIT STRING
      }

      Content ::= CHOICE{
            requestPIN RequestPIN,
            sendITSID SendITSID,
            sendPin SendPIN,
```

```
55                pairRslt PairingResult,
56                sendPUC SendPUC,
57                banlift BanLiftingResult,
58                requestRejected RequestRejected,
59                requestData RequestData,
60                requestOK RequestAccepted,
61                dataUnavailable DataUnavailable,
62                negAns NegativeAnswer
63          }
64
65          ------------------
66          --CHECKSUM TYPES--
67          ------------------
68
69          Checksum ::= SEQUENCE{
70                --SHA2 checksum
71          }
72    END
73
```

```
PINPUCDataFieldsModule DEFINITIONS AUTOMATIC TAGS ::= BEGIN
EXPORTS SendPIN, SendPUC, PairingResult, RequestPIN, RequestRejected,
BanLiftingResult;
IMPORTS ;

	----------
	---Utils--
	----------

	PUC ::= SEQUENCE (SIZE(8)) OF
	INTEGER (SIZE(0..9))

	PIN ::=	SEQUENCE (SIZE(4)) OF
		INTEGER (SIZE(0..9))

	--------------------------
	--Messages From ITS Unit--
	--------------------------

	SendPIN {PIN:pin} ::= SEQUENCE {
		sid BIT STRING ('03'H),
		pin PIN (pin)
	}

	SendPUC {PUC:puc} ::= SEQUENCE {
		sid BIT STRING ('05'H),
		puc PUC (puc)
	}
	--------------------
	--Messages From VU--
	--------------------

	PairingResult ::= SEQUENCE{
		sid BIT STRING ('04'H),
		result BOOLEAN
	}

	RequestPIN {MType:receivedRequest}::= SEQUENCE{
		sid BIT STRING ('01'H)
	}

	RequestRejected ::= SEQUENCE{
		sid BIT STRING ('07'H),
		banTimeRemaining GeneralizedTime, --PermaBan == 1k years-- }

	BanLiftingResult ::= SEQUENCE{
		sid BIT STRING ('06'H),
		result BOOLEAN
	}
END
```

```
RequestDataFields DEFINITIONS AUTOMATIC TAGS ::= BEGIN
	EXPORTS RequestAccepted,RequestData, DataUnavailable ;
	IMPORTS StandardEvent, PersonalEvent, StandardFault FROM EventsModule;

	------------------
	---From ITS Unit--
	------------------
	RequestData ::= SEQUENCE{
		sid BIT STRING ('08'H),
		requestedData DataTypeCode,
		...
	}

	-----------
	--From VU--
	-----------
	RequestAccepted ::=SEQUENCE{
		sid BIT STRING ('09'H),
		trtp DataTypeCode,
		dataSheet CHOICE{
			standardData StandardTachDataContent,
			personalData PersonalTachDataContent,
			gnss GNSSDataContent,
			standardEvent StandardEventContent,
			personalEvent PersonalEventContent,
			standardFault StandardFaultContent,
			manufacturerdata ManufacturerDataContent,
			...
		}
	}

	DataTypeCode ::=CHOICE{
		standardTachData BIT STRING ('01'H),
		personalTachData BIT STRING ('02'H),
		gnssData BIT STRING ('03'H),
		standardEventData BIT STRING ('04'H),
		personalEventData BIT STRING ('05'H),
		standardFaultData BIT STRING ('06'H),
		manufacturerData BIT STRING ('07'H),
		...
	}

	DataUnavailable ::=SEQUENCE{
		sid BIT STRING ('0A'H),
		trtp DataTypeCode,
		reason UnavailableDataCodes
	}

	UnavailableDataCodes ::= CHOICE{
		noDataAvailable BIT STRING ('10'H),
		personalDataNotShared BIT STRING ('11'H),
		...
	}
	----------------------------
	--Complete Tachograph Data--
	----------------------------
	--The format of the data was taken from the ISO16844-7 norm, more information
available in this ISO document—

```

```
Time ::= SEQUENCE{
	seconds INTEGER (0..59.75), --increment: 0.25s--
	minutes INTEGER (0..59), --increment: 1min--
	hours INTEGER (0..23), --increment: 1h--
	day INTEGER (0.25.. 31.75), --increment: 0.25d--
	month INTEGER (1..12), --increment: 1month--
	year INTEGER (1985..2235), --increment: 1year--
	locMinOffset INTEGER (-59..59), --increment: 1min--
	locHouroffset INTEGER (-23..23)--increment: 1h--
}

Date ::= SEQUENCE{
	month INTEGER (1..12), --increment: 1month--
	day INTEGER (0.25.. 31.75), --increment: 0.25d--
	year INTEGER (1985..2235) --increment: 1year--
}

DriverName ::=SEQUENCE{
	codePageSurname UTF8String, --See ISO/IEC 8859--
	surname UTF8String,
	codePageFirstname UTF8String, --See ISO/IEC 8859--
	firstname UTF8String,
}

--------------------
--Message Content--
--------------------

StandardTachDataContent ::= SEQUENCE{
	trtp DataTypeCode (DataTypeCode.&standardTachData),
	personal BOOLEAN (FALSE),
	data StandardTachyDataSheet,
}

PersonalTachDataContent ::= SEQUENCE{
	trtp DataTypeCode (DataTypeCode.&personalTachData),
	personal BOOLEAN (TRUE),
	data PersonalTachyDataSheet
}

GNSSDataContent ::= SEQUENCE{
	trtp DataTypeCode (DataTypeCode.&gnssData),
	personal BOOLEAN (TRUE),
	data GNSSDataSheet
}

StandardEventContent ::= SEQUENCE{
	trtp DataTypeCode (DataTypeCode.&standardEventData),
	personal BOOLEAN (FALSE),
	data StandardEventDataSheet
}

PersonalEventContent ::= SEQUENCE{
	trtp DataTypeCode (DataTypeCode.&personalEventData),
	personal BOOLEAN (TRUE),
	data PersonalEventDataSheet
}

StandardFaultContent ::= SEQUENCE{
```

```
243                 trtp DataTypeCode (DataTypeCode.&standardFaultData),
244                 personal BOOLEAN (FALSE),
245                 data StandardFault
246           }
247
248           ManufacturerDataContent ::= SEQUENCE{
249                 trtp DataTypeCode (DataTypeCode.&manufacturerData),
250                 personal BOOLEAN (TRUE),
251                 ...
252           }
253
254           ---------------
255           --DATA SHEETS--
256           ---------------
257
258           --Data sheet format follows ISO 16844-7.--
259           StandardTachyDataSheet ::= SEQUENCE{
260                 vin UTF8String (SIZE(17)),
261                 calibrationDate Date,
262                 driveRecognize INTEGER (2 UNION 12),
263                 driverCardDriver1 INTEGER (2 UNION 12),
264                 driverCardDriver2 INTEGER (2 UNION 12),
265                 timeDate Time,
266                 highResolutionTotalVehicleDistance INTEGER (0..21055406), --increment:
267     5m--
268                 serviceComponentIdentification INTEGER (0..255),
269                 serviceDelayCalendarTimeBased INTEGER (-125..125), --increment: 1week-
270     -
271                 nextCalibrationDate Date,
272                 speedAuthorised INTEGER (0..250.996), --increment 1/256km/h--
273                 tachographCardSlot1 INTEGER (0..4...), --Maximum 250--
274                 tachographCardSlot2 INTEGER (0..4...), --Maximum 250--
275                 outOfScopeCondition INTEGER(2 UNION 12),
276                 modeOfOperation INTEGER (0..4...), --Maximum 250--
277                 registeringMemberState UTF8String,
278           vehicleRegistrationNumber SEQUENCE {
279                       codePageVRN INTEGER (0..255),
280                       vrn OCTET STRING (SIZE(13)),
281                 },
282                 tachographNextMandatoryDownloadDate Date,
283                 ...
284           }
285
286           PersonalTachyDataSheet ::= SEQUENCE{
287                 tachographVehicleSpeed INTEGER (0..250.996), --increment 1/256km/h--
288                 driver1WorkingState INTEGER (2 UNION 12 UNION 102 UNION 112 UNION 1002
289     UNION 1012...),
290                 driver2WorkingState INTEGER (2 UNION 12 UNION 102 UNION 112 UNION 1002
291     UNION 1012...),
292
293                 driver1TimeRelatedStates INTEGER(2 UNION 12 UNION 102 UNION 112 UNION
294     1002 UNION
295                                                   1012 UNION 1102 UNION 1112 UNION
296     10002 UNION 10012 UNION
297                                                   10102 UNION 10112 UNION 11002 UNION
298     11012...),
299                 driver2TimeRelatedStates INTEGER(2 UNION 12 UNION 102 UNION 112 UNION
300     1002 UNION
```

```
                                                    1012 UNION 1102 UNION 1112 UNION
10002 UNION 10012 UNION
                                                    10102 UNION 10112 UNION 11002 UNION
11012...),

             overSpeed INTEGER (2 UNION 12),
             driver1Identification INTEGER (SIZE(19)), --TODO NEED FURTHER SPECS
FROM TACHO REGULATION--
             driver2Identification INTEGER (SIZE(19)), --TODO NEED FURTHER SPECS
FROM TACHO REGULATION--
             driver1ContinuousDrivingTime INTEGER (0.. 64255), --increment: 1min--
             driver2ContinuousDrivingTime INTEGER (0.. 64255), --increment: 1min--
             driver1CurrentDurationOfSelectedActivity INTEGER (0.. 64255), --
increment: 1min--
             driver2CurrentDurationOfSelectedActivity INTEGER (0.. 64255), --
increment: 1min--
             driver1Name DriverName,
             driver2Name DriverName,
             driver1CumulatedDrivingTimePreviousAndCurrentWeek INTEGER (0.. 64255),
--increment: 1min--
             driver2CumulatedDrivingTimePreviousAndCurrentWeek INTEGER (0.. 64255),
--increment: 1min--
             engineSpeed INTEGER(0..8031.875), --increment: 0,125r/min--
             driver1EndOfLastDailyRestPeriod Time,
             driver2EndOfLastDailyRestPeriod Time,
             driver1EndOfLastWeeklyRestPeriod Time,
             driver2EndOfLastWeeklyRestPeriod Time,
             driver1EndOfSecondLastWeeklyRestPeriod Time,
             driver2EndOfSecondLastWeeklyRestPeriod Time,
             driver1CurrentDailyDrivingTime INTEGER (0.. 64255), --increment: 1min-
-
             driver2CurrentDailyDrivingTime INTEGER (0.. 64255), --increment: 1min-
-
             driver1CurrentWeeklyDrivingTime INTEGER (0.. 64255), --increment:
1min--
             driver2CurrentWeeklyDrivingTime INTEGER (0.. 64255), --increment:
1min--
             driver1TimeLeftUntilNewDailyRestPeriod INTEGER (0.. 64255), --
increment: 1min--
             driver2TimeLeftUntilNewDailyRestPeriod INTEGER (0.. 64255), --
increment: 1min--
             driver1CardExpiryDate Date,
             driver2CardExpiryDate Date,
             driver1CardNextMandatoryDownloadDate Date,
             driver2CardNextMandatoryDownloadDate Date,
             driver1TimeLeftUntilNewWeeklyRestPeriod INTEGER (0.. 64255), --
increment: 1min--
             driver2TimeLeftUntilNewWeeklyRestPeriod INTEGER (0.. 64255), --
increment: 1min--
             driver1NumberOfTimes9hDailyDrivingTimesExceeded INTEGER (0..13),
             driver2NumberOfTimes9hDailyDrivingTimesExceeced INTEGER (0..13),
             driver1CumulativeUninterruptedRestTime INTEGER (0.. 64255), --
increment: 1min--
             driver2CumulativeUninterruptedRestTime INTEGER (0.. 64255), --
increment: 1min--
             driver1MinimumDailyRest INTEGER (0.. 64255), --increment: 1min--
             driver2MinimumDailyRest INTEGER (0.. 64255), --increment: 1min--
             driver1MinimumWeeklyRest INTEGER (0.. 64255), --increment: 1min--
             driver2MinimumWeeklyRest INTEGER (0.. 64255), --increment: 1min--
```

```
360                driver1MaximumDailyPeriod INTEGER (0..250), --increment: 1h--
361                driver2MaximumDailyPeriod INTEGER (0..250), --increment: 1h--
362                driver1MaximumDailyDrivingTime INTEGER (910 UNION 1010),
363                driver2MaximumDailyDrivingTime INTEGER (910 UNION 1010),
364                driver1NumberOfUsedReducedDailyRestPeriods INTEGER (0..13),
365                driver2NumberOfUsedReducedDailyRestPeriods INTEGER (0..13),
366                driver1RemainingCurrentDrivingTime INTEGER (0.. 64255), --increment:
367   1min--
368                driver2RemainingCurrentDrivingTime INTEGER (0.. 64255), --increment:
369   1min--
370                ...
371          }
372
373          GNSSDataSheet ::=  SEQUENCE {
374          gnssPosition GeoCoordinates
375                --See Appendix 1 for definition of GeoCoordinates--
376          }
377
378          StandardEventDataSheet ::= SEQUENCE{
379                events SEQUENCE OF StandardEvent
380          }
381
382          PersonalEventDataSheet ::= SEQUENCE{
383                events SEQUENCE OF PersonalEvent
384          }
385   END
386
387   EventsModule DEFINITIONS AUTOMATIC TAGS ::= BEGIN
388          EXPORTS ALL;
389          IMPORTS NationAlpha FROM Appendix1; --See Appendix 1 for more information
390   about NationAlpha--
391
392                SecurityBreachEvent ::=SEQUENCE{
393                      --See Annex 1B for more information--
394                }
395
396                RecordingEquipmentFaultType ::= SEQUENCE{
397                      --See Annex 1B for more information--
398                }
399
400                StandardEvent::= CHOICE{
401                      insertionInvalidCard InsertionOfANonValidCard,
402                      cardConflict CardConflict,
403                      timeOverlap TimeOverlap,
404                      previousSessionNotClosed LastCardSessionNotCorrectlyClosed,
405                      overSpeeding OverSpeeding,
406                      powerSupplyInterruption PowerSupplyInterruption,
407                      comErrorWithRemoteFacility
408   CommunicationErrorWithTheRemoteCommunicationFacility,
409                      absenceGNSSPosition
410   AbsenceOfPositionInformationFromGNSSReceiver,
411                      positionDataError PositionDataError,
412                      motionDataError MotionDataError,
413                      vehicleMotionConflict VehicleMotionConflict,
414                      securityBreachAttempt SecurityBreachAttempt,
415                      timeConflict TimeConflict,
416                      ...
417                }
418
```

```
PersonalEvent ::= CHOICE{
	lackOfAppropriateCard DrivingWithoutAnAppropriateCard,
	cardInsertionWhileDriving CardInsertionWhileDriving,
	overSpeeding OverSpeeding,
	...
}

StandardFault ::= CHOICE{
	cardFault CardFault,
	recordingEquipementFault RecordingEquipmentFault,
...
}

---------------
--EVENTS LIST--
---------------

InsertionOfANonValidCard::=SEQUENCE{
	beginDate GeneralizedTime,
	endDate GeneralizedTime,
	carsdType SEQUENCE OF UTF8String,
	cardsNumber SEQUENCE OF INTEGER,
	issuingMemberState SEQUENCE OF NationAlpha,
	cardsGeneration SEQUENCE OF INTEGER
}

CardConflict ::= SEQUENCE{
	beginDate GeneralizedTime,
	endDate GeneralizedTime,
	carsdType SEQUENCE OF UTF8String,
	cardsNumber SEQUENCE OF INTEGER,
	issuingMemberState SEQUENCE OF NationAlpha,
	cardsGeneration SEQUENCE OF INTEGER
}

TimeOverlap ::=SEQUENCE{
	beginDate GeneralizedTime,
	endDate GeneralizedTime,
	carsdType SEQUENCE OF UTF8String,
	cardsNumber SEQUENCE OF INTEGER,
	issuingMemberState SEQUENCE OF NationAlpha,
	cardsGeneration SEQUENCE OF INTEGER,
	numberSimilarEvent INTEGER
}

DrivingWithoutAnAppropriateCard ::= SEQUENCE{
	beginDate GeneralizedTime,
	endDate GeneralizedTime,
	carsdType SEQUENCE OF UTF8String,
	cardsNumber SEQUENCE OF INTEGER,
	issuingMemberState SEQUENCE OF NationAlpha,
	cardsGeneration SEQUENCE OF INTEGER,
	numberOfSimilarEvent INTEGER
}

CardInsertionWhileDriving ::= SEQUENCE{
	date GeneralizedTime,
	carsdType SEQUENCE OF UTF8String,
	cardsNumber SEQUENCE OF INTEGER,
```

```
478                     issuingMemberState SEQUENCE OF NationAlpha,
479                     numberOfSimilarEvents INTEGER
480             }
481
482             LastCardSessionNotCorrectlyClosed ::=SEQUENCE{
483                     beginDate GeneralizedTime,
484                     endDate GeneralizedTime,
485                     carsdType SEQUENCE OF UTF8String,
486                     cardsNumber SEQUENCE OF INTEGER,
487                     issuingMemberState SEQUENCE OF NationAlpha,
488                     cardsGeneration SEQUENCE OF INTEGER,
489                     oldSession SEQUENCE{
490                             beginDate GeneralizedTime,
491                             endDate GeneralizedTime,
492                             vrn UTF8String,
493                             issuingMemberState NationAlpha,
494                             cardsGeneration INTEGER,
495                     }
496             }
497
498             OverSpeeding ::=SEQUENCE{
499                     beginDate GeneralizedTime,
500                     endDate GeneralizedTime,
501                     maximumSpeed INTEGER,
502                     averageSpeed INTEGER,
503                     cardType UTF8String,
504                     cardNumber INTEGER,
505                     issuingMemberState NationAlpha,
506                     cardGeneration INTEGER,
507                     numberOfSimilarEvents INTEGER
508             }
509
510             PowerSupplyInterruption ::=SEQUENCE{
511                     beginDate GeneralizedTime,
512                     endDate GeneralizedTime,
513                     carsdType SEQUENCE OF UTF8String,
514                     cardsNumber SEQUENCE OF INTEGER,
515                     issuingMemberState SEQUENCE OF NationAlpha,
516                     cardsGeneration SEQUENCE OF INTEGER,
517                     numberOfSimilarEvent INTEGER
518             }
519
520             CommunicationErrorWithTheRemoteCommunicationFacility ::=SEQUENCE{
521                     beginDate GeneralizedTime,
522                     endDate GeneralizedTime,
523                     carsdType SEQUENCE OF UTF8String,
524                     cardsNumber SEQUENCE OF INTEGER,
525                     issuingMemberState SEQUENCE OF NationAlpha,
526                     cardsGeneration SEQUENCE OF INTEGER,
527                     numberOfSimilarEvent INTEGER
528             }
529
530             AbsenceOfPositionInformationFromGNSSReceiver ::= SEQUENCE{
531                     beginDate GeneralizedTime,
532                     endDate GeneralizedTime,
533                     carsdType SEQUENCE OF UTF8String,
534                     cardsNumber SEQUENCE OF INTEGER,
535                     issuingMemberState SEQUENCE OF NationAlpha,
536                     cardsGeneration SEQUENCE OF INTEGER,
```

```
537                 numberOfSimilarEvent INTEGER
538           }
539
540           PositionDataError ::= SEQUENCE{
541                 beginDate GeneralizedTime,
542                 endDate GeneralizedTime,
543                 carsdType SEQUENCE OF UTF8String,
544                 cardsNumber SEQUENCE OF INTEGER,
545                 issuingMemberState SEQUENCE OF NationAlpha,
546                 cardsGeneration SEQUENCE OF INTEGER,
547                 numberOfSimilarEvent INTEGER
548           }
549
550           MotionDataError ::= SEQUENCE{
551                 beginDate GeneralizedTime,
552                 endDate GeneralizedTime,
553                 carsdType SEQUENCE OF UTF8String,
554                 cardsNumber SEQUENCE OF INTEGER,
555                 issuingMemberState SEQUENCE OF NationAlpha,
556                 cardsGeneration SEQUENCE OF INTEGER,
557                 numberOfSimilarEvent INTEGER
558           }
559
560           VehicleMotionConflict ::= SEQUENCE{
561                 beginDate GeneralizedTime,
562                 endDate GeneralizedTime,
563                 carsdType SEQUENCE OF UTF8String,
564                 cardsNumber SEQUENCE OF INTEGER,
565                 issuingMemberState SEQUENCE OF NationAlpha,
566                 cardsGeneration SEQUENCE OF INTEGER,
567                 numberOfSimilarEvent INTEGER
568           }
569
570           SecurityBreachAttempt ::= SEQUENCE{
571                 beginDate GeneralizedTime,
572                 endDate GeneralizedTime OPTIONAL,
573                 carsdType SEQUENCE OF UTF8String,
574                 cardsNumber SEQUENCE OF INTEGER,
575                 issuingMemberState SEQUENCE OF NationAlpha,
576                 numberOfSimilarEvent INTEGER,
577                 typeOfEvent SecurityBreachEvent
578           }
579
580
581           TimeConflict ::= SEQUENCE{
582                 beginDate GeneralizedTime,
583                 endDate GeneralizedTime,
584                 carsdType SEQUENCE OF UTF8String,
585                 cardsNumber SEQUENCE OF INTEGER,
586                 issuingMemberState SEQUENCE OF NationAlpha,
587                 cardsGeneration SEQUENCE OF INTEGER,
588                 numberOfSimilarEvent INTEGER
589           }
590
591           ---------------
592           --FAULTS LIST--
593           ---------------
594
595           CardFault ::= SEQUENCE{
```

```
596                     beginDate GeneralizedTime,
597                     endDate GeneralizedTime,
598                     carsdType SEQUENCE OF UTF8String,
599                     cardsNumber SEQUENCE OF INTEGER,
600                     issuingMemberState SEQUENCE OF NationAlpha,
601                     cardsGeneration SEQUENCE OF INTEGER,
602             }
603
604             RecordingEquipmentFault ::= SEQUENCE{
605                     beginDate GeneralizedTime,
606                     endDate GeneralizedTime,
607                     faultType RecordingEquipmentFaultType,
608                     carsdType SEQUENCE OF UTF8String,
609                     cardsNumber SEQUENCE OF INTEGER,
610                     issuingMemberState SEQUENCE OF NationAlpha,
611                     cardsGeneration SEQUENCE OF INTEGER,
612             }
613 END
```

Dodatek 14

FUNKCE DÁLKOVÉ KOMUNIKACE

OBSAH

1 ÚVOD

Tento dodatek specifikuje koncepci a postupy provádění funkce dálkové komunikace (dále jen komunikace) podle článku 9 nařízení (EU) č. 165/2014 (dále jen nařízení).

DSC_1 Nařízení (EU) č. 165/2014 stanoví, že tachograf musí být vybaven funkcí dálkové komunikace, která musí zástupcům příslušných kontrolních orgánů umožnit číst informace tachografu z projíždějících vozidel pomocí dálkového dotazovacího zařízení (čtecí komunikační zařízení včasného dálkového odhalování [REDCR]), konkrétně dotazovacího zařízení s bezdrátovým připojením pomocí rozhraní CEN 5,8 GHz vyhrazených komunikací krátkého dosahu (DSRC).

Je třeba zdůraznit, že tato funkce je určena pouze pro předběžné třídění, které identifikuje vozidla pro podrobnější kontrolu, a nenahrazuje formální kontrolní postup podle ustanovení nařízení (EU) č. 165/2014. Viz 9. bod odůvodnění v preambuli tohoto nařízení, kde se uvádí, že dálková komunikace mezi tachografem a kontrolními orgány pro účely silniční kontroly usnadňuje cílené silniční kontroly.

DSC_2 *Data* se vyměňují prostřednictvím *komunikace* s použitím bezdrátového přenosu DSRC 5,8 GHz odpovídajícího tomuto dodatku a testovaného na příslušné parametry normy EN 300 674-1, {Electromagnetic compatibility and Radio spectrum Matters (ERM); Road Transport and Traffic Telematics (RTTT); Dedicated Short Range Communication (DSRC) transmission equipment (500 kbit/s / 250 kbit/s) operating in the 5,8 GHz Industrial, Scientific and Medical (ISM) band; Part 1: General characteristics and test methods for Road Side Units (RSU) and On -Board Units (OBU)}.

DSC_3 *Komunikace* je prostřednictvím komunikačního zařízení navázána pouze v případě, že je zařízením příslušného kontrolního orgánu vyžádána pomocí radiokomunikačních prostředků splňujících požadavky (*čtečkou komunikačního zařízení včasného dálkového odhalování* (REDCR)).

DSC_4 Pro zajištění integrity musí být *data* zabezpečená.

DSC_5 Přístup ke sdělovaným *datům* mají pouze příslušné kontrolní orgány pověřené kontrolou porušování nařízení (ES) č. 561/2006 a nařízení (EU) č. 165/2014 a dílny, pokud je to nutné k ověření správného fungování tachografu.

DSC_6 *Data* vyměňovaná v průběhu *komunikace* se musí omezit na data nezbytně nutná pro účely cílených silničních kontrol vozidel s potenciálně zmanipulovaným či zneužitým tachografem.

DSC_7 Integrita a bezpečnost dat je zaručena zabezpečením *dat* v celku ve vozidle (VU) a předáváním pouze zabezpečených přenášených dat a bezpečnostních dat (viz 5.4.4) prostřednictvím bezdrátového zařízení dálkové komunikace 5,8 GHz DSRC, což znamená, že prostředky k porozumění datům předávaným *komunikací* a k ověření jejich pravosti mají pouze pověřené osoby příslušných kontrolních orgánů. Viz dodatek 11 Společné bezpečnostní mechanismy.

DSC_8 *Data* musí obsahovat časové razítko okamžiku poslední aktualizace.

DSC_9 Obsah bezpečnostních dat je zpřístupněn pouze příslušným kontrolním orgánům a pod jejich kontrolou a stranám, se kterými sdílejí tyto informace, a je mimo rámec opatření *komunikace*, která je předmětem tohoto dodatku, kromě případů, kdy tato *komunikace* s každým balíčkem přenášených dat zajišťuje přenos balíčku bezpečnostních dat.

DSC_10 Stejnou architekturu a zařízení podle tohoto dodatku musí být možné používat pro získávání dalších datových koncepcí (např. vážení na palubě).

DSC_11 Je třeba zdůraznit, že v souladu s ustanoveními nařízení (EU) č. 165/2014 (článek 7) nesmějí být prostřednictvím *komunikace* sdělovány údaje týkající se totožnosti řidiče.

2 ROZSAH

Rozsah tohoto dodatku je omezen na stanovení podmínek, za jakých zástupci příslušných kontrolních orgánů používají specifikovanou bezdrátovou komunikaci 5,8 GHz DSRC pro získávání údajů (*dat*) na dálku ze zaměřeného vozidla, která ukazují, že zaměřené vozidlo potenciálně porušuje nařízení (EU) č. 165/2014 a měla by být zvážena možnost jeho zastavení pro další šetření.

Nařízení (EU) č. 165/2014 požaduje, aby se shromažďovaná data omezovala pouze na údaje nebo se týkala údajů, které identifikují potenciální přestupek, jak je uvedeno v článku 9 nařízení (EU) č. 165/2014.

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.

Tento dodatek specifikuje:

— Komunikační zařízení, postupy a protokoly používané pro *komunikaci*

— Normy a předpisy, které musí rádiové zařízení splňovat

— Předkládání *dat komunikačnímu* zařízení

— Dotazovací a stahovací postupy a posloupnost operací

— *Data* k přenosu

— Potenciální výklad *dat* přenášených při *komunikaci*

— Poskytování bezpečnostních dat v souvislosti s *komunikací*

— Dostupnost *dat* příslušným kontrolním orgánům

— Jak může *čtečka komunikačního zařízení včasného dálkového odhalování* požadovat různé druhy dat týkajících se nákladu a vozového parku

Pro upřesnění, tento dodatek nestanoví:

— Postup a řízení sběru *dat* v celku ve vozidle (které jsou funkcí konstrukce výrobku, pokud nejsou stanoveny jinde v nařízení (EU) č. 165/2014)

— Formu poskytování získaných dat zástupci příslušného kontrolního orgánu ani kritéria, která příslušné kontrolní orgány používají při rozhodování o tom, jaká vozidla mají zastavit (která jsou funkcí konstrukce výrobku, pokud nejsou stanovena jinde v nařízení (EU) č. 165/2014 nebo politickým rozhodnutím příslušných kontrolních orgánů). Je třeba zdůraznit, že *komunikace* pouze poskytuje *data* příslušným kontrolním orgánům, aby tyto orgány mohly provádět informovaná rozhodnutí.

— Bezpečnostní podmínky dat (např. šifrování) týkající se obsahu *dat* (které jsou stanoveny v dodatku 11 – Společné bezpečnostní mechanismy.

— Podrobnosti jiných koncepcí dat než RTM, která lze získávat pomocí stejné architektury a zařízení.

— Podrobnosti chování a řízení mezi VU a DSRC-VU ani chování v rámci DSRC-VU (jiného než poskytování *dat* v případě vyžádání ze strany REDCR).

3 ZKRATKY, DEFINICE A ZNAČENÍ

V tomto dodatku se používají tyto specifické zkratky a definice:

Anténa	Elektrické zařízení, které přeměňuje elektrickou energii na rádiové vlny a opačně, používané ve spojení s rádiovým vysílačem nebo rádiovým přijímačem. Při vysílání rádiový vysílač předává na anténní svorky elektrický proud oscilující s určitou rádiovou frekvencí a anténa vyzařuje energii proudu ve formě elektromagnetického vlnění (rádiové vlny). Při přijímání anténa zachycuje určitou energii elektromagnetické vlny a vytváří na svých svorkách mírné napětí, které je předáváno přijímači, kde se zesiluje.
Komunikace	Výměna informací/dat mezi DSRC-REDCR a DSRC-VU podle části 5 na základě vztahu hlavní jednotka – vedlejší jednotka za účelem získání dat.
Data	Zabezpečená data definovaného formátu (viz 5.4.4) požadovaná ze strany *DSRC-REDCR* a poskytovaná *DSRC-REDCR* celkem ve vozidle *DSRC-VU* prostřednictvím spojení 5,8 GHz DSRC podle bodu 5 níže.
Nařízení (EU) č. 165/2014	Nařízení Evropského parlamentu a Rady (EU) č. 165/2014 ze dne 4. února 2014 o tachografech v silniční dopravě, o zrušení nařízení Rady (EHS) č. 3821/85 o záznamovém zařízení v silniční dopravě a o změně nařízení Evropského parlamentu a Rady (ES) č. 561/2006 o harmonizaci některých předpisů v sociální oblasti týkajících se silniční dopravy
AID	identifikátor aplikace
BLE	bluetooth s nízkou energií
BST	servisní tabulka signálů

CIWD	vložení karty během řízení
CRC	kontrola cyklickým kódem
DSC (n)	identifikátor požadavku na specifický dodatek DSRC
DSRC	vyhrazené spojení krátkého dosahu
DSRC-REDCR	čtečka komunikačního zařízení včasného dálkového odhalování DSRC
DSRC-VU	celek ve vozidle DSRC. Toto je „zařízení včasného dálkového odhalování“ definované v příloze 1C.
DWVC	jízda bez platné karty
EID	identifikátor prvku
LLC	kontrola logického spojení
LPDU	datová jednotka protokolu LLC
OWS	palubní vážicí systém
PDU	datová jednotka protokolu
REDCR	čtečka komunikačního zařízení včasného dálkového odhalování Toto je „čtečka komunikačního zařízení včasného dálkového odhalování“ definované v příloze 1C.
RTM	dálkové sledování tachografů
SM-REDCR	bezpečnostní modul – čtečka komunikačního zařízení včasného dálkového odhalování
TARV	telematické aplikace pro regulovaná vozidla (řada norem ISO 15638)
VU	celek ve vozidle
VUPM	paměť přenášených dat celku ve vozidle
VUSM	bezpečnostní modul celku ve vozidle
VST	servisní tabulka vozidla
WIM	vážení za jízdy
WOB	vážení na palubě

Specifikace definovaná v tomto dodatku odkazuje na všechny následující předpisy a normy nebo jejich části a je na nich závislá. V rámci ustanovení tohoto dodatku jsou specifikovány příslušné normy nebo příslušná ustanovení norem. V případě jakýchkoli rozporů mají přednost ustanovení tohoto dodatku. V případě jakýchkoli rozporů, k nimž se tento dodatek jasně nevyjadřuje, má přednost postup podle ERC 70-03 (s kontrolou příslušných parametrů EN 300 674-1), v sestupném pořadí důležitosti podle EN 12795, EN 12253 EN 12834 a EN 13372, 6.2, 6.3, 6.4 a 7.1.

Předpisy a normy, na které odkazuje tento dodatek, jsou:

[1] Nařízení (EU) č. 165/2014 ze dne 4. února 2014 o tachografech v silniční dopravě, o zrušení nařízení Rady (EHS) č. 3821/85 o záznamovém zařízení v silniční dopravě a o změně nařízení Evropského parlamentu a Rady (ES) č. 561/2006 o harmonizaci některých předpisů v sociální oblasti týkajících se silniční dopravy.

[2] Nařízení Evropského parlamentu a Rady (ES) č. 561/2006 o harmonizaci některých předpisů v sociální oblasti týkajících se silniční dopravy, o změně nařízení Rady (EHS) č. 3821/85 a (ES) č. 2135/98 a o zrušení nařízení Rady (EHS) č. 3820/85 (Text s významem pro EHP).

[3] ERC 70-03 CEPT: ECC Recommendation 70-03: Relating to the Use of Short Range Devices (SRD)

[4] ISO 15638 Intelligent transport systems — Framework for cooperative telematics applications for regulated commercial freight vehicles (TARV).

[5] EN 300 674-1 Electromagnetic compatibility and Radio spectrum Matters (ERM); Road Transport and Traffic Telematics (RTTT); Dedicated Short Range Communication (DSRC) transmission equipment (500 kbit/s / 250 kbit/s) operating in the 5,8 GHz Industrial, Scientific and Medical (ISM) band; Part 1: General characteristics and test methods for Road Side Units (RSU) and On-Board Units (OBU).

[6] EN 12253 Road transport and traffic telematics – Dedicated short-range communication – Physical layer using microwave at 5.8 GHz.

[7] EN 12795 Road transport and traffic telematics – Dedicated short-range communication – Data link layer: medium access and logical link control.

[8] EN 12834 Road transport and traffic telematics – Dedicated short-range communication – Application layer.

[9] EN 13372 Road transport and traffic telematics – Dedicated short-range communication – Profiles for RTTT applications

[10] ISO 14906 Electronic fee collection — Application interface definition for dedicated short- range communication

4 OPERAČNÍ SCÉNÁŘE

4.1 **Přehled**

Nařízení (EU) č. 165/2014 stanoví specifické a kontrolované scénáře, v nichž má být *komunikace* používána.

Podporované scénáře:

„*Communication Profile 1: Roadside inspection using a short range wireless communication Remote Early Detection Communication Reader instigating a physical roadside inspection (master-:-slave)*

Reader Profile 1a: pomocí komunikačního zařízení včasného dálkového odhalování nasměrovaného ručně nebo dočasně namontovaného a nasměrovaného u silnice

Reader Profile 1b: via a vehicle mounted and directed Remote Early Detection Communication Reader“.

4.1.1 *Podmínky přenosu dat pomocí rozhraní 5,8 GHz DSRC*

POZNÁMKA: Pro znázornění příslušných souvislostí je komunikační zařízení zobrazeno na obrázku 14.3 níže.

4.1.1.1 Data uchovávaná ve VU

DSC_12 VU odpovídá za aktualizaci každých 60 sekund a uchovávání v něm uložených dat nezávisle na komunikační funkci DSRC. Způsob, jakým je tohoto cíle dosaženo, je vnitřní funkcí VU specifikovanou v nařízení (EU) č. 165/2014, příloze 1 C, bodě 3.19 „*Dálková komunikace pro cílené silniční kontroly*“ a není specifikován v tomto dodatku.

4.1.1.2 Data předávaná zařízení DSRC-VU

DSC_13 VU odpovídá za aktualizaci dat tachografu DSRC (*data*), kdykoli jsou data uložená ve VU aktualizována, v intervalu stanoveném v 4.1.1.1 (DSC_12) nezávisle na komunikační funkci DSRC.

DSC_14 Základem získávání a aktualizace dat jsou data VU, a způsob, jakým je toho dosaženo, je uveden v příloze 1 C bodě 3.19 „*Dálková komunikace pro cílené silniční kontroly*“, nebo pokud příslušné informace uvedeny nejsou, je funkcí konstrukce výrobku a není v tomto dodatku uveden. Způsob spojení mezi zařízením DSRC-VU a VU je uveden v části 5.6.

4.1.1.3 Obsah údajů

DSC_15 Obsah a formát *dat* musí být po dekódování strukturované a dostupné ve formě a formátu uvedeném v bodě 5.4.4 tohoto dodatku (Struktury dat).

4.1.1.4 Předkládání údajů

DSC_16 *Data*, která jsou často aktualizována v souladu s postupy podle bodu 4.1.1.1, musí být zajištěna před prezentací systému *DSRC-VU* a předložena jako hodnota zabezpečeného systému dat pro dočasné uložení v *DSRC-VU* jako aktuální verze *dat*. Tato *data* jsou přenesena z *VUSM* do DSRC funkce *VUPM*. *VUSM* a *VUPM* jsou funkce, a nikoli nutně fyzikální veličiny. Forma fyzické realizace pro provádění těchto funkcí je záležitostí návrhu výrobku, pokud nejsou uvedeny jinde v nařízení (EU) č. 165/2014.

4.1.1.5 Bezpečnostní data

DSC_17 Bezpečnostní data (*securityData*), obsahující údaje požadované *REDCR* pro účely dekódování dat, jsou poskytována v souladu s dodatkem 11 – Společné bezpečnostní mechanismy – a prezentována jako hodnota systému dat pro dočasné uložení v *DSRC-VU* jako aktuální verze *securityData* ve formě stanovené v tomto dodatku části 5.4.4.

4.1.1.6 Data VUPM určená k přenosu pomocí rozhraní DSRC

DSC_18 Systém dat, který musí být ve vždy dostupný ve funkci DSRC VUPM pro okamžitý přenos na požádání ze strany *REDCR*, je definován v části 5.4.4 pro úplné specifikace modulu ASN.1.

Obecný přehled komunikačního profilu 1

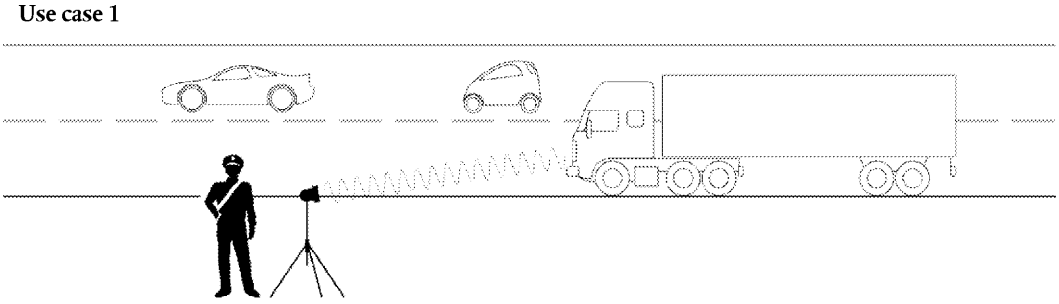
Tento profil se vztahuje na případ použití, kdy pověřená osoba příslušného kontrolního orgánu používá komunikační zařízení včasného dálkového odhalování s dálkovým spojením krátkého dosahu (rozhraní 5,8 GHz DSRC pracující v rozsahu ERC 70-03 a testované pro příslušné parametry EN 300 674-1, jak je popsáno v oddílu 5) (*REDCR*) pro dálkovou identifikaci vozidel, která potenciálně porušují nařízení (EU) č. 165/2014. Po této identifikaci pověřená osoba příslušného kontrolního orgánu, která kontroluje dotazování, rozhodne, zda má být vozidlo zastaveno.

4.1.2 *Profil 1a: pomocí čtečky komunikačního zařízení včasného dálkového odhalování nasměrovaného ručně nebo dočasně namontovaného a nasměrovaného u silnice*

V tomto případě použití se pověřená osoba příslušného kontrolního orgánu nachází na silnici a zaměřuje *REDCR* držené v ruce, namontované na stativu nebo jinak přenosné ze silnice do středu předního okna cíleného vozidla. Dotazování se provádí pomocí rozhraní 5,8 GHz DSRC pracujícího v rozsahu ERC 70-03 a testovaného pro příslušné parametry EN 300 674-1, jak je popsáno v oddílu 5. Viz obrázek 14.1 (případ použití 1).

Obrázek 14.1

Sledování ze silnice pomocí 5,8 GHz DSRC



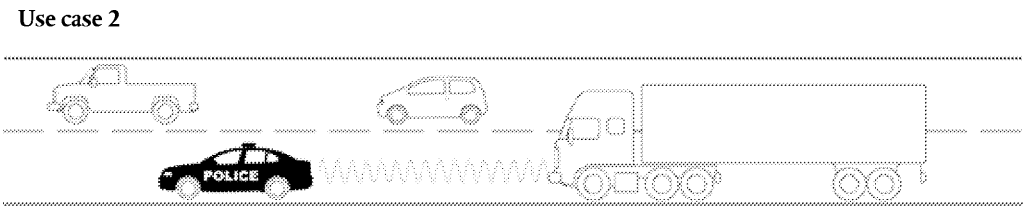
Silniční REDCR

4.1.3 *Profil 1b: pomocí čtečky komunikačního zařízení včasného dálkového odhalování namontovaného a nasměrovaného na vozidle*

V tomto případě použití se pověřená osoba příslušného kontrolního orgánu nachází v jedoucím vozidle, a buď zaměřuje přenosné *REDCR* držené v ruce z vozidla do středu předního skla cíleného vozidla, nebo je *REDCR* namontováno uvnitř vozidla nebo na něm tak, aby směřovalo do středu předního skla cíleného vozidla, je-li vozidlo s čtečkou komunikačního zařízení včasného dálkového odhalování v příslušné poloze vůči cílenému vozidlu (např. přímo před ním ve směru jízdy). Dotazování se provádí pomocí rozhraní 5,8 GHz DSRC pracujícího v rozsahu ERC 70-03 a testovaného pro příslušné parametry EN 300 674-1, jak je popsáno v oddílu 5. Viz obrázek 14.2. (Případ použití 2).

Obrázek 14.2

Sledování z vozidla pomocí 5,8 GHz DSRC



Mobilní REDCR

4.2 **Zabezpečení/integrita**

Aby bylo možné ověřovat pravost a integritu stahovaných dat pomocí dálkové komunikace, jsou zabezpečená *data* ověřována a dešifrována v souladu s dodatkem 11 – Společné bezpečnostní mechanismy.

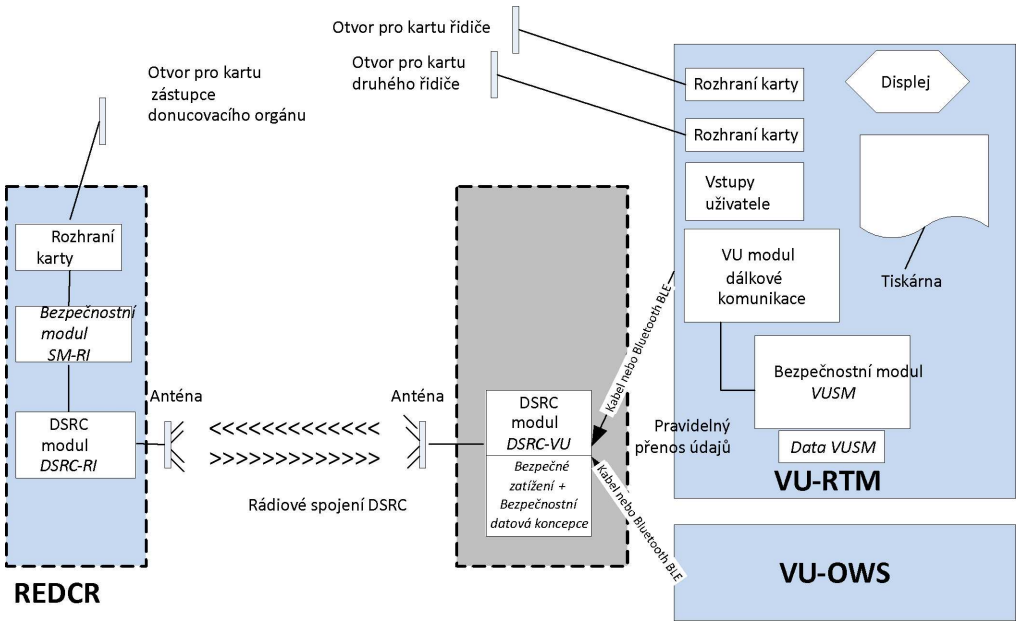
5 STRUKTURA A PROTOKOLY DÁLKOVÉ KOMUNIKACE

5.1 **Struktura**

Struktura funkce dálkové komunikace v inteligentním tachografu je znázorněna a popsána na obrázku 14.3.

Obrázek 14.3

Struktura funkce dálkové komunikace



DSC_19 Ve VU jsou umístěny tyto funkce:

— Bezpečnostní modul (*VUSM*). Tato funkce ve VU je odpovědná za zabezpečení *dat*, která mají být přenesena z *DSRC-VU* k pověřené osobě příslušného kontrolního orgánu prostřednictvím dálkové komunikace.

— Zabezpečená data jsou uložena v paměti VUSM. V intervalech stanovených v 4.1.1.1 (DSC_12) VU šifruje a doplňuje systém RTMdata (který obsahuje přenášená data a hodnoty zabezpečeného systému dat stanovené níže v tomto dodatku) uchovávaný v paměti DSRC-VU. Provoz bezpečnostního modulu je definován v dodatku 11– Společné bezpečnostní mechanismy – a mimo rozsah tohoto dodatku s výjimkou případů, kdy bude třeba poskytnout aktualizace komunikačnímu zařízení VU při každé změně dat VUSM.

— Komunikace mezi VU a DSRC-VU může být drátová komunikace nebo komunikace bluetooth s nízkým napětím (BLE) a fyzické umístění DSRC-VU může být totožné s anténou na čelním skle vozidla, může být vnitřní částí VU nebo jakékoli přechodné umístění.

— DSRC-VU musí mít trvalý spolehlivý zdroj napájení. Prostředky, kterými je toho dosaženo, jsou konstrukčním rozhodnutím.

— Paměť DSRC-VU musí být stálá, aby se data na DSRC-VU uchovala, i když je zapalování vozidla vypnuto.

— Je-li komunikace mezi VU a DSRC-VU realizována pomocí BLE a zdrojem energie je jednorázově použitelná baterie, musí být zdroj energie DSRC-VU vyměněn při každé pravidelné kontrole a výrobce zařízení DSRC-VU je odpovědný za to, aby byl tento zdroj energie dostatečný na dobu od jedné pravidelné kontroly k další a byl zajištěn normální přístup k datům prostřednictvím REDCR po celou tuto dobu bez výpadků nebo přerušení.

— Zařízení „paměti přenášených dat“ VU RTM (*VUPM*). Tato funkce ve VU je odpovědná za poskytování a aktualizaci *dat*. Obsah *dat*. Obsah dat („TachographPayload“) je definován v 5.4.4/5.4.5 níže a je aktualizován v intervalu stanoveném v bodě 4.1.1.1 (DSC_12).

— DSRC-VU. Tato funkce, která je umístěna v anténě nebo je s ní spojena a komunikuje s VU prostřednictvím drátového nebo bezdrátového (BLE) spojení, obsahuje aktuální data (*data VUPM*) a řídí odpovědi na dotazy v systému 5,8 GHz DSRC. Přerušení spojení nebo rušení s funkcí zařízení DSRC během normálního provozu vozidla je považováno za porušení nařízení (EU) č. 165/2014.

— Bezpečnostní modul (REDCR) (*SM-REDCR*) je funkce používaná pro dešifrování a kontrolu integrity dat z VU. Prostředky, kterými je toho dosaženo, jsou určeny v dodatku 11 – Společné bezpečnostní mechanismy a nejsou definovány v tomto dodatku.

— Funkce zařízení DSRC (REDCR) (*DSRC-REDCR*) zahrnuje přijímač-vysílač 5,8 GHz a příslušný firmware a software, který řídí *komunikaci* s *DSRC-VU* v souladu s tímto dodatkem.

— *DSRC-REDCR* sleduje *DSRC-VU* cíleného vozidla, získává *data* (aktuální *data VUPM* cíleného vozidla) prostřednictvím spojení DSRC a přijatá data zpracovává a ukládá ve svém *SM-REDCR*.

— Anténa DSRC-VU musí být umístěna v místě, ve kterém je optimální komunikace DSRC mezi vozidlem a silniční anténou (obecně uprostřed nebo poblíž středu předního okna vozidla …). U lehkých vozidel se umístí v horní části čelního skla.

— Před anténou nebo v její blízkosti nesmí být žádné kovové předměty (např. štítky se jménem, nálepky, fóliové antireflexní (tónovací) pásky, sluneční clony, stěrače v klidové poloze), které by mohly narušovat komunikaci.

— Anténa musí být namontována tak, aby její směr zaměření byl přibližně rovnoběžný s povrchem silnice.

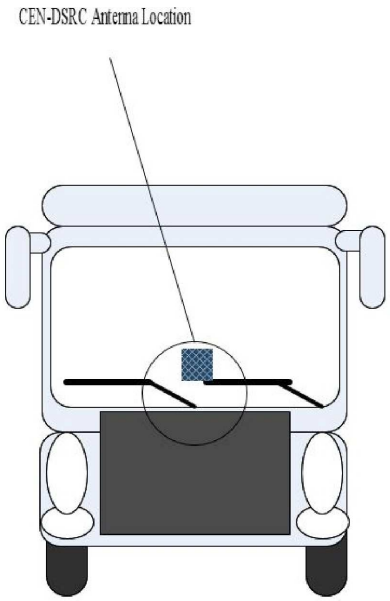
DSC_20 Anténa a komunikace musí pracovat v rámci ERC 70-03, musí být testovány pro příslušné parametry EN 300 674-1 jak je popsáno v oddíle 5. Anténa a komunikace mohou používat techniky zmírňování rizika rušení bezdrátové sítě, jak je popsáno ve zprávě ECC 228, například použitím filtrů při komunikaci CEN DSRC 5.8 GHz.

DSC_21 Anténa DSRC musí být spojena se zařízením DSRC-VU buď přímo v modulu namontovaném na čelním skle nebo v jeho blízkosti, nebo prostřednictvím vyhrazeného kabelu s konstrukcí, která ztěžuje nezákonné přerušení spojení. Přerušení spojení nebo rušení s funkcí antény je považováno za porušení nařízení (EU) č. 165/2014. Úmyslné zakrývání antény nebo jiná nežádoucí manipulace negativně ovlivňující její provozní výkon jsou považovány za porušení nařízení (EU) č. 165/2014.

DSC_22 Tvarový činitel antény není stanoven a je komerčním rozhodnutím, pokud namontované zařízení DSRC-VU splňuje požadavky shody podle části 5 níže. Anténa musí být umístěna podle pokynů DSC 19 a podle obrázku 14.4 (ovál) a účinně podporuje případy užití popsané v 4.1.2 a 4.1.3.

Obrázek 14.4

Příklad polohy antény 5,8 GHz DSRC na čelním skle regulovaných vozidel



Tvarový činitel *REDCR* a jeho anténa se mohou měnit podle podmínek čtečky (montáž na stativu, držení v ruce, montáž ve/na vozidle atd.) a pracovního postupu pověřené osoby příslušného kontrolního orgánu.

Funkce zobrazování a/nebo oznamování pověřené osobě příslušného kontrolního orgánu znázorňuje výsledky funkce dálkové komunikace. Informace se mohou zobrazovat na obrazovce, jako tištěný výstup, zvukový signál nebo kombinace těchto možností. Způsob tohoto zobrazování a/nebo oznamování závisí na požadavcích pověřených osob příslušných kontrolních orgánů a konstrukci zařízení a v tomto dodatku není stanoven.

DSC_23 Konstrukce a tvarový činitel *REDCR* jsou funkcí komerčního provedení, které pracuje v rámci ERC 70-03, a konstrukčních a výkonnostních specifikací stanovených v tomto dodatku (oddíl 5.3.2), čímž je trhu poskytnuta maximální pružnost v navrhování a dodávání zařízení, které odpovídá konkrétním scénářům dotazování příslušného kontrolního orgánu při provádění konkrétních sledovacích scénářů.

DSC_24 Konstrukce a tvarový činitel *DSRC-VU* a jeho umístění uvnitř nebo vně VU jsou funkcí komerčního provedení, které pracuje v rámci ERC 70-03, a konstrukčních a výkonnostních specifikací stanovených v tomto dodatku (oddíl 5.3.2) a v tomto bodě (5.1).

DSC_25 *DSRC-VU* však musí být přiměřeně schopno přijímat hodnoty systémů dat z jiných inteligentních zařízení ve vozidle prostřednictvím otevřeného průmyslového standardního spojení a protokolů (např. ze zařízení vážení na palubě), pokud jsou tyto systémy dat identifikovány jedinečnými a známými identifikátory aplikací/názvy souborů a instrukce k provozování těchto protokolů jsou dostupné Evropské komisi a bezplatně také výrobcům příslušného zařízení.

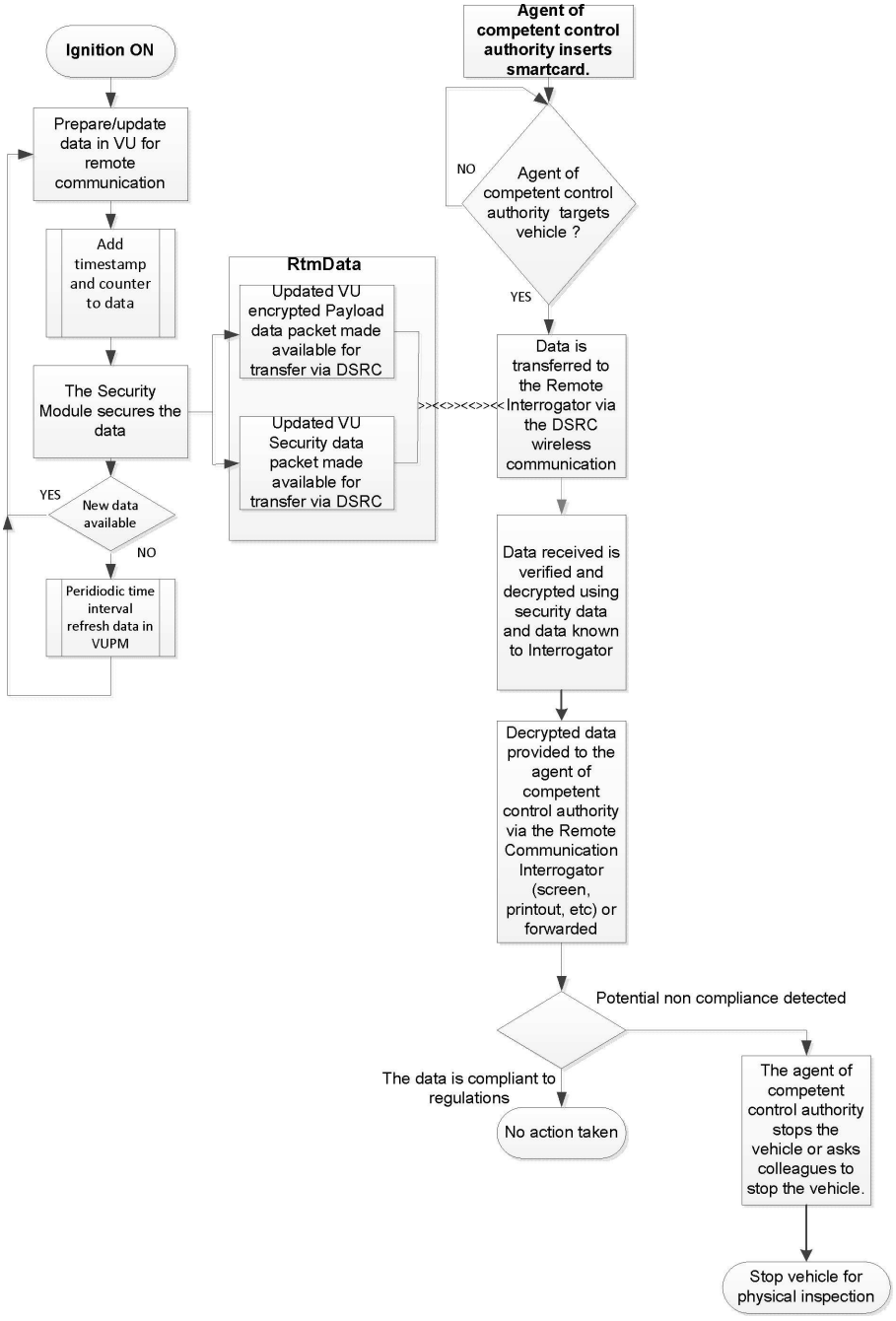
5.2 Vývojový diagram

5.2.1 *Činnosti*

Vývojový diagram činností je znázorněn na obrázku 14.5.

Obrázek 14.5

Vývojový diagram funkce dálkové komunikace



Kroky jsou popsány níže:

a. Kdykoli je vozidlo v provozu (zapnuté zapalování), tachograf předává data funkci VU. Funkce VU zpracovává *data* pro funkci dálkové komunikace (zašifrovaná) a aktualizuje *VUPM* v paměti *DSRC-VU* (jak je definováno v bodech 4.1.1.1–4.1.1.2). Získaná *data* jsou formátována, jak je uvedeno v bodech 5.4.4–5.4.5 níže.

b. Při každé příležitosti, kdy jsou *data* aktualizována, je rovněž aktualizováno časové razítko definované v zabezpečeném systému dat.

c. Funkce *VUSM* zabezpečuje data v souladu s postupy stanovenými v dodatku 11.

d. Při každé příležitosti, kdy jsou *data* aktualizována (viz 4.1.1.1–4.1.1.2), jsou přenesena do *DSRC-VU*, kde nahrazují všechna předchozí data, aby tato aktualizovaná *data* byla vždy k dispozici v případě komunikace s *REDCR*. Při předávání z VU do DSRC-VU jsou *data* označena názvem souboru *RTMData* nebo identifikátory ApplicationID a atributy.

e. Chce-li pověřená osoba příslušného kontrolního orgánu zaměřit vozidlo a získat z něj *data*, musí tato pověřená osoba příslušného kontrolního orgánu nejprve vložit do *REDCR* chytrou kartu, která dovoluje *komunikaci* a *SM-REDCR* umožňuje ověřit její pravost a dešifrovat data.

f. Pověřená osoba příslušného kontrolního orgánu potom zaměří vozidlo a pomocí dálkové komunikace si vyžádá data. *REDCR* otevře relaci rozhraní 5,8 GHz DSRC s *DSRC-VU* cíleného vozidla a vyžádá si *data*. *Data* jsou přenesena do *REDCR* prostřednictvím systému bezdrátové komunikace DSCR atribut používajícího službu aplikace GET, jak je stanoveno v oddíle 5.4. Atribut obsahuje šifrované hodnoty přenášených dat a zabezpečená data DSRC.

g. Data jsou zařízením *REDCR* analyzována a předána pověřené osobě příslušného kontrolního orgánu.

h. Pověřená osoba příslušného kontrolního orgánu použije data k tomu, aby rozhodla, zda má vozidlo zastavit k podrobné kontrole, či nikoli, nebo požádat jinou pověřenou osobu příslušného kontrolního orgánu o zastavení vozidla.

5.2.2 *Interpretace dat přijímaných prostřednictvím komunikace DSRC*

DSC_26 Data přijatá prostřednictvím rozhraní 5,8 GHz mají význam a smysl stanovený v bodech 5.4.4 a 5.4.5 níže a pouze takový význam a smysl a jsou chápána ve smyslu zde stanovených cílů. V souladu s ustanoveními nařízení (EU) č. 165/2014 musí být *data* používána pouze pro poskytování náležitých informací příslušnému kontrolnímu orgánu, aby mohl rozhodnout, zda má vozidlo zastavit pro účely fyzické kontroly, a následně zlikvidována v souladu s článkem 9 nařízení (EU) č. 165/2014.

5.3 **Parametry fyzického rozhraní DSRC pro dálkovou komunikaci**

5.3.1 *Omezení umístění*

DSC_27 Dálkové sledování vozidel prostřednictvím rozhraní 5,8 GHz DSRC by nemělo být používáno v rozsahu do 200 metrů od provozní brány 5,8 GHz DSRC.

5.3.2 *Parametry downlinku a uplinku*

DSC_28 Zařízení používané pro dálkové sledování tachografů musí odpovídat doporučení ERC 70-03 a parametrům stanoveným v tabulkách 14.1 a 14.2 níže a pracovat v jejich rozsahu.

DSC_29 Pro zajištění kompatibility s provozními parametry jiných standardních systémů 5,8 GHz DSRC musí dále zařízení používané pro dálkové sledování tachografů odpovídat parametrům EN 12253 a EN 13372.

Konkrétně:

Tabulka 14.1

Parametry downlinku

Item No.	Parameter	Value(s)	Remark
D1	Downlink Carrier Frequencies	There are four alternatives which may be used by an REDCR: 5.7975 GHz 5.8025 GHz 5.8075 GHz 5.8125 GHz	Within ERC 70-03. Carrier Frequencies may be selected by the implementer of the roadside system and need not be known in the DSRC-VU (Consistent with EN 12253, EN 13372)
D1a (*)	Tolerance of Carrier Frequencies	within ± 5 ππμ	(Consistent with EN 12253)
D2 (*)	RSU (REDCR) Transmitter Spectrum Mask	Within ERC 70-03. REDCR shall be according to Class B,C as defined in EN 12253. No other specific requirement within this Annex	Parameter used for controlling interference between interrogators in proximity (as defined in EN 12253 and EN 13372).
D3	OBU(DSRC-VU) Minimum Frequency Range	5.795 – 5.815 GHz	(Consistent with EN 12253)
D4 (*)	Maximum E.I.R.P.	Within ERC 70-03 (unlicensed) and within National Regulation Maximum +33 dBm	(Consistent with EN 12253)
D4a	Angular E.I.R.P. mask	According to declared and published specification of interrogator designer	(Consistent with EN 12253)
D5	Polarisation	Left hand circular	(Consistent with EN 12253)
D5a	Cross-Polarisation	XPD: In bore sight: (REDCR) RSU t ≥ 15 δB (DSRC-VU) OBU r ≥ 10 δB At -3 dB area: (REDCR) RSU t ≥ 10 δB (DSRC-VU) OBU r ≥ 6 δB	(Consistent with EN 12253)
D6 (*)	Modulation	Two level amplitude modulation.	(Consistent with EN 12253)
D6a (*)	Modulation Index	0,5 … 0,9	(Consistent with EN 12253)

Item No.	Parameter	Value(s)	Remark
D6b	Eye Pattern	≥ 90 % (time) / ≥ 85 % (amplitude)	
D7 (*)	Data Coding	FM0 „1“ bit has transitions only at the beginning and end of the bit interval. „0“ bit has an additional transition in the middle of the bit interval compared to the „1“ bit.	(Consistent with EN 12253)
D8 (*)	Bit rate	500 kBit/s	(Consistent with EN 12253)
D8a	Tolerance of Bit Clock	better than ± 100 ppm	(Consistent with EN 12253)
D9 (*)	Bit Error Rate (B.E.R.) for communication	≤ 10^{-6} when incident power at OBU (DSRC-VU) is in the range given by [D11a to D11b].	(Consistent with EN 12253)
D10	Wake-up trigger for OBU (DSRC-VU)	OBU (DSRC-VU) shall wake up on receiving any frame with 11 or more octets (including preamble)	No special wake-up pattern is necessary. DSRC-VU may wake up on receiving a frame with less than 11 octets (Consistent with EN 12253)
D10a	Maximum Start Time	≤ 5 ms	(Consistent with EN 12253)
D11	Communication zone	Spatial region within which a B.E.R. according to D9a is achieved	(Consistent with EN 12253)
D11a (*)	Power Limit for communication (upper).	– 24dBm	(Consistent with EN 12253)
D11b (*)	Power Limit for communication (lower).	Incident power: 43 dBm (boresight) 41 dBm (within – 45 ° – + 45° Corresponding to the plane parallel to the road surface when the DSRC-VU later is installed in the vehicle (Azimuth))	(Consistent with EN 12253) Extended requirement for horizontal angles up to ± 45 °, due to the use cases defined in this annex.
D12 (*)	Cut-off power level of (DSRC-VU)	– 60 dBm	(Consistent with EN 12253)
D13	Preamble	Preamble is mandatory.	(Consistent with EN 12253)
D13a	Preamble Length and Pattern	16 bits ± XXXXXXXXXXXXXXXX	(Consistent with EN 12253)

Item No.	Parameter	Value(s)	Remark
D13b	Preamble Wave form	An alternating sequence of low level and high level with pulse duration of 2 µs. The tolerance is given byD8a	(Consistent with EN 12253)
D13c	Trailing Bits	The RSU (REDCR) is permitted to transmit a maximum of 8 bits after the end flag. An OBU (DSRC-VU) is not required to take these additional bits into account.	(Consistent with EN 12253)

(*) – Downlink parameters subject to conformance testing in accordance with relevant parameter test from EN 300 674-1

Tabulka 14.2

Parametry uplinku

Item No.	Parameter	Value(s)	Remark
U1 (*)	Sub-carrier Frequencies	A OBU (DSRC-VU) shall support 1.5 MHz and 2.0 MHz An RSU (REDCR) shall support 1.5 MHz or 2.0 MHz or both. U1-0: 1.5 MHz U1-1: 2.0 MHz	Selection of sub-carrier frequency (1.5 MHz or 2.0 MHz) depends on the EN 13372 profile selected.
U1a (*)	Tolerance of Sub- carrier Frequencies	within ± 0,1 %	(Consistent with EN 12253)
U1b	Use of Side Bands	Same data on both sides	(Consistent with EN 12253)
U2 (*)	OBU (DSRC-VU) Transmitter Spectrum Mask	According to EN12253 1) Out band power: see ETSI EN 300674-1 2) In band power: [U4a] dBm in 500 kHz 3) Emission in any other uplink channel: U2(3)-1 = – 35 dBm in 500 kHz	(Consistent with EN 12253)
U4a (*)	Maximum Single Side Band E.I.R.P. (boresight)	Two options: U4a-0: – 14 dBm U4a-1: – 21 dBm	According to declared and published specification of equipment designer
U4b (*)	Maximum Single Side Band E.I.R.P. (35°)	Two options: — Not applicable — – 17dBm	According to declared and published specification of equipment designer
U5	Polarisation	Left hand circular	(Consistent with EN 12253)

Item No.	Parameter	Value(s)	Remark
U5a	Cross Polarisation	XPD: In bore sight: (REDCR) RSU r ≥ 15 δB (DSRC-VU) OBU t ≥ 10 δB At – 3 dB: (REDCR) RSU r ≥ 10 δB (DSRC-VU) OBU t ≥ 6 δB	(Consistent with EN 12253)
U6	Sub-Carrier Modulation	2-PSK Encoded data synchronised with sub-carrier: Transitions of encoded data coincide with transitions of sub- carrier.	(Consistent with EN 12253)
U6b	Duty Cycle	Duty Cycle: 50 % ± α, α ≤ 5 %	(Consistent with EN 12253)
U6c	Modulation on Carrier	Multiplication of modulated sub- carrier with carrier.	(Consistent with EN 12253)
U7 (*)	Data Coding	NRZI (No transition at beginning of „1“ bit, transition at beginning of „0“ bit, no transition within bit)	(Consistent with EN 12253)
U8 (*)	Bit Rate	250 kbit/s	(Consistent with EN 12253)
U8a	Tolerance of Bit Clock	Within ± 1 000 ππμ	(Consistent with EN 12253)
U9	Bit Error Rate (B.E.R.) for communication	$\leq 10^{-6}$	(Consistent with EN 12253)
U11	Communication Zone	The spatial region within which the DSRC-VU is situated such that its transmissions are received by the REDCR with a B.E.R. of less than that given by U9a.	(Consistent with EN 12253)
U12a (*)	Conversion Gain (lower limit)	1 dB for each side band Range of angle: Circularly symmetric between bore sight and ± 35° and	
		within – 45° – + 45°Corresponding to the plane parallel to the road surface when the DSRC-VU later is installed in the vehicle (Azimuth)	Greater that the specified value range for horizontal angles up to ± 45°, due to the use cases defined in this annex.
U12b (*)	Conversion Gain (upper limit)	10 dB for each side band	Less than the specified value range for each side band within a circular cone around boresight of ± 45° opening angle
U13	Preamble	Preamble is mandatory.	(Consistent with EN 12253)

Item No.	Parameter	Value(s)	Remark
U13a	Preamble Length and Pattern	32 to 36 µs modulated with sub- carrier only, then 8 bits of NRZI coded „0“ bits.	(Consistent with EN 12253)
U13b	Trailing Bits	The DSRC-VU is permitted to transmit a maximum of 8 bits after the end flag. A RSU (REDCR) is not required to take these additional bits into account.	(Consistent with EN 12253)

(*) – Uplink parameters subject to conformance testing in accordance with relevant parameter test from EN 300 674-1

5.3.3 *Konstrukce antény*

5.3.3.1 Anténa REDCR

DSC_30 Konstrukce antény *REDCR* je funkcí komerčního návrhu a funguje v mezích stanovených v bodě 5.3.2, přičemž je přizpůsoben tak, aby byl optimalizován výkon čtení *DSRC-REDCR* pro specifický účel a podmínky čtení, pro které bylo *REDCR* navrženo.

5.3.3.2 Anténa VU

DSC_31 Konstrukce antény *REDCR* je funkcí komerčního návrhu a funguje v mezích stanovených v bodě 5.3.2, přičemž je přizpůsoben tak, aby byl optimalizován výkon čtení *DSRC-REDCR* pro specifický účel a podmínky čtení, pro které bylo *REDCR* navrženo.

DSC_32 Anténa VU je připevněna k čelnímu sklu vozidla nebo v jeho blízkosti, jak je uvedeno v bodě 5.1 výše.

DSC_33 Ve zkušebním prostředí v dílně (viz část 6.3) by se anténa DSCR-VU upevněná, jak je popsáno výše v bodě 5.1, měla úspěšně připojit ke standardní zkušební komunikaci a úspěšně zajistit transakci RTM podle definice v tomto dodatku na vzdálenost 2 až 10 metrů, po více než 99 % času, zprůměrováno na 1 000 přečtených dotazů.

5.4 **Požadavky protokolu DSRC pro RTM**

5.4.1 *Přehled*

DSC_34 Transakční protokol pro stahování *dat* pomocí rozhraní 5,8 GHz DSRC musí být v souladu s následujícími kroky. Tento oddíl popisuje postup transakce v ideálních podmínkách, aniž by docházelo k opakovanému vysílání nebo přerušení komunikace.

POZNÁMKA Účelem iniciační fáze (krok 1) je vytvoření komunikace mezi *REDCR* a DSRC celků ve vozidle, které se dostaly do transakční zóny 5,8 GHz DSRC (řídicí jednotka-vedlejší jednotka), ale dosud nenavázaly komunikaci s *REDCR*, a informování procesů aplikace.

— **Krok 1** Inicializace. *REDCR* vyšle rámec obsahující „servisní tabulku signálů“ (BST), která obsahuje identifikátory aplikace (AID) v servisním seznamu, který podporuje. V aplikaci RTM se jednoduše jedná o službu s hodnotou AID = 2 (Freight&Fleet). *DSRC-VU* vyhodnotí přijatou BST a odpoví (viz níže) seznamem podporovaných aplikací v doméně Freight&Fleet nebo neodpoví, nejsou-li podporovány žádné aplikace. Jestliže *REDCR* neuvádí AID = 2, DSRC-VU neodpoví na REDCR.

— **Krok 2** *DSRC-VU* vyšle rámec obsahující žádost o přidělení soukromého okna.

— **Krok 3** *REDCR* vyšle rámec obsahující přidělení soukromého okna.

— **Krok 4** *DSRC-VU* použije přidělené soukromé okno pro odeslání rámce obsahujícího servisní tabulku svého vozidla (VST). Tato VST obsahuje seznam všech různých instancí aplikací, které tento *DSRC-VU* podporuje v rámci AID = 2. Různé instance jsou identifikovány pomocí jedinečně generovaných EID, které jsou vždy spojeny s hodnotou parametru Application Context Mark (kontextová značka aplikace) indikující aplikaci a podporovanou normu.

— **Krok 5** *REDCR* potom analyzuje nabízenou VST, a buď ukončí spojení (RELEASE), protože nemá zájem o nic, co VST může nabídnout (tj. přijímá VST od *DSRC-VU*, který nepodporuje transakci RTM), nebo přijme-li příslušnou VST, spustí instanci aplikace.

— **Krok 6** Za tímto účelem REDCR odešle rámec obsahující příkaz k načtení dat RTM, označující instanci aplikace RTM uvedením identifikátoru, který určí příslušnou instanci aplikace RTM (jak stanoví DSRC-VU ve VST) a přidělí soukromé okno.

— **Krok 7** *DSRC-VU* použije nově přidělené soukromé okno pro odeslání rámce, který obsahuje adresovaný identifikátor, který odpovídá instanci aplikace RTM, jak je uvedeno ve VST, společně s atributem *RtmData* (prvek přenášených dat + bezpečnostní prvek).

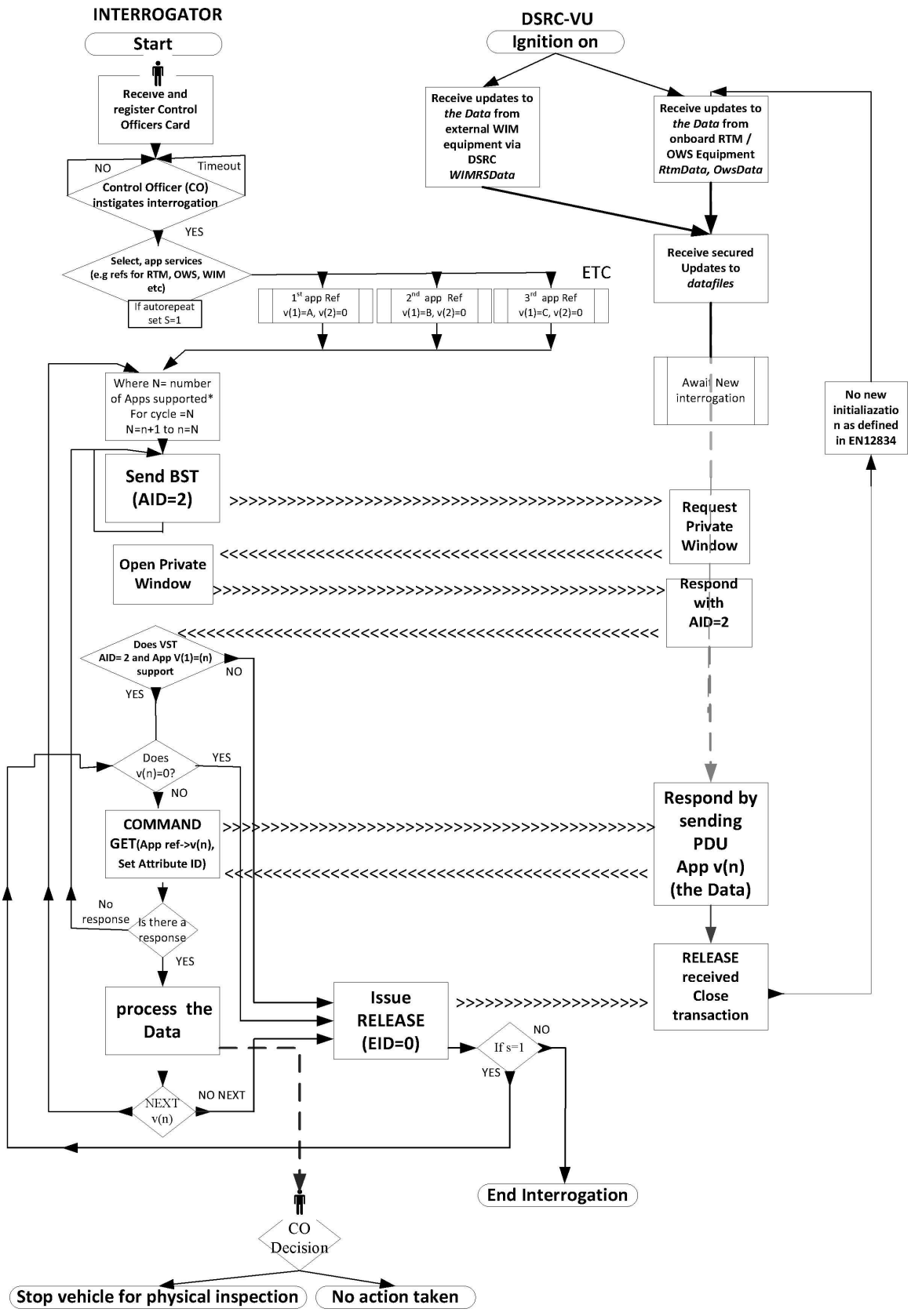
— **Krok 8** Je-li požadováno více služeb, hodnota „n“ se změní na další servisní referenční číslo a proces se opakuje.

— **Krok 9** *REDCR* potvrdí přijetí dat odesláním rámce obsahujícího příkaz RELEASE do *DSRC-VU*, aby byla relace ukončena, NEBO v případě, že se mu nepodaří vyhodnotit úspěšné přijetí LDPU, vrátí se do kroku 6.

Viz obrázek 14.6 a názorný popis transakčního protokolu.

Obrázek 14.6

Vývojový diagram RTM přes 5.8 GHz DSRC



5.4.2 *Příkazy*

DSC_35 Následující příkazy jsou jediné funkce používané ve fázi transakce RTM

— **INITIALISATION.request**: Příkaz vydaný REDCR ve formě rádiové zprávy s definicí aplikací, které REDCR podporuje.

— **INITIALISATION.response**: Odpověď DSRC-VU potvrzující spojení a obsahující seznam podporovaných případů aplikací s charakteristikami a informacemi, jak k nim přistupovat (EID).

— **GET.request**: Příkaz vydaný *REDCR* pro *DSRC-VU*, který určí příslušnou realizaci aplikace pomocí definovaného EID, jak byl přijat ve VST, a dává *DSRC-VU* pokyn k odeslání vybraných atributů s *daty*. Cílem příkazu GET je pro *REDCR* získání *dat* od *DSRC-VU*.

— **GET.response**: Odpověď DSRC-VU, která obsahuje požadovaná *data*.

— **ACTION.request ECHO**: Příkaz pro *DSRC-VU*, aby vrátil data z *DSRC-VU* do *REDCR*. Cílem příkazu ECHO je umožnit dílnám nebo testovacím zařízením pro typové zkoušky testovat funkci spojení DSRC bez nutnosti přístupu k bezpečnostním údajům.

— **ACTION**.response ECHO: Odpověď DSRC VU na příkaz ECHO.

— **EVENT_REPORT.request** RELEASE: Příkaz pro *DSRC-VU*, že transakce je ukončena. Cílem příkazu RELEASE je ukončení relace s *DSRC-VU*. Po přijetí příkazu RELEASE *DSRC-VU* neodpovídá na žádné další dotazy v rámci aktuálního spojení. Podle EN 12834 se DSRC-VU nepřipojí dvakrát ke stejnému dotazovacímu zařízení, není-li mimo komunikační zónu 255 sekund nebo změní-li se ID signálu dotazovacího zařízení.

5.4.3 *Pořadí dotazovacích příkazů*

DSC_36 Z hlediska pořadí příkazů a odpovědí lze transakci popsat takto:

Sequence	Sender		Receiver	Description	Action
1	REDCR	>	DSRC-VU	Initialisation of the communication link – Request	REDCR broadcasts BST
2	*DSRC-VU*	>	*REDCR*	*Initialisation of the communication link – Response*	*If BST supports AID=2 then DSRC-VU Requests a private window*
3	REDCR	>	DSRC-VU	Grants a private window	Sends Frame containing private window allocation
4	*DSRC-VU*	>	*REDCR*	*Sends VST*	*Sends Frame comprising VST*
5	REDCR	>	DSRC-VU	Sends GET.request for data in Attribute for specific EID	
6	*DSRC-VU*	>	*REDCR*	*Sends GET.response with requested Attribute for specific EID*	*Sends Attribute (RTMData, OWSData….) with data for specific EID*

Sequence	Sender		Receiver	Description	Action
7	REDCR	>	DSRC-VU	Sends GET.request for data other Attribute (if appropriate)	
8	*DSRC-VU*	>	*REDCR*	*Sends GET.response with requested Attribute*	*Sends Attribute with data for specific EID*
9	REDCR	>	DSRC-VU	Acknowledges successful receipt of data	Sends RELEASE command which closes transaction
10	*DSRC-VU*			*Closes transaction*	

Příklad pořadí a obsahu transakce s vyměňovanými rámci, jak je stanoveno v článcích 5.4.7 a 5.4.8.

5.4.4 *Struktury dat*

DSC_37 Sémantická struktura *dat* předávaných rozhraním 5,8 GHz DSRC odpovídá popisu uvedenému v této příloze. Struktura těchto dat je stanovena v tomto článku.

DSC_38 Přenášená data (data RTM) obsahují řetězec

1. dat EncryptedTachographPayload, která jsou šifrováním údaje TachographPayload stanoveného v ASN.1 v části 5.4.5. Způsob šifrování je popsán v dodatku 11;
2. dat DSRCSecurityData, stanovených v dodatku 11.

DSC_39 Data RTM jsou označena jako atribut RTM = 1 a přenášena v kontejneru RTM =10.

DSC_40 Kontextová značka RTM identifikuje podporované standardní části v řadě TARV norem (RTM odpovídá části 9)

Definice modulu ASN.1 pro data DSRC v aplikaci RTM je určena takto:

```
    TarvRtm {iso(1) standard(0) 15638 part9(9) version1(1)}
    DEFINITIONS AUTOMATIC TAGS
    ::= BEGIN
    IMPORTS
    -- Imports data attributes and elements from EFC which are used for RTM
    LPN
    FROM EfcDsrcApplication {iso(1) standard(0) 14906 application(0) version5(5)}

    -- Imports function parameters from the EFC Application Interface Definition
    SetMMIRq
    FROM EfcDsrcApplication {iso(1) standard(0) 14906 application(0) version5(5)}

    -- Imports the L7 DSRCData module data from the EFC Application Interface Definition
    Action-Request, Action-Response, ActionType, ApplicationList, AttributeIdList, AttributeList,
    Attributes,
    BeaconID, BST, Dsrc-EID, DSRCApplicationEntityID, Event-Report-Request, Event-Report- Response,
    EventType, Get-Request, Get-Response, Initialisation-Request, Initialisation-Response,
    ObeConfiguration, Profile, ReturnStatus, Time, T-APDUs, VST
    FROM EfcDsrcGeneric {iso(1) standard(0) 14906 generic(1) version5(5)};


    -- Definitions of the RTM functions:
    RTM-InitialiseComm-Request ::= BST
    RTM-InitialiseComm-Response::= VST
    RTM-DataRetrieval-Request::= Get-Request (WITH COMPONENTS {fill (SIZE(1)), eid, accessCredentials ABSENT,iid
    ABSENT,  attrIdList})
    RTM-DataRetrieval-Response::= Get-Response {RtmContainer} (WITH COMPONENTS {..., eid, iid ABSENT})
    RTM-TerminateComm::= Event-Report-Request {RtmContainer}(WITH COMPONENTS {mode (FALSE), eid (0),
    eventType (0)})

    RTM-TestComm-Request::= Action-Request {RtmContainer} (WITH COMPONENTS {..., eid (0), actionType
    (15), accessCredentials ABSENT, iid ABSENT})

    RTM-TestComm-Response::= Action-Response {RtmContainer} (WITH COMPONENTS {..., fill (SIZE(1)), eid
    (0), iid ABSENT})

    -- Definitions of the RTM attributes:
    RtmData ::= SEQUENCE {
          encryptedTachographPayload OCTET STRING (SIZE(67)) (CONSTRAINED BY { -- calculated encrypting
    TachographPayload as per Appendix 11 --}),
          DSRCSecurityData OCTET STRING
          }
    TachographPayload ::= SEQUENCE {
                tp15638VehicleRegistrationPlate LPN -- Vehicle Registration Plate as per EN 15509.
                tp15638SpeedingEvent            BOOLEAN,  -- 1= Irregularities in speed (see Annex 1C)
                tp15638DrivingWithoutValidCard  BOOLEAN,     -- 1= Invalid card usage (see Annex 1C)
                tp15638DriverCard               BOOLEAN,-- 0= Indicates a valid driver card  (see Annex 1C)
                tp15638CardInsertion            BOOLEAN, -- 1= Card insertion while driving (see Annex 1C)
                tp15638MotionDataError          BOOLEAN, -- 1= Motion data error (see Annex 1C)
                tp15638VehicleMotionConflict    BOOLEAN, -- 1= Motion conflict (see Annex 1C)
                tp156382ndDriverCard            BOOLEAN, -- 1= Second driver card inserted (see Annex 1C)
                tp15638CurrentActivityDriving   BOOLEAN, -- 1= other activity selected;
                                                          -- 0= driving selected
                tp15638LastSessionClosed        BOOLEAN, -- 1= improperly, 0= properly, closed
                tp15638PowerSupplyInterruption  INTEGER (0..127), -- Supply interrupts in the last 10 days
                tp15638SensorFault              INTEGER (0..255),-- eventFaultType as per data dictionary
    -- All subsequent time related types as defined in Annex 1C.
                tp15638TimeAdjustment           INTEGER(0..4294967295), -- Time of the last time adjustment
                tp15638LatestBreachAttempt      INTEGER(0..4294967295), -- Time of last breach attempt
                tp15638LastCalibrationData      INTEGER(0..4294967295), -- Time of last calibration data
                tp15638PrevCalibrationData      INTEGER(0..4294967295), -- Time of previous calibration data
                tp15638DateTachoConnected       INTEGER(0..4294967295), -- Date tachograph connected
                tp15638CurrentSpeed             INTEGER (0..255), -- Last current recorded speed
                tp15638Timestamp                INTEGER(0..4294967295) -- Timestamp of current record[2]
                }
Rtm-ContextMark ::= SEQUENCE {
  standardIdentifier    StandardIdentifier, -- identifier of the TARV part and its version

  RtmCommProfile          INTEGER {
                                  C1 (1),
                                  C2 (2)
                                  } (0..255) DEFAULT 1
  }
RtmTransferAck ::= INTEGER {
                  Ok (1),
                  NoK (2)
                  } SIZE (1..255)
```

```
StandardIdentifier ::= OBJECT IDENTIFIER
RtmContainer ::= CHOICE {
        integer                         [0]    INTEGER,
        bitstring                       [1]    BIT STRING,
        octetstring                     [2]    OCTET STRING (SIZE (0..127, ...)),
        universalString                 [3]    UniversalString,
        beaconId                        [4]    BeaconID,
        t-apdu                          [5]    T-APDUs,
        dsrcApplicationEntityId         [6]    DSRCApplicationEntityID,
        dsrc-Ase-Id                     [7]    Dsrc-EID,
        attrIdList                      [8]    AttributeIdList,
        attrList                        [9]    AttributeList{RtmContainer},
        rtmData                         [10]   RtmData,
        rtmContextmark                  [11]   Rtm-ContextMark,
        reserved12                      [12]   NULL,
        reserved13                     [13]   NULL,
        reserved14                      [14]   NULL,
        time                            [15]   Time,
-- values from 16 to 255 reserved for ISO/CEN usage
        }}

END
```

5.4.5 *Prvky RTMData, provedené akce a definice*

DSC_41 Hodnoty dat vypočítávané VU a používané pro aktualizaci zabezpečených dat v DSRC-VU se vypočítávají podle pravidel stanovených v tabulce 14.3:

Tabulka 14.3

Prvky RTMData, provedené akce a definice

(1) RTM Data Element	(2) Action performed by the VU		(3) ASN.1 definition of data
RTM1 **Vehicle Registration Plate**	The VU shall set the value of the *tp15638VehicleRegistrationPlate* data element RTM1 from the recorded value of the data type *VehicleRegistrationIdentification* as defined in Appendix 1 *VehicleRegistrationIdentification*	Vehicle Registration Plate expressed as a string of characters	`tp15638VehicleRegstrationPlate LPN, --Vehicle Registration Plate imported from ISO 14906 with the limitation specified in EN 15509 which is a SEQUENCE comprising Country Code followed by an alphabet indicator followed by the plate number itself, which is always 14 octets (padded with zero's) so the EN 15509 LPN type length is always 17 octets, of which 14 are the "real" plate number.`

(1) RTM Data Element	(2) Action performed by the VU		(3) ASN.1 definition of data
RTM2 **Speeding Event**	The VU shall generate a boolean value for data element RTM2 tp15638SpeedingEvent. The tp15638SpeedingEvent value shall be calculated by the VU from the number of Over Speeding Events recorded in the VU in the last 10 days of occurrence, as defined in Annex 1C. If there is at least one tp15638SpeedingEvent in the last 10 days of occurrence, the tp15638SpeedingEvent value shall be set to TRUE. ELSE if there are no events in the last 10 days of occurrence, the tp15638SpeedingEvent shall be set to FALSE.	1 (TRUE) – Indicates irregularities in speed within last 10 days of occurrence	`tp15638speedingEvent BOOLEAN,`
RTM3 **Driving Without Valid Card**	The VU shall generate a boolean value for data element RTM3 tp15638DrivingWithoutValidCard. The VU shall assign a value of True to the tp15638DrivingWithoutValidCard variable if the VU data has recorded at least one event in the last 10 days of occurrence of type „Driving without an appropriate card“ event as defined in Annex 1C. ELSE if there are no events in the last 10 days of occurrence, the tp15638DrivingWithoutValidCard variable shall be set to FALSE.	1 (TRUE) = Indicates invalid card usage	`tp15638DrivingWithoutValidCard` `BOOLEAN,`
RTM4 **Valid Driver Card**	The VU shall generate a boolean value for data element RTM4 tp15638DriverCard on the basis of the data stored in the VU and defined in Appendix 1. If no valid driver card is present the VU shall set the variable to TRUE ELSE if a valid driver card is present the VU shall set the variable to FALSE	0 (FALSE) = Indicates a valid driver card	`tp15638DriverCard BOOLEAN,`
RTM5 **Card Insertion while Driving**	The VU shall generate a boolean value for data element RTM5. The VU shall assign a value of TRUE to the tp15638CardInsertion variable if the VU data has recorded in the last 10 days of occurrence at least one event of type „Card insertion while driving.“ as defined in Annex 1C. ELSE if there are no such events in the last 10 days of occurrence, the tp15638CardInsertion variable shall be set to FALSE.	1 (TRUE) = Indicates card insertion while driving within last 10 days of occurrence	`tp15638CardInsertion BOOLEAN,`
RTM6 **Motion Data Error**	The VU shall generate a boolean value for data element RTM6. The VU shall assign a value of TRUE to the tp15638MotionDataError variable if the VU data has in the last 10 days of occurrence recorded at least one event of type „Motion data error“ as defined in Annex 1C. ELSE if there are no such events in the last 10 days of occurrence, the tp15638MotionDataError variable shall be set to FALSE.	1 (TRUE) = Indicates motion data error within last 10 days of occurrence	`tp15638motionDataError BOOLEAN,`

(1) RTM Data Element	(2) Action performed by the VU		(3) ASN.1 definition of data
RTM7 **Vehicle Motion Conflict**	The VU shall generate a boolean value for data element RTM7. The VU shall assign a value of TRUE to the tp15638vehicleMotionConflict variable if the VU data has in the last 10 days recorded at least one event of type Vehicle Motion Conflict (value '0A'H). ELSE if there are no events in the last 10 days of occurrence, the tp15638vehicleMotionConflict variable shall be set to FALSE.	1 (TRUE) = Indicates motion conflict within last 10 days of occurrence	`tp15638vehicleMotionConflict` `BOOLEAN,`
RTM8 **2nd Driver Card**	The VU shall generate a boolean value for data element RTM8 on the basis of Annex 1C („Driver Activity Data" CREW and CO-DRIVER). If a 2nd valid driver card is present the VU shall set the variable to TRUE ELSE if a 2nd valid driver card is not present the VU shall set the variable to FALSE	1 (TRUE) = Indicates a second driver card inserted	`tp156382ndDriverCard BOOLEAN,`
RTM9 **Current Activity**	The VU shall generate a boolean value for data element RTM9. If the current activity is recorded in the VU as any activity other than „DRIVING" as defined in Annex 1C the VU shall set the variable to TRUE ELSE if the current activity is recorded in the VU as „DRIVING" the VU shall set the variable to FALSE	1 (TRUE) = other activity selected; 0 (FALSE) = driving selected	`tp15638currentActivityDriving` `BOOLEAN`
RTM10 **Last Session Closed**	The VU shall generate a boolean value for data element RTM10. If the last card session was not properly closed as defined in Annex 1C the VU shall set the variable to TRUE. ELSE if the last card session was properly closed the VU shall set the variable to FALSE	1 (TRUE) = improperly closed 0 (FALSE) = properly closed	`tp15638lastSessionClosed` `BOOLEAN`
RTM11 **Power Supply Interruption**	The VU shall generate an integer value for data element RTM11. The VU shall assign a value for the tp15638 „PowerSupplyInterruption variable equal to the longest power supply interruption" according to Article 9, Reg (EU) 165/2014 of type „Power supply interruption" as defined in Annex 1C. ELSE if in the last 10 days of occurrence there are have been no Power supply interruption events the value of the integer shall be set to 0.	— Number of power supply interruptions in last 10 days of occurrence	`tp15638powerSupplyInterruption` `INTEGER (0..127),`

(1) RTM Data Element	(2) Action performed by the VU		(3) ASN.1 definition of data
RTM12 **Sensor Fault**	The VU shall generate an integer value for data element RTM12. The VU shall assign to the variable sensorFault a value of: — 1 if an event of type '35'H Sensor fault has been recorded in the last 10 days, — 2 if an event of type GNSS receiver fault (either internal or external with enum values '51'H or '52'H) has been recorded in the last 10 days. — 3 if an event of type '53'H External GNSS communication fault has been recorded in the last 10 days of occurrence. — 4 If both Sensor Fault and GNSS receiver faults have been recorded in the last 10 days of occurrence — 5 If both Sensor Fault and External GNSS communication faults have been recorded in the last 10 days of occurrence — 6 If both GNSS receiver fault and External GNSS communication fault have been recorded in the last 10 days of occurrence — 7 If all three sensor faults, have been recorded in the last 10 days of occurrence ELSE it shall assign a value of 0 if no events have been recorded in the last 10 days of occurrence	— sensor fault one octet as per data dictionary	`tp15638SensorFault INTEGER (0..255),`
RTM13 **Time Adjustment**	The VU shall generate an integer value (timeReal from Appendix 1) for data element RTM13 on the basis of the presence of Time Adjustment data as defined in Annex 1C. The VU shall assign the value of time at which the last time adjustment data event has occurred. ELSE if no „Time Adjustment" event. as defined in Annex 1C is present in the VU data it shall set a value of 0	Time of the last time adjustment	`tp15638TimeAdjustment INTEGER(0..4294967295),`
RTM14 **Security Breach Attempt**	The VU shall generate an integer value (timeReal from Appendix 1) for data element RTM14 on the basis of the presence of a Security breach attempt event as defined in Annex 1C. The VU shall set the value of the time of the latest security breach attempt event recorded by the VU. ELSE if no „security breach attempt" event as defined in Annex 1C is present in the VU data it shall set a value of 0x00FF.	Time of last breach attempt — Default value =0x00FF	`tp15638LatestBreachAttempt INTEGER(0..4294967295),`
RTM15 **Last Calibration**	The VU shall generate an integer value (timeReal from Appendix 1) for data element RTM15 on the basis of the presence of Last Calibration data as defined in Annex 1C. The VU shall set the value of time of the latest two calibrations (RTM15 and RTM16), which are set in VuCalibrationData defined in Appendix 1. The VU shall set the value for RTM15 to the timeReal of the latest calibration record.	Time of last calibration data	`tp15638LastCalibrationData INTEGER(0..4294967295),`

(1) RTM Data Element	(2) Action performed by the VU		(3) ASN.1 definition of data
RTM16 **Previous Calibration**	The VU shall generate an integer value (timeReal from Appendix 1) for data element RTM16 of the calibration record preceding that of the last calibration ELSE if there has been no previous calibration the VU shall set the value of RTM16 to 0.	Time of previous calibration data	`tp15638PrevCalibrationData` `INTEGER(0..4294967295),`
RTM17 **Date Tachograph Connected**	For data element RTM17 the VU shall generate an integer value (timeReal from Appendix 1). The VU shall set the value of the time of the initial installation of the VU. The VU shall extract this data from the VuCalibrationData (Appendix 1) from the vuCalibrationRecords with CalibrationPurpose equal to: '03'H	Date tachograph connected	`tp15638DateTachoConnected` `INTEGER(0..4294967295),`
RTM18 **Current Speed**	The VU shall generate an integer value for data element RTM18. The VU shall set the value for RTM16 to the last current recorded speed at the time of the latest update of the RtmData.	Last current recorded speed	`tp15638CurrentSpeed INTEGER (0..255),`
RTM19 **Časové razítko**	For data element RTM19 the VU shall generate an integer value (timeReal from Appendix 1). The VU shall set the value for RTM19 to the time of the latest update of the RtmData.	Timestamp of current TachographPayload record	`tp15638Timestamp` `INTEGER(0..4294967295),`

5.4.6 *Mechanismus přenosu dat*

DSC_42 Výše definovaná přenášená data jsou vyžádána REDCR po inicializační fázi a následně předána *DSRC-VU* v přiděleném okně. Příkaz GET používá REDCR pro stažení dat.

DSC_43 Pro všechny výměny DSRC jsou data šifrována pomocí PER (Packed Encoding Rules).

5.4.7 *Podrobný popis transakce DSRC*

DSC_44 Inicializace se provádí podle DSC_44–DSC_48) a tabulek 14.4–14.9. V inicializační fázi REDCR začne odesílat rámec obsahující BST (servisní tabulka signálů) podle EN 12834 a EN 13372, 6.2, 6.3, 6.4 a 7.1 s nastaveními podle následující tabulky 14.4.

Tabulka 14.4

Inicializace – nastavení rámce BST

Field	Settings
Link Identifier	Broadcast address
BeaconId	As per EN 12834
Time	As per EN 12834
Profile	No extension, 0 or 1 to be used
MandApplications	No extension, EID not present, Parameter not present, AID = 2 Freight&Fleet
NonMandApplications	Not present
ProfileList	No extension, number of profiles in list = 0
Fragmentation header	No fragmentation
Layer 2 settings	Command PDU, UI command

Praktický příklad nastavení uvedených v tabulce 14.4 s označením šifrování bitů je uveden v následující tabulce 14.5.

Tabulka 14.5

Inicializace – příklad obsahu rámce BST

Octet #	Attribute/Field	Bits in octet	Description
1	FLAG	0111 1110	Start flag
2	Broadcast ID	1111 1111	Broadcast address
3	MAC Control Field	1010 0000	Command PDU
4	LLC Control field	0000 0011	UI command
5	Fragmentation header	1xxx x001	No fragmentation

Octet #	Attribute/Field	Bits in octet	Description
6	BST	1000	Initialisation request
	SEQUENCE {		
	OPTION indicator BeaconID SEQUENCE { ManufacturerId INTEGER (0..65535)	0	NonMand applications not present
		xxx	Manufacturer Identifier
7		xxxx xxxx	
8		xxxx x	
	IndividualID INTEGER (0..134217727)	xxx	27 bit ID available for manufacturer
9		xxxx xxxx	
10		xxxx xxxx	
11	}	xxxx xxxx	
12	Time INTEGER (0..4294967295)	xxxx xxxx	32 bit UNIX real time
13		xxxx xxxx	
14		xxxx xxxx	
15		xxxx xxxx	
16	Profile INTEGER (0..127,...)	0000 0000	No extension. Example profile 0
17	MandApplications SEQUENCE (SIZE (0..127,...)) OF {	0000 0001	No extension, Number of mandApplications = 1
18	SEQUENCE {		
	OPTION indicator	0	EID not present
	OPTION indicator	0	Parameter not present
	AID DSRCApplicationEntityID } }	00 0010	No extension. AID= 2 Freight&Fleet

Octet #	Attribute/Field	Bits in octet	Description
19	ProfileList SEQUENCE (0..127,…) OF Profile }	0000 0000	No extension, number of profiles in list = 0
20	FCS	xxxx xxxx	Frame check sequence
21		xxxx xxxx	
22	Flag	0111 1110	End Flag

DSC_45 Po přijetí BST požádá *DSRC-VU* o přidělení soukromého okna, jak je uvedeno v EN 12795 a EN 13372, 7.1.1, bez jakýchkoli specifických nastavení RTM. Tabulka 14.6 uvádí příklad šifrování bitů.

Tabulka 14.6

Inicializace – obsah rámce žádosti o přidělení soukromého okna

Octet #	Attribute/Field	Bits in octet	Description
1	FLAG	0111 1110	Start flag
2	Private LID	xxxx xxxx	Link address of specific DSRC-VU
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control field	0110 0000	Private window request
7	FCS	xxxx xxxx	Frame check sequence
8		xxxx xxxx	
9	Flag	0111 1110	End Flag

DSC_46 REDCR potom odpoví přidělením soukromého okna, podle specifikace v EN 12795 a EN 13372, 7.1.1, bez jakýchkoli specifických nastavení RTM.

Tabulka 14.7 uvádí příklad šifrování bitů.

Tabulka 14.7

Inicializace – obsah rámce přidělení soukromého okna

Octet #	Attribute/Field	Bits in octet	Description
1	FLAG	0111 1110	Start flag
2	Private LID	xxxx xxxx	Link address of the specific DSRC-VU
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control field	0010 s000	Private window allocation
7	FCS	xxxx xxxx	Frame check sequence
8		xxxx xxxx	
9	Flag	0111 1110	End Flag

DSC_47 Po přijetí přiděleného soukromého okna *DSRC-VU* odešle svou VST (servisní tabulka vozidla) podle definice v EN 12834 a EN 13372, 6.2, 6.3, 6.4 a 7.1 s nastaveními podle tabulky 14.8 pomocí přiděleného přenosového okna.

Tabulka 14.8

Inicializace – nastavení rámce VST

Field	Settings
Private LID	As per EN 12834
VST parameters	Fill=0, then for each supported application: EID present, parameter present, AID=2, EID as generated by the OBU
Parameter	No extension, Contains the RTM Context Mark
ObeConfiguration	The optional ObeStatus field may be present, but shall not be used by the REDCR
Fragmentation header	No fragmentation
Layer 2 settings	Command PDU, UI command

DSC_48 *DSRC-VU* podporuje aplikaci „Freight and Fleet“ označenou identifikátorem aplikace ‘2’. Mohou být podporovány i další identifikátory aplikací, ale nejsou přítomny v této VST, protože BST pouze požaduje AID=2. Pole „Aplikace“ obsahuje seznam případů podporovaných aplikací v *DSRC-VU*. Pro každou realizaci podporované aplikace je uveden odkaz na příslušnou normu tvořený kontextovou značkou Rtm, která je složena z IDENTIFIKÁTORU OBJEKTU představujícího příslušnou normu, její část (9 pro RTM) a případně její verzi a navíc EID vytvořený DSRC-VU a spojený s daným případem aplikace.

Praktický příklad nastavení stanovených v tabulce 14.8 s označením šifrování bitů je uveden v tabulce 14.9.

Tabulka 14.9

Inicializace – příklad obsahu rámce VST

Octet #	Attribute/Field	Bits in octet	Description
1	FLAG	0111 1110	Start flag
2	Private LID	xxxx xxxx	Link address of the specific DSRC-VU
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control field	1100 0000	Command PDU
7	LLC Control field	0000 0011	UI command
8	Fragmentation header	1xxx x001	No fragmentation
9	VST SEQUENCE {	1001	Initialisation response
	Fill BIT STRING (SIZE(4))	0000	Unused and set to 0
10	Profile INTEGER (0..127,…) Applications SEQUENCE OF {	0000 0000	No extension. Example profile 0
11		0000 0001	No extension, 1 application
12	SEQUENCE {		
	OPTION indicator	1	EID present
	OPTION indicator	1	Parameter present
	AID DSRCApplicationEntityID	00 0010	No extension. AID= 2 Freight&Fleet
13	EID Dsrc-EID	xxxx xxxx	Defined within the OBU and identifying the application instance.

Octet #	Attribute/Field	Bits in octet	Description
14	Parameter Container {	0000 0010	No extension, Container Choice = 02, Octet string
15		0000 1000	No extension, Rtm Context Mark length = 8
16	Rtm-ContextMark::= SEQUENCE { StandardIdentifier standardIdentifier	0000 0110	Object Identifier of the supported standard, part, and version. Example: ISO (1) Standard (0) TARV (15638) part9 (9) Version1 (1). First octet is 06H, which is the Object Identifier Second octet is 06H, which is its length. Subsequent 6 octets encode the example Object Identifier Note that only one element of the sequence is present (the optional RtmCommProfile element is omitted)
17		0000 0110	
18		0010 1000	
19		1000 0000	
20		1111 1010	
21		0001 0110	
22		0000 1001	
23		0000 0001	
24	ObeConfiguration Sequence { OPTION indicator	0	ObeStatus not present
	EquipmentClass INTEGER (0..32767)	xxx xxxx	
25		xxxx xxxx	
26	ManufacturerId INTEGER (0..65535)	xxxx xxxx	Manufacturer identifier for the DSRC-VU as described in ISO 14816 Register
27		xxxx xxxx	
28	FCS	xxxx xxxx	Frame check sequence
29		xxxx xxxx	
30	Flag	0111 1110	End Flag

DCS_49 REDCR potom načte data vydáním příkazu GET odpovídajícímu příkazu GET podle definic v EN 13372, 6.2, 6.3, 6.4 a EN 12834 s nastaveními uvedenými v tabulce 14.10.

Tabulka 14.10

Prezentace – nastavení rámce žádosti GET

Field	Settings
Invoker Identifier (IID)	Not present
Link Identifier (LID)	Link address of the specific DSRC-VU
Chaining	No

Field	Settings
Element Identifier (EID)	As specified in the VST. No extension
Access Credentials	No
AttributeIdList	No extension, 1 attribute, AttributeID = 1 (RtmData)
Fragmentation	No
Layer2 settings	Command PDU, Polled ACn command

Tabulka 14.11 uvádí příklad čtení dat RTM.

Tabulka 14.11

Prezentace – příklad rámce žádosti Get

Octet #	Attribute/Field	Bits in octet	Description
1	FLAG	0111 1110	Start flag
2	Private LID	xxxx xxxx	Link address of the specific DSRC-VU
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control field	1010 s000	Command PDU
7	LLC Control field	n111 0111	Polled ACn command, n bit
8	Fragmentation header	1xxx x001	No fragmentation
9	Get.request SEQUENCE {	0110	Get request
	OPTION indicator	0	Access Credentials not present
	OPTION indicator	0	IID not present
	OPTION indicator	1	AttributeIdList present
	Fill BIT STRING(SIZE(1))	0	Set to 0.
10	EID INTEGER(0..127,…)	xxxx xxxx	The EID of the RTM application instance, as specified in the VST. No extension
11	AttributeIdList SEQUENCE OF { AttributeId }}	0000 0001	No extension, number of attributes = 1
12		0000 0001	AttributeId=1, RtmData. No extension

Octet #	Attribute/Field	Bits in octet	Description
13	FCS	xxxx xxxx	Frame check sequence
14		xxxx xxxx	
15	Flag	0111 1110	End Flag

DSC_50 Po přijetí žádosti GET odešle *DSRC-VU* odpověď GET s požadovanými daty odpovídajícími odpovědi GET podle definic v EN 13372, 6.2, 6.3, 6.4 a EN 12834 s nastaveními podle tabulky 14.12.

Tabulka 14.12

Prezentace – nastavení rámce odpovědi GET

Field	Settings
Invoker Identifier (IID)	Not present
Link Identifier (LID)	As per EN 12834
Chaining	No
Element Identifier (EID)	As specified in the VST.
Access Credentials	No
Fragmentation	No
Layer2 settings	Response PDU, Response available and command accepted, ACn command

Tabulka 14.13 uvádí příklad čtení dat RTM.

Tabulka 14.13

Prezentace – příklad obsahu rámce odpovědi

Octet #	Attribute/Field	Bits in octet	Description
1	FLAG	0111 1110	Start flag
2	Private LID	xxxx xxxx	Link address of the specific DSRC-VU
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	

Octet #	Attribute/Field	Bits in octet	Description
6	MAC Control field	1101 0000	Response PDU
7	LLC Control field	n111 0111	Response available, ACn command n bit
8	LLC Status field	0000 0000	Response available and command accepted
9	Fragmentation header	1xxx x001	No fragmentation
10	Get.response SEQUENCE {	0111	Get response
	OPTION indicator	0	IID not present
	OPTION indicator	1	Attribute List present
	OPTION indicator	0	Return status not present
	Fill BIT STRING(SIZE(1))	0	Not used
11	EID INTEGER(0..127,…)	xxxx xxxx	Responding from the RTM application Instance. No extension,
12	AttributeList SEQUENCE OF {	0000 0001	No extension, number of attributes = 1
13	Attributes SEQUENCE { AttributeId	0000 0001	No extension, AttributeId=1 (RtmData)
14	AttributeValue CONTAINER {	0000 1010	No extension, Container Choice = 10_{10}.
15		kkkk kkkk	RtmData
16		kkkk kkkk	
17		kkkk kkkk	
…		…	
n	}}}}	kkkk kkkk	
n+1	FCS	xxxx xxxx	Frame check sequence
n+2		xxxx xxxx	
n+3	Flag	0111 1110	End Flag

DSC_51 REDCR potom ukončí spojení vydáním příkazu EVENT_REPORT, RELEASE podle EN 13372, 6.2, 6.3, 6.4 a EN 12834, 7.3.8 bez jakýchkoli specifických nastavení RTM. Tabulka 14.14 uvádí příklad šifrování bitů příkazu RELEASE.

Tabulka 14.14

Ukončení. EVENT_REPORT uvolnění obsahu rámce

Octet #	Attribute/Field	Bits in octet	Description
1	FLAG	0111 1110	Start flag
2	Private LID	xxxx xxxx	Link address of the specific DSRC-VU
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control field	1000 s000	The frame contains a command LPDU
7	LLC Control field	0000 0011	UI command
8	Fragmentation header	1xxx x001	No fragmentation
9	EVENT_REPORT.request SEQUENCE {	0010	EVENT_REPORT (Release)
	OPTION indicator	0	Access Credentials not present
	OPTION indicator	0	Event parameter not present
	OPTION indicator	0	IID not present
	Mode BOOLEAN	0	No response expected
10	EID INTEGER (0..127,…)	0000 0000	No extension, EID = 0 (System)
11	EventType INTEGER (0..127,…) }	0000 0000	Event type 0 = Release
12	FCS	xxxx xxxx	Frame check sequence
13		xxxx xxxx	
14	Flag	0111 1110	End Flag

DSC_52 Neočekává se, že *DSRC-VU* odpoví na příkaz Release. Komunikace je poté ukončena.

5.4.8 *Popis transakce testu DSRC*

DSC_53 Úplné testy, které zahrnují zabezpečení dat, musí být prováděny podle dodatku 11 – Společné bezpečnostní mechanismy oprávněnými osobami s přístupem k bezpečnostním postupům pomocí normálních příkazů GET stanovených výše.

DSC_54 Uvedení do provozu a pravidelné kontrolní testy, které vyžadují dešifrování a pochopení obsahu dešifrovaných údajů, se provádějí v souladu s dodatkem 11 – Společné bezpečnostní mechanismy a dodatkem 9 – Schválení typu – minimální rozsah požadovaných zkoušek.

Základní komunikaci DSRC však lze testovat příkazem ECHO. Tyto testy mohou být požadovány po uvedení do provozu, při pravidelné kontrole nebo jindy podle požadavků příslušného kontrolního orgánu nebo nařízení (EU) č. 165/2014 (viz 6 níže).

DSC_55 Pro provedení tohoto základního testu komunikace REDCR vydá příkaz ECHO během relace, tj. po úspěšném dokončení inicializační fáze. Sekvence interakcí je tak podobná sekvenci sledování:

— Krok 1 *REDCR* vyšle „servisní tabulku signálů“ (BST), která obsahuje identifikátory aplikace (AID) v servisním seznamu, který podporuje. V aplikacích RTM se jednoduše jedná o službu s hodnotou AID = 2.

DSRC-VU vyhodnotí přijatou BST, a pokud zjistí, že BST požaduje Freight&Fleet (AID = 2), *DSRC-VU* odpoví. Pokud *REDCR* nenabízí AID = 2, *DSRC-VU* ukončí transakci s *REDCR*.

— Krok 2 *DSRC-VU* vyšle žádost o přidělení soukromého okna.

— Krok 3 REDCR vyšle přidělení soukromého okna.

— Krok 4 *DSRC-VU* použije přidělené soukromé okno pro odeslání servisní tabulky svého vozidla (VST). Tato VST obsahuje seznam všech různých realizací aplikace, které tento *DSRC-VU* podporuje v rámci AID = 2. Různé realizace jsou identifikovány pomocí jedinečných EID, které jsou vždy spojeny s hodnotou parametru uvádějící podporovaný příklad použití.

— Krok 5 *REDCR* potom analyzuje nabízenou VST a buď ukončí spojení (RELEASE), protože nemá zájem o nic, co VST může nabídnout (tj. přijímá VST od *DSRC-VU*, který nepodporuje transakci RTM), nebo přijme-li příslušnou VST, spustí realizaci aplikace.

— Krok 6 *REDCR* odešle příkaz (ECHO) příslušnému *DSRC-VU* a přidělí soukromé okno.

— Krok 7 *DSRC-VU* použije nově přidělené soukromé okno pro odeslání rámce odpovědi ECHO.

V následujících tabulkách je uveden praktický příklad výměnné relace ECHO.

DSC_56 Inicializace je provedena podle 5.4.7 (DSC_44 – DSC_48) a tabulek 14.4 – 14.9.

DSC_57 REDCR potom odešle příkaz ACTION, ECHO odpovídající ISO 14906 a obsahující 100 oktetů dat bez speciálního nastavení RTM. V tabulce 14.15 je uveden obsah rámce odeslaného REDCR.

Tabulka 14.15

Příklad rámce žádosti ACTION, ECHO

Octet #	Attribute/Field	Bits in octet	Description
1	FLAG	0111 1110	Start flag
2	Private LID	xxxx xxxx	Link address of the specific DSRC-VU
3		xxxx xxxx	

Octet #	Attribute/Field	Bits in octet	Description
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control field	1010 s000	Command PDU
7	LLC Control field	n111 0111	Polled ACn command, n bit
8	Fragmentation header	1xxx x001	No fragmentation
9	ACTION.request SEQUENCE {	0000	Action request (ECHO)
	OPTION indicator	0	Access Credentials not present
	OPTION indicator	1	Action parameter present
	OPTION indicator	0	IID not present
	Mode BOOLEAN	1	Response expected
10	EID INTEGER (0..127,…)	0000 0000	No extension, EID = 0 (System)
11	ActionType INTEGER (0..127,…)	0000 1111	No extension, Action type ECHO request
12	ActionParameter CONTAINER {	0000 0010	No extension, Container Choice = 2
13		0110 0100	No extension. String length = 100 octets
14		xxxx xxxx	Data to be echoed
…		…	
113	}}	xxxx xxxx	
114	FCS	xxxx xxxx	Frame check sequence
115		xxxx xxxx	
116	Flag	0111 1110	End Flag

DSC_58 Při přijímání žádosti ECHO odešle *DSRC-VU* odpověď ECHO o 100 oktetech dat a reaguje na přijatý příkaz v souladu s ISO 14906 bez speciálního nastavení pro RTM. Tabulka 14.16 uvádí příklad šifrování na úrovni bitů.

Tabulka 14.16

Příklad rámce odpovědi ACTION, ECHO

Octet #	Attribute/Field	Bits in octet	Description
1	FLAG	0111 1110	Start flag
2	Private LID	xxxx xxxx	Link address of the specific VU
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control field	1101 0000	Response PDU
7	LLC Control field	n111 0111	ACn command n bit
8	LLC status field	0000 0000	Response available
9	Fragmentation header	1xxx x001	No fragmentation
10	ACTION.response SEQUENCE {	0001	ACTION response (ECHO)
	OPTION indicator	0	IID not present
	OPTION indicator	1	Response parameter present
	OPTION indicator	0	Return status not present
	Fill BIT STRING (SIZE (1))	0	Not used
11	EID INTEGER (0..127,…)	0000 0000	No extension, EID = 0 (System)
12	ResponseParameter CONTAINER {	0000 0010	No extension, Container Choice = 2
13		0110 0100	No extension. String length = 100 octets
14		xxxx xxxx	Echoed data
…		…	
113	}}	xxxx xxxx	
114	FCS	xxxx xxxx	Frame check sequence
115		xxxx xxxx	
116	Flag	0111 1110	End Flag

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.

5.5.2 *Příkazy*

DSC_60 Příkazy používané pro transakci OWS jsou stejné jako příkazy používané pro transakci RTM.

5.5.3 *Pořadí dotazovacích příkazů*

DSC_61 Pořadí dotazovacích příkazů pro data OWS je stejné jako pro data RTM.

5.5.4 *Struktury dat*

DSC_62 Přenášená data (data OWS) obsahují řetězec

1. dat EncryptedOwsPayload, která jsou šifrováním OwsPayload podle ASN.1 v části 5.5.5. Způsob šifrování je stejný jako pro RtmData, který je uveden v dodatku 11;

2. DSRCSecurityData, vypočítaných se stejným algoritmem jako pro RTMData, který je uveden v dodatku 11.

5.5.5 *Modul ASN.1 pro transakci OWS DSRC*

DSC_63. Definice modulu ASN.1 pro data DSRC v aplikaci RTM je určena takto:

```
   TarvOws {iso(1) standard(0) 15638 part20(20)
   version1(1)} DEFINITIONS AUTOMATIC TAGS
   ::= BEGIN
   IMPORTS
   -- Imports data attributes and elements from EFC which are used for OWS
   LPN
   FROM EfcDsrcApplication {iso(1) standard(0) 14906 application(0) version5(5)}

   -- Imports function parameters from the EFC Application Interface Definition
   SetMMIRq
   FROM EfcDsrcApplication {iso(1) standard(0) 14906 application(0) version5(5)}

   -- Imports the L7 DSRCData module data from the EFC Application Interface Definition
   Action-Request, Action-Response, ActionType, ApplicationList, AttributeIdList, AttributeList,
   Attributes,
   BeaconID, BST, Dsrc-EID, DSRCApplicationEntityID, Event-Report-Request, Event-Report- Response,
   EventType, Get-Request, Get-Response, Initialisation-Request, Initialisation-Response,
   ObeConfiguration, Profile, ReturnStatus, Time, T-APDUs, VST
   FROM EfcDsrcGeneric {iso(1) standard(0) 14906 generic(1) version5(5)};

   -- Definitions of the OWS functions:
   OWS-InitialiseComm-Request ::= BST
   OWS-InitialiseComm-Response::= VST
   OWS-DataRetrieval-Request::= Get-Request (WITH COMPONENTS {fill (SIZE(1)), eid, accessCredentials
   ABSENT, iid ABSENT, attrIdList})
   OWS-DataRetrieval-Response::= Get-Response {OwsContainer} (WITH COMPONENTS {..., eid, iid ABSENT})
   OWS-TerminateComm::= Event-Report-Request {OwsContainer}(WITH COMPONENTS {mode (FALSE), eid (0),
   eventType (0)})
   OWS-TestComm-Request::= Action-Request {OwsContainer} (WITH COMPONENTS {..., eid (0), actionType
   (15), accessCredentials ABSENT, iid ABSENT})
   OWS-TestComm-Response::= Action-Response {OwsContainer} (WITH COMPONENTS {..., fill (SIZE(1)), eid
   (0), iid ABSENT})

   -- Definitions of the OWS attributes:
   OwsData :: = SEQUENCE {
        encryptedOwsPayload OCTET STRING (SIZE(51)) (CONSTRAINED BY { -- calculated encrypting
   OwsPayload as per Appendix 11 --}),
        DSRCSecurityData OCTET STRING
        }
   OwsPayload :: = SEQUENCE {
              tp15638VehicleRegistrationPlate LPN -- Vehicle Registration Plate as per EN 15509.
              recordedWeight INTEGER (0..65535),           -- 0= Total measured weight of the  heavy
   goods vehicle                                                          -- with 10 Kg
   resolution.
              axlesConfiguration OCTET STRING SIZE (3),     -- 0= 20 bits allowed for the number
                                                                  -- of axles for 10 axles.
              axlesRecordedWeight OCTET STRING SIZE (20),   -- 0= Recorded Weight for each axle
                                                                -- with 10 Kg resolution.
              tp15638Timestamp              INTEGER(0..4294967295)      -- Timestamp of current record
        }

Ows-ContextMark ::= SEQUENCE {
  standardIdentifier    StandardIdentifier, -- identifier of the TARV part and its version
        }

StandardIdentifier ::= OBJECT IDENTIFIER
  OwsContainer ::= CHOICE {
        integer                       [0]    INTEGER,
        bitstring                     [1]    BIT STRING,
        octetstring                   [2]    OCTET STRING (SIZE (0..127, ...)),
        universalString               [3]    UniversalString,
        beaconId                      [4]    BeaconID,
        t-apdu                        [5]    T-APDUs,
        dsrcApplicationEntityId       [6]    DSRCApplicationEntityID,
        dsrc-Ase-Id                   [7]    Dsrc-EID,
        attrIdList                    [8]    AttributeIdList,
        attrList                      [9]    AttributeList{RtmContainer},
        reserved10                    [10]   NULL,
        OwsContextmark                [11]   Ows-ContextMark,
        OwsData                       [12]   OwsData,
        reserved13                    [13]   NULL,
        reserved14                    [14]   NULL,
        time                          [15]   Time,
-- values from 16 to 255 reserved for ISO/CEN usage
        }}

END
```

5.5.6 *Prvky OwsData, provedené akce a definice*

Prvky OwsData jsou určeny na podporu směrnice (EU) 2015/719 o maximálních hmotnostech a rozměrech těžkých nákladních vozidel. Mají tento význam:

— recordedWeight znamená celkovou naměřenou hmotnost nákladního vozidla s rozlišením 10 kg podle EN ISO 14906. Například hodnota 2 500 znamená celkovou hmotnost 25 tun.

— axlesConfiguration znamená konfiguraci těžkého nákladního vozidla podle počtu náprav. Konfigurace je definována pomocí bitové masky 20 bitů (rozšíření z EN ISO 14906).

Bitová maska 2 bitů znamená konfiguraci nápravy v následujícím formátu:

— hodnota 00B znamená, že hodnota „není dostupná“, protože vozidlo nemá zařízení na měření váhy na nápravě,

— hodnota 01B znamená, že náprava není dostupná,

— hodnota 10B znamená, že náprava je dostupná a váha byla vypočítána a naměřena a je udávána v poli axlesRecordedWeight,

— hodnota 11B je vyhrazena pro budoucí použití.

Poslední čtyři bity jsou vyhrazeny pro budoucí použití.

Počet náprav										
Počet náprav na tažné jednotce			Počet náprav na přívěsu							
00/01/10/11	00/01/10/11	00/01/10/11	00/01/10/11	00/01/10/11	00/01/10/11	00/01/10/11	00/01/10/11	00/01/10/11	00/01/10/11	RFU (4 bity)

— axlesRecordedWeight znamená specifickou hmotnost zaznamenanou pro každou nápravu s rozlišením 10 kg. Pro každou nápravu se použijí dva oktety. Například hodnota 150 znamená hmotnost 1 500 kg.

Další druhy dat jsou definovány v 5.4.5.

5.5.7 *Mechanismus přenosu dat*

DSC_64 Mechanismus přenosu dat pro data OWS mezi dotazovacím zařízením a zařízením DSRC ve vozidle je stejný jako pro data RTM (viz 5.4.6).

DSC_65 Přenos dat mezi platformou shromažďující data maximální hmotnosti a zařízením DSRC ve vozidle je založen na fyzickém spojení a rozhraních a protokolu stanoveném v části 5.6.

5.6 **Přenos dat mezi DSRC-VU a VU**

5.6.1 *Fyzické spojení a rozhraní*

DSC_66 Spojení mezi *VU* a *DSRC-VU* může být provedeno buď fyzickým kabelem, nebo bezdrátovou komunikací krátkého dosahu na bázi Bluetooth v4.0 BLE.

DSC_67 Bez ohledu na volbu fyzického spojení a rozhraní jsou splněny tyto požadavky:

DSC_68 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 otevřeným standardním spojením. VU se s DSRC-VU spojuje buď

i) pomocí pevného kabelu délky nejméně 2 metry s přímým konektorem DIN 41612 H11 – schválenou zástrčkou na straně DSRC-VU s 11 kolíky a odpovídající zásuvkou se schválením DIN/ISO na straně VU,

ii) pomocí zařízení Bluetooth Low Energy (BLE)

iii) pomocí standardního spojení ISO 11898 nebo SAE J1939

DSC_69 b) Definice rozhraní a spojení mezi VU a DSRC-VU musí podporovat příkazy protokolu aplikace stanovené v 5.6.2. a

DSC_70 c) VU a DSRC-VU musí podporovat přenos dat prostřednictvím spojení s ohledem na výkon a napájení.

5.6.2 *Protokol aplikace*

DSC_71 Protokol aplikace mezi zařízením vzdálené komunikace VU a DSRC-VU je odpovědný za pravidelný přenos dat vzdálené komunikace z VU do DSRC.

DSC_72 Jsou určeny tyto hlavní příkazy:

1. 1. Inicializace komunikačního spojení – žádost
2. Inicializace komunikačního spojení – odpověď
3. Odeslání dat s identifikátorem aplikace RTM a přenášená data podle dat RTM
4. Potvrzení dat
5. Ukončení komunikačního spojení – žádost
6. Ukončení komunikačního spojení – odpověď

DSC_73 V ASN1.0 mohou být předchozí příkazy definovány takto:

```
Remote Communication DT Protocol DEFINITIONS ::= BEGIN

     RCDT-Communication Link Initialization - Request ::= SEQUENCE {
          LinkIdentifier INTEGER
     }

     RCDT-Communication Link Initialization - Response::= SEQUENCE {
          LinkIdentifier INTEGER,
          answer         BOOLEAN
     }

          RCDT- Send Data ::=
          SEQUENCE { LinkIdentifier
          INTEGER, DataTransactionId
          INTEGER, RCDTData
          SignedTachographPayload
     }

          RCDT Data Acknowledgment ::
          SEQUENCE { LinkIdentifier
          INTEGER, DataTransactionId
          INTEGER,
          answer         BOOLEAN
     }

          RCDT-Communication Link Termination - Request ::= SEQUENCE {
          LinkIdentifier INTEGER
     }

          RCDT-Communication Link Termination - Response::= SEQUENCE {
          LinkIdentifier INTEGER,
          answer         BOOLEAN
     }

End
```

DSC_74 Popis příkazů a parametrů:

— RCDT-Communication Link Initialization – Request se používá pro inicializaci komunikačního spojení. Příkaz je odeslán z VU do DSRC-VU. VU stanoví LinkIdentifier a sdělí jej DSRC-VU pro vytvoření specifického komunikačního spojení.

(Pozn.: slouží k podpoře budoucích spojení a dalších aplikací/modulů jako např. vážení na palubě).

— RCDT-Communication Link Initialization – Response používá DSRC-VU pro odeslání odpovědi na žádost o inicializaci komunikačního spojení. Příkaz odešle DSRC-VU do VU. Příkaz poskytuje výsledek inicializace jako odpověď = 1 (úspěch) nebo = 0 (selhání).

DSC_75 Inicializace komunikačního spojení se provádí po instalaci, kalibraci a spuštění motoru/VU.

— RCDT-Send Data používá VU pro odeslání podepsaných RCDTData (tj. *dat vzdálené komunikace*) do DSRC-VU. Data jsou odesílána každých 60 sekund. Parametr DataTransactionId označuje specifický přenos dat. LinkIdentifier rovněž zajišťuje správnost příslušného odkazu.

— RCDT-Data Acknowledgment odesílá DSRC-VU jako zpětnou vazbu do VU po přijetí dat z příkazu RCDT-Send Data označeného parametrem DataTransactionId. Parametr odpovědi je 1 (úspěch) nebo = 0 (selhání). Pokud VU přijme víc než tři odpovědi odpovídající 0 nebo pokud VU nepřijme pro specifický dříve odeslaný příkaz se specifickým DataTransactionId, VU generuje a zaznamená událost.

— RCDT-Communication Link Termination request odesílá VU do DSRC-VU pro ukončení spojení pro specifický LinkIdentifier.

DSC_76 Při novém spuštění DSRC-VU nebo VU by všechny stávající komunikační odkazy měly být odstraněny, protože se mohou vyskytovat „zbytkové“ odkazy v důsledku neočekávaného vypnutí VU.

— RCDT-Communication Link Termination – Response odesílá DSRC-VU do VU pro potvrzení žádosti o ukončení spojení ze strany VU pro specifický LinkIdentifier.

5.7 **Řešení chyb**

5.7.1 *Záznamy a komunikace dat v DSRC-VU*

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 '62'H Chyba komunikace zařízení vzdálené komunikace s časovým razítkem.

DSC_78 *VU* uchovává soubor označený jedinečným názvem, který mohou pracovníci kontroly snadno identifikovat pro účely zaznamenání„poruchy interní komunikace VU“.

DSC_79 Pokud se VUPM neúspěšně pokusí získat data VU z bezpečnostního modulu (pro předání do VU-DSRC), zaznamená toto selhání s typem EventFaultType a hodnotou enum nastavenou na *'62'H* Chyba komunikace *zařízení vzdálené komunikace* s časovým razítkem. Selhání komunikace je zjištěno, není-li zpráva RCDT Data Acknowledgment pro příslušný příkaz (tj. se stejnými zprávami DataTransactionId v Send Data a Acknowledgment) RCDT Send Data přijata déle než během tří následných pokusů.

5.7.2 *Chyby bezdrátové komunikace*

DSC_80 Řešení chyb komunikace odpovídá ustanovením příslušných norem DSRC, konkrétně EN 300 674-1, EN 12253, EN 12795, EN 12834 a příslušným parametrům EN 13372.

5.7.2.1 *Chyby šifrování a podpisu*

DSC_81 Chyby šifrování a podpisu se řeší v souladu s dodatkem 11 Společné bezpečnostní mechanismy a nejsou přítomné v žádných chybových hlášeních spojených s přenosem dat DSRC.

5.7.2.2 *Záznam chyb*

Médium DSRC je dynamická bezdrátová komunikace v prostředí nejistých atmosférických a interferenčních podmínek, zejména v kombinacích „přenosné REDCR“ a „pohybující se vozidlo“ v rámci této aplikace. Je proto třeba uvědomit si rozdíl mezi „chybou čtení“ a „chybovými“ podmínkami. Při přenosu prostřednictvím bezdrátového rozhraní je chyba čtení běžná a důsledkem je obvykle nový pokus, tj. nová relace BST a nový pokus o sekvenci, které ve většině případů vedou k úspěšnému komunikačnímu spojení a přenosu dat, pokud se cílové vozidlo během času potřebného pro nový přenos nedostane z dosahu. („Úspěšný“ případ „čtení“ může zahrnovat několik pokusů a nových spojení.)

Chyba čtení může být důsledkem nesprávného spárování antén (chyba „zaměření“); zastínění jedné z antén – může být úmyslné, ale rovněž důsledkem fyzické přítomnosti jiného vozidla; rádiové interference, zejména zařízení WIFI v pásmu cca 5,8 GHz nebo jiných veřejně přístupných bezdrátových komunikací nebo může být způsobeno radarovou interferencí nebo nepříznivými atmosférickými podmínkami (např. za bouřky); nebo jednoduše vyjetím z dosahu komunikace DSRC. Jednotlivé případy chyb čtení nelze z jejich povahy zaznamenat, protože komunikace nebyla prostě navázána.

Pokud však oprávněná osoba příslušných kontrolních orgánů zaměří vozidlo a pokusí se zjistit jeho *DSRC-VU*, ale nedojde k úspěšnému přenosu dat, může k tomuto selhání dojít v důsledku úmyslné manipulace, a proto musí mít oprávněná osoba příslušných kontrolních orgánů k dispozici prostředek pro zaznamenání selhání a upozornění kolegů na cestě o možné manipulaci. Kolegové potom mohou zastavit vozidlo a provést fyzickou kontrolu. Pokud však není úspěšně navázána komunikace, systém DSRC-VU nemůže poskytnout data týkající se selhání. Podávání těchto zpráv je proto funkcí konstrukce zařízení REDCR.

„Selhání čtení“ je technicky odlišné od „chyby“. V této souvislosti je „chyba“ přijetí špatné hodnoty.

Přenos dat do *DSRC-VU* je realizován již v zabezpečené podobě, proto musí být ověřen poskytovatelem dat (viz 5.4).

Data následně přenášená vzdušným rozhraním se kontrolují cyklickými redundantními kontrolami na komunikační úrovni. Je-li CRC úspěšná, jsou data správná. Není-li CRC úspěšná, jsou data přenášena znovu. Pravděpodobnost, že by nesprávná data mohla úspěšně projít CRC, je statisticky tak nízká, že může být zanedbána.

Není-li validace CRC úspěšná a není čas pro nový přenos a přijetí správných dat, nebude výsledkem chyba, ale případ specifického typu selhání čtení.

Jediné smysluplné „selhání“ dat, které může být zaznamenáno, je chyba počtu úspěšných inicializací transakcí, které nevedou k úspěšnému přenosu dat do REDCR.

DSC_82 REDCR proto zaznamenává počet časově označených případů, kdy je „inicializační“ fáze sledování DSRC úspěšná, ale transakce je ukončena před úspěšným přijetím *dat* v REDCR. Tato data jsou k dispozici oprávněné osobě příslušných kontrolních orgánů a jsou uložena v paměti zařízení REDCR. Způsob, jakým je toho dosaženo, je záležitostí konstrukce výrobku nebo specifikace příslušného kontrolního orgánu.

Jedinými smysluplnými „chybnými“ daty, která mohou být zaznamenána, je počet případů, kdy REDCR nedokáže dešifrovat přijatá *data*. Je však třeba zmínit, že tyto případy souvisejí pouze s účinností softwaru REDCR. Data mohou být technicky dešifrována, ale nedávají sémantický smysl.

DSC_83 *REDCR* proto zaznamenává počet časově označených případů, kdy se neúspěšně pokusilo dešifrovat data přijatá přes rozhraní DSRC.

6 UVEDENÍ DO PROVOZU A PRAVIDELNÉ KONTROLNÍ TESTY PRO FUNKCE DÁLKOVÉ KOMUNIKACE OBECNÉ INFORMACE

6.1 **Obecné informace**

DSC_84 Pro funkci dálkové komunikace jsou určeny dva typy testů:

1) Test ECHO pro posouzení bezdrátového komunikačního kanálu *DSRC-REDCR* >>-:-<*DSRC-VU*.
2) Koncový bezpečnostní test, který ověřuje, že je karta dílny schopna přístupu k šifrovanému a podepsanému datovému obsahu vytvořenému VU a přenášenému bezdrátovým komunikačním kanálem.

6.2 **ECHO**

Tento článek obsahuje ustanovení speciálně vytvořená pro testování funkční aktivity *DSRC-REDCR* >>-:-<*DSRC-VU*.

Cílem příkazu ECHO je umožnit dílnám nebo testovacím zařízením pro typové zkoušky testovat funkci spojení DSRC bez nutnosti přístupu k bezpečnostním údajům. Testovací zařízení proto musí být pouze schopno inicializovat komunikaci DSRC (odeslání BST s AID = 2) a potom odeslat příkaz ECHO a v případě, že DSRC pracuje, přijmout odezvu ECHO. Podrobnosti viz 5.4.8. V případě, že tuto odezvu přijme správně, může být spojení DSRC (*DSRC-REDCR* >>-:-<*DSRC-VU*) validováno jako správně fungující.

6.3 **Testy validace obsahu zabezpečených dat**

DSC_85 Tento test je určen pro validaci koncového bezpečnostního toku dat. Pro tento test je nutná testovací čtečka DSRC. Tato čtečka provádí stejné funkce a je realizována se stejnými specifikacemi jako čtečka používaná oprávněnými osobami s tím rozdílem, že karta dílny je používána pro ověření totožnosti uživatele testovací čtečky DSRC, nikoli kontrolní karty. Test lze provádět po počáteční aktivaci inteligentního tachografu nebo na konci kalibračního postupu. Po aktivaci celek ve vozidle generuje zabezpečená data včasné detekce a sdělí je zařízení dálkové komunikace.

DSC_86 Pracovníci dílny musí testovací čtečku DSRC umístit ve vzdálenosti 2 až 10 metrů před vozidlem.

DSC_87 Potom pracovníci dílny vloží do testovací čtečky DSRC kartu dílny a odešlou požadavek na zjištění dat včasné detekce do celku ve vozidle. Po úspěšném zjištění pracovníci dílny přijatá data zkontrolují, aby se přesvědčili, že byla úspěšně validována z hlediska integrity a dešifrována.

Dodatek 15

MIGRACE: POSTUPY PŘI SOUČASNÉ EXISTENCI NĚKOLIKA GENERACÍ ZAŘÍZENÍ

OBSAH

1. DEFINICE

Pro účely tohoto dodatku se použijí tyto definice:

systém inteligentního tachografu: podle definice v této příloze (kapitola 1: definice bbb);

systém tachografu první generace: podle definice v tomto nařízení (článek 2: definice 1);

systém tachografu druhé generace: podle definice v tomto nařízení (článek 2: definice 7);

datum zavedení: podle definice v této příloze (kapitola 1: definice ccc);

inteligentní vyhrazené zařízení (IDE): zařízení používané ke stahování dat podle definice v dodatku 7 této přílohy.

2. OBECNÁ USTANOVENÍ

2.1. **Přechod na novou generaci**

V preambuli této přílohy je uveden přehled o přechodu z první na druhou generaci systémů tachografů.

Kromě ustanovení této preambule:

— snímače pohybu první generace nebudou interoperabilní s celky ve vozidle druhé generace,

— instalace snímačů pohybu druhé generace do vozidel bude zahájena současně s instalací celků ve vozidle druhé generace,

— bude nutný další vývoj zařízení pro stahování dat a kalibrační zařízení, aby bylo podporováno používání obou generací záznamového zařízení a karet tachografu.

2.2. **Interoperabilita mezi celky ve vozidle a kartami**

Rozumí se, že karty tachografu první generace jsou interoperabilní s celky ve vozidle první generace (v souladu s přílohou 1B tohoto nařízení), zatímco karty tachografu druhé generace jsou interoperabilní s celky ve vozidle druhé generace (v souladu s přílohou 1C tohoto nařízení). Kromě toho se uplatní níže uvedené požadavky.

MIG_001 Kromě případů uvedených v požadavcích MIG_004 a MIG_005 mohou být karty tachografu první generace nadále používány v celcích ve vozidle druhé generace až do uplynutí jejich data platnosti. Jejich držitelé však mohou požádat o jejich výměnu za karty tachografu druhé generace, jakmile budou k dispozici.

MIG_002 Celky ve vozidle druhé generace musí být schopny používat jakoukoli platnou vloženou kartu řidiče, kontrolní kartu nebo kartu podniku první generace.

MIG_003 Tato schopnost může být jednou provždy v uvedeném celku ve vozidle dílnami odstraněna, takže karty tachografu první generace nemohou být již dále přijímány. To lze provést pouze poté, co Evropská komise zahájí postup, jehož cílem je dílny požádat, aby tak učinily, např. během každé periodické kontroly tachografu.

MIG_004 Celky ve vozidle druhé generace musí být schopny používat pouze karty dílny druhé generace.

MIG_005 Pro určení provozního režimu musí celky ve vozidle druhé generace přihlížet pouze k typům platných vložených karet bez ohledu na jejich generace.

MIG_006 Jakoukoli platnou kartu tachografu druhé generace musí být možné použít v celcích ve vozidle první generace naprosto stejným způsobem jako kartu tachografu první generace stejného typu.

2.3. **Interoperabilita mezi celky ve vozidle a snímači pohybu**

Rozumí se, že snímače pohybu první generace jsou interoperabilní s první generací celků ve vozidle, zatímco snímače pohybu druhé generace jsou interoperabilní s druhou generací celků ve vozidle. Kromě toho se uplatní níže uvedené požadavky.

MIG_007 Celky ve vozidle druhé generace nebudou moci být spárovány a používány se snímači pohybu první generace.

MIG_008 Snímače pohybu druhé generace mohou být spárovány a používány pouze s celky ve vozidle druhé generace, nebo s oběma generacemi celků ve vozidle.

2.4. **Interoperabilita mezi celky ve vozidle, kartami tachografu a zařízením pro stahování dat**

MIG_009 Zařízení pro stahování dat lze používat pouze s jednou generací celků ve vozidle a karet tachografu, nebo s oběma.

2.4.1 *Přímé stahování z karet prostřednictvím inteligentního vyhrazeného zařízení (IDE)*

MIG_010 Data se musí z karet tachografu jedné generace vložených do čtečky karet stahovat pomocí IDE s použitím bezpečnostních mechanismů a protokolu pro stahování dat této generace a stahovaná data musí být ve formátu definovaném pro tuto generaci.

MIG_011 Aby se umožnila kontrola řidičů kontrolními orgány, které nepatří do EU, musí být rovněž umožněno stahování dat z karty řidiče (a karty dílny) druhé generace naprosto stejným způsobem jako z karty řidiče (a karty dílny) první generace. Uvedené stahování musí zahrnovat:

— nepodepsané elementární soubory (EF) `IC` a `ICC`,

— nepodepsané elementární soubory (EF) (první generace) `Card_Certificate` a `CA_Certificate`,

— ostatní elementární soubory EF s aplikačními daty (v rámci souboru TACHO DF) 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 TACHO_G2 DF).

2.4.2 *Stahování z karet prostřednictvím celku ve vozidle*

MIG_012 Data se musí stahovat z karty druhé generace vložené do celku ve vozidle první generace pomocí protokolu pro stahování dat první generace. Karta musí na příkazy celku ve vozidle odpovídat naprosto stejným způsobem jako karta první generace a stahovaná data musí mít stejný formát jako data stahovaná z karty první generace.

MIG_013 Data se musí stahovat z karty první generace vložené do celku ve vozidle druhé generace pomocí protokolu pro stahování dat definovaného v dodatku 7 této přílohy. Celek ve vozidle musí vysílat příkazy do karty naprosto stejným způsobem jako celek ve vozidle první generace a stahovaná data musí respektovat formát definovaný pro karty první generace.

2.4.3 *Stahování z celku ve vozidle*

MIG_014 Data se 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, a stahování dat z celku ve vozidle dílnami, které nepatří do EU, lze také volitelně umožnit stahování dat z celků ve vozidle druhé generace pomocí bezpečnostních mechanismů první generace a protokolu pro stahování dat první generace. Stahovaná data musí mít stejný formát jako data stahovaná z celku ve vozidle první generace. Tuto možnost lze zvolit pomocí příkazů v menu.

2.5. **Interoperabilita mezi celkem ve vozidle a kalibračním zařízením**

MIG_016 Kalibrační zařízení musí být schopno provádět kalibraci všech generací tachografu pomocí kalibračního protokolu příslušné generace. Kalibrační zařízení lze použít pouze s jednou generací tachografu, nebo s oběma.

3. HLAVNÍ KROKY V OBDOBÍ PŘED DATEM ZAVEDENÍ

MIG_017 Testovací klíče a certifikáty musí být výrobcům k dispozici nejpozději **30 měsíců** před datem zavedení.

MIG_018 Zkoušky interoperability musí být připraveny k zahájení, jestliže o to výrobci požádají, nejpozději **15 měsíců** před datem zavedení.

MIG_019 Oficiální klíče a certifikáty musí být výrobcům k dispozici nejpozději **12 měsíců** před datem zavedení.

MIG_020 Členské státy musí být schopny vydávat karty dílny druhé generace nejpozději **3 měsíce** před datem zavedení.

MIG_021 Členské státy musí být schopny vydávat všechny typy karet tachografu druhé generace nejpozději **1 měsíc** před datem zavedení.

4. USTANOVENÍ PRO OBDOBÍ PO DATU ZAVEDENÍ

MIG_022 Po datu zavedení musí členské státy vydávat pouze karty tachografu druhé generace.

MIG_023 Výrobci celků ve vozidle / snímačů pohybu budou smět vyrábět celky ve vozidle / snímače pohybu první generace, dokud budou používány v praxi, aby mohly být vyměňovány vadné součásti.

MIG_024 Výrobci celků ve vozidle / snímačů pohybu budou smět požadovat a obdržet zachování schválení typu celků ve vozidle / snímačů pohybu první generace, které již byly typově schváleny.

Dodatek 16

ADAPTÉR PRO VOZIDLA KATEGORIE M1 A N1

OBSAH

1. ZKRATKY A REFERENČNÍ DOKUMENTY

1.1. **Zkratky**

TBD bude stanoveno později

VU celek ve vozidle (*Vehicle Unit*)

1.2. **Referenční normy**

ISO16844-3 Road vehicles – Tachograph systems – Part 3: Motion sensor interface (Silniční vozidla – Systémy tachografu – Část 3: Rozhraní snímače pohybu

2. VŠEOBECNÉ CHARAKTERISTIKY A FUNKCE ADAPTÉRU

2.1. **Všeobecný popis adaptéru**

ADA_001 Adaptér dodává připojenému celku ve vozidle (VU) zabezpečené údaje o pohybu vozidla trvale odpovídající rychlosti vozidla a vzdálenosti ujeté vozidlem.

Adaptér je určen pouze pro vozidla, která musí být vybavena záznamovým zařízením v souladu s tímto nařízením.

Musí být namontován a používán pouze u typů vozidel vymezených v definici yy) „adaptér" přílohy IC, u kterých není mechanicky možné namontovat jiný typ existujícího snímače pohybu, který je jinak v souladu s ustanoveními této přílohy a dodatků 1 až 16.

Adaptér nesmí být mechanicky propojen s pohyblivou částí vozidla, ale je napojen na impulsy rychlosti/vzdálenosti, které jsou generovány integrovanými snímači nebo alternativními rozhraními.

ADA_002 Snímač pohybu schváleného typu (podle ustanovení této přílohy IC oddílu 8, Schválení typu záznamového zařízení a karet tachografu) musí být umístěn do skříně adaptéru, která musí obsahovat také zařízení na převod impulsů indukující přicházející impulsy do zabudovaného snímače pohybu. Vlastní zabudovaný snímač pohybu musí být propojen s celkem ve vozidle tak, aby rozhraní mezi celkem ve vozidle a adaptérem bylo v souladu s požadavky normy ISO 16844-3.

2.2. **Funkce**

ADA_003 Adaptér musí zajišťovat tyto funkce:

— propojení a přizpůsobování příchozích impulsů rychlosti,

— indukci přicházejících impulsů do zabudovaného snímače rychlosti,

— všechny funkce zabudovaného snímače pohybu dodávající zabezpečené údaje o pohybu vozidla do celku ve vozidle.

2.3. **Zabezpečení**

ADA_004 Zabezpečení systému adaptéru není certifikováno na základě všeobecného bezpečnostního cíle pro snímače pohybu definovaného v dodatku 10 této přílohy. Namísto toho se použijí požadavky na zabezpečení specifikované v oddíle 4.4 tohoto dodatku.

3. POŽADAVKY NA ZÁZNAMOVÉ ZAŘÍZENÍ U NAMONTOVANÉHO ADAPTÉRU

Požadavky uvedené v následujících kapitolách udávají, jak je třeba rozumět požadavkům v této příloze, je-li použit adaptér. Příslušná čísla požadavků přílohy IC jsou uvedena v závorkách.

ADA_005 Záznamové zařízení každého vozidla vybaveného adaptérem musí být v souladu se všemi ustanoveními této přílohy kromě případů, kdy je v tomto dodatku uvedeno jinak.

ADA_006 Je-li namontován adaptér, záznamové zařízení zahrnuje kabely, adaptér (včetně snímače pohybu) a celek ve vozidle [01].

ADA_007 Funkce detekce událostí a/nebo závad záznamového zařízení se pozměňuje takto:

— událost „přerušení elektrického napájení" aktivuje celek ve vozidle, pokud zařízení není v kalibračním režimu, při každém přerušení elektrického napájení zabudovaného snímače pohybu delším než 200 milisekund [79],

— událost „chybné údaje o pohybu vozidla" aktivuje celek ve vozidle při přerušení normálního toku dat mezi zabudovaným snímačem pohybu a celkem ve vozidle a/nebo v případě chyby integrity nebo ověření pravosti dat přenášených mezi zabudovaným snímačem pohybu a celkem ve vozidle [83],

— událost „pokus o narušení zabezpečení“ aktivuje celek ve vozidle v jakémkoli jiném případě, který ohrožuje zabezpečení zabudovaného snímače pohybu, pokud zařízení není v kalibračním režimu [85],

— chybu „záznamového zařízení“ aktivuje celek ve vozidle, pokud zařízení není v kalibračním režimu, v případě jakékoliv závady na zabudovaném snímači pohybu [88].

ADA_008 Závady adaptéru zjistitelné záznamovým zařízením jsou závady související se zabudovaným snímačem pohybu [88].

ADA_009 Kalibrační funkce celku ve vozidle musí umožnit automatické spárování zabudovaného snímače pohybu a celku ve vozidle [202, 204].

4. KONSTRUKČNÍ A FUNKČNÍ POŽADAVKY NA ADAPTÉR

4.1. **Propojení a přizpůsobení přicházejících impulsů rychlosti**

ADA_011 Vstupní rozhraní adaptéru musí přijímat frekvenční impulsy odpovídající rychlosti vozidla a vzdálenosti ujeté vozidlem. Elektrické charakteristiky přicházejících impulsů jsou: *definuje výrobce*. Úpravy přístupné pouze výrobci adaptéru a schválené dílně provádějící montáž adaptéru musí v příslušných případech umožnit správné propojení vstupu adaptéru s vozidlem.

ADA_012 Vstupní rozhraní adaptéru musí být v příslušných případech schopné násobit nebo dělit frekvenci přicházejících impulsů rychlosti pevně stanoveným faktorem pro přizpůsobení signálu rozsahu faktoru k definovanému v této příloze (4 000 až 25 000 impulsů/km). Tento pevně stanovený faktor může být naprogramován pouze výrobcem adaptéru a schválenou dílnou provádějící montáž adaptéru.

4.2. **Indukce přicházejících impulsů do zabudovaného snímače pohybu**

ADA_013 Přicházející impulsy, případně přizpůsobené výše uvedeným způsobem, musí být indukovány do zabudovaného snímače pohybu tak, aby každý přicházející impuls byl snímačem pohybu detekován.

4.3. **Zabudovaný snímač pohybu**

ADA_014 Zabudovaný snímač pohybu musí být stimulován indukovanými impulsy, což mu umožní generovat údaje o pohybu vozidla přesně odpovídající pohybu vozidla, jako by byl mechanicky propojen s pohyblivou částí vozidla.

ADA_015 K identifikaci adaptéru využívá celek ve vozidle identifikační data zabudovaného snímače pohybu [95].

ADA_016 Montážní data uložená v zabudovaném snímači pohybu jsou považována za data představující montážní data adaptéru [122].

4.4. **Bezpečnostní požadavky**

ADA_017 Skříň adaptéru musí být konstruována tak, aby ji nebylo možno otevřít. Musí být opatřena plombou, aby bylo možné snadno zjistit pokusy o nepovolenou manipulaci (např. vizuální kontrolou, viz ADA_035). Plomby musí splňovat stejné požadavky jako plomby na snímačích pohybu [398 až 406].

ADA_018 Nesmí být možné odstranit zabudovaný snímač pohybu z adaptéru bez porušení plomby (plomb) skříně adaptéru nebo porušení plomby mezi snímačem a skříní adaptéru (viz ADA_034).

ADA_019 Adaptér musí zajistit, aby údaje o pohybu vozidla mohly být zpracovávány a odvozovány pouze ze vstupu adaptéru.

4.5. **Provozní charakteristiky**

ADA_020 Adaptér musí být plně provozuschopný v rozsahu teplot definovaném výrobcem.

ADA_021 Adaptér musí být plně provozuschopný v rozsahu vlhkostí od 10 % do 90 % [214].

ADA_022 Adaptér musí být chráněn proti přepětí, záměně polarity napájecího napětí a zkratu [216].

ADA_023 Adaptér musí buď:

— reagovat na magnetické pole, které ruší detekci pohybu vozidla; za takových okolností celek ve vozidle zaznamená a uloží závadu snímače [88]; nebo

— musí mít snímací prvek, který je chráněn proti magnetickým polím, případně je vůči jejich působení imunní [217].

ADA_024 Adaptér musí odpovídat mezinárodnímu předpisu EHK OSN R10, vztahujícímu se k elektromagnetické kompatibilitě, a musí být chráněn proti elektrostatickým výbojům a přechodovým jevům [218].

4.6. **Materiály**

ADA_025 Adaptér musí splňovat stupeň ochrany (*definují výrobci v závislosti na montážní poloze*) [220, 221].

ADA_026 Barva skříně adaptéru je žlutá.

4.7. **Značení**

ADA_027 K adaptéru musí být připevněn popisný štítek, který obsahuje tyto údaje:

— název a adresu výrobce adaptéru,

— katalogové číslo adaptéru podle výrobce a rok jeho výroby,

— značku schválení typu adaptéru nebo záznamového zařízení zahrnujícího adaptér,

— datum montáže adaptéru,

— identifikační číslo vozidla, do něhož byl namontován.

ADA_028 Popisný štítek dále obsahuje tyto údaje (pokud je není možno přímo přečíst na vnější straně zabudovaného snímače pohybu):

— název výrobce zabudovaného snímače pohybu,

— katalogové číslo zabudovaného snímače pohybu podle výrobce a rok jeho výroby,

— značka schválení typu zabudovaného snímače pohybu.

5. MONTÁŽ ZÁZNAMOVÉHO ZAŘÍZENÍ PŘI POUŽITÍ ADAPTÉRU

5.1. **Montáž**

ADA_029 Adaptéry musí být do vozidel montovány pouze výrobci vozidel nebo schválenými dílnami oprávněnými k montáži, aktivaci a kalibraci digitálních a inteligentních tachografů.

ADA_030 Schválená dílna provádějící montáž adaptéru musí seřídit vstupní rozhraní a zvolit dělicí poměr vstupního signálu (v příslušných případech).

ADA_031 Schválená dílna provádějící montáž adaptéru musí skříň adaptéru zaplombovat.

ADA_032 Adaptér musí být namontován co možná nejblíže té části vozidla, která zajišťuje přicházející impulsy.

ADA_033 Kabely pro přívod energie do adaptéru musí být červené (kladný pól) a černé (uzemnění).

5.2. **Plomby**

ADA_034 Platí tyto požadavky na plombování:

— skříň adaptéru musí být zaplombovaná (viz ADA_017),

— jestliže je možné odstranit zabudovaný snímač ze skříně adaptéru bez poškození plomby (plomb) skříně adaptéru, musí být skříň zabudovaného snímače plombou spojena se skříní adaptéru (viz ADA_018),

— skříň adaptéru musí být plombou spojena s vozidlem,

— propojení adaptéru a zařízení, které zajišťuje přicházející impulsy, musí být zaplombováno na obou koncích (pokud je to přiměřeně možné).

6. KONTROLY, PROHLÍDKY A OPRAVY

6.1. **Periodické prohlídky**

ADA_035 Při použití adaptéru musí každá pravidelná prohlídka (pravidelnou prohlídkou se rozumí prohlídka v souladu s požadavky [409] až [413] přílohy 1C) záznamového zařízení zahrnovat kontroly, zda:

— adaptér nese správnou značku schválení typu,

— plomby na adaptéru a jeho připojeních jsou neporušené,

— adaptér je namontován tak, jak je uvedeno na montážním štítku,

— adaptér je namontován podle pokynů výrobce adaptéru a/nebo vozidla,

— montáž adaptéru je pro kontrolované vozidlo schválená.

ADA_036 Tyto prohlídky musí zahrnovat kalibraci a výměnu všech plomb bez ohledu na jejich stav.

7. SCHVÁLENÍ TYPU ZÁZNAMOVÉHO ZAŘÍZENÍ PŘI POUŽITÍ ADAPTÉRU

7.1. **Všeobecně**

ADA_037 Záznamové zařízení musí být předloženo ke schválení typu úplné, včetně adaptéru [425].

ADA_038 Každý adaptér může být předložen ke schválení typu samostatně nebo jako součást záznamového zařízení.

ADA_039 Uvedené schválení typu musí zahrnovat funkční zkoušky zahrnující adaptér. Kladné výsledky každé z těchto zkoušek jsou uvedeny v příslušném osvědčení [426].

7.2. **Osvědčení o funkčnosti**

ADA_040 Osvědčení o funkčnosti adaptéru nebo záznamového zařízení zahrnujícího adaptér musí být výrobci adaptéru doručeno až po úspěšném absolvování všech funkčních zkoušek v tomto minimálním rozsahu.

Č.	Zkouška	Popis	Související požadavky
1.	**Administrativní šetření**		
1.1	Dokumentace	Správnost dokumentace adaptéru	
2.	**Vizuální kontrola**		
2.1.	Shoda adaptéru s dokumentací		
2.2.	Identifikace/značení adaptéru		ADA_027, ADA_028
2.3	Materiály použité v adaptéru		[219] až [223] ADA_026
2.4.	Plomby		ADA_017, ADA_018, ADA_034
3.	**Funkční zkoušky**		
3.1	Indukce impulsů rychlosti do zabudovaného snímače pohybu		ADA_013
3.2	Propojení a přizpůsobení přicházejících impulsů rychlosti		ADA_011, ADA_012
3.3	Přesnost měření pohybu vozidla		[30] až [35], [217]
4.	**Environmentální zkoušky**		
4.1	Výsledky zkoušek výrobce	Výsledky environmentálních zkoušek výrobce	ADA_020, ADA_021, ADA_022, ADA_024
5.	**Elektromagnetická kompatibilita (EMC)**		
5.1	Vyzařované emise a citlivost	Ověření shody se směrnicí 2006/28/ES	ADA_024
5.2	Výsledky zkoušek výrobce	Výsledky environmentálních zkoušek výrobce	ADA_024

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

Úřad pro publikace Evropské unie
2985 Lucemburk
LUCEMBURSKO

CS