Pravidlá postupu organizácie členského štátu (SK-MSA) týkajúce sa informačného systému inteligentných tachografov v Slovenskej republike

Verzia 1.3
August 2023

1 Úvod

1.1 Prehľad

Systém digitálnych tachografov druhej generácie nazývaných „Smart Tachograph" bol zavedený nariadením Európskeho parlamentu a Rady (EÚ) č. 165/2014. Inteligentný tachograf verzie 2 je povinný pre novoregistrované vozidlá od 21. augusta 2023 a pre všetky vozidlá zaradené do medzinárodnej prepravy od 21. augusta 2025.
V prílohe IC k vykonávaciemu nariadeniu Komisie (EÚ) č. 2016/799 sa ustanovujú technické požiadavky na konštrukciu, skúšky, inštaláciu, prevádzku a opravy inteligentných tachografov a ich súčastí.
Dodatok č. 11 k prílohe IC (Spoločné bezpečnostné mechanizmy) špecifikuje mechanizmy, ktoré zaisťujú:

- vzájomnú autentifikáciu medzi rôznymi komponentmi systému tachografov.
- dôvernosť, integritu, autentickosť, prípadne neodmietnutie údajov prenášaných medzi rôznymi komponentmi systému tachografu alebo údajov stiahnutých na externé pamäťové médium.

V časti B dodatku č. 11 sa opisuje, ako sa pri realizácii systémov tachografov druhej generácie využívajú kryptografické systémy s verejným kľúčom založené na eliptických krivkách a symetrické kryptografické systémy založené na štandarde AES.
Na podporu kryptografických systémov s verejným kľúčom bola navrhnutá infraštruktúra verejného kľúča (PKI), zatiaľ čo symetrický kryptografický systém závisí od hlavných kľúčov (master keys), ktoré je potrebné doručiť príslušným účastníkom. Bola vytvorená infraštruktúra skladajúca sa z troch vrstiev. Na európskej úrovni je za generovanie a správu párov koreňových verejno-súkromných kľúčov s príslušnými certifikátmi a symetrickými hlavnými kľúčmi zodpovedná organizácia European Root Certification Authority (ERCA). ERCA vydáva certifikáty pre certifikačné organizácie členských štátov (MSCA) a distribuuje symetrické hlavné kľúče (master keys) jednotlivým organizáciám MSCA. Organizácie MSCA sú zodpovedné za vydávanie certifikátov pre zariadenia inteligentných tachografov (Smart Tachograph) a tiež aj za distribúciu symetrických hlavných kľúčov a ďalších dát odvodených od hlavných kľúčov, ktoré sa majú nainštalovať do zariadení inteligentných tachografov.
Tento dokument predstavuje certifikačné pravidlá (CP) pre infraštruktúru PKI slovenského certifikačnej organizácie MSCA označovanú ako (SK-CA). Stanovuje postupy na úrovni SK-CA pre generovanie kľúčov, správu kľúčov a podpisovanie certifikátov pre systém inteligentných tachografov na základe pravidiel certifikácie ERCA. Aby SK-CA mohla vydávať osvedčenia, prípadne symetrické kľúče personalizátorom systémov, musia spĺňať požiadavky stanovené v tomto dokumente.
Tento dokument sa riadi rámcovými zásadami pre CP opísanými v RFC 3647.
Ako samotná organizácia SK-CA dodržiava tieto pravidlá certifikácie a pravidlá týkajúce sa infraštruktúry symetrických kľúčov, je opísané vo „Vyhlásení o certifikačnej praxi SK-CA (CPS)" pre systémy inteligentných tachografov.
Digitálne tachografy (systém prvej generácie) a inteligentné tachografy (systém druhej generácie) sú dva rôzne logické systémy, ktoré sú prevádzkované súbežne, avšak nezávisle od seba. Z tohto dôvodu sa musia dodržiavať osobitné postupy organizácií členských štátov (MSA), aby sa v budúcnosti predišlo problémom, keď dôjde k ukončeniu prevádzkovania digitálnych tachografov a ich príslušnej ERCA (1. gen.). Z tohto dôvodu zostanú okrem týchto pravidiel (SK-MSA-CP) naďalej v platnosti aj „Pravidlá postupu organizácie členského štátu pre informačný systém digitálnych tachografov platné v Slovenskej republike“.
Kľúčové slová, ako sú „požadované“, „musia“, „nesmú“, „mali by“, „nemali by“, „odporúča sa“, „môžu“ a „voliteľne“ použité v tomto dokumente, je potrebné interpretovať tak, ako je to opísané v RFC 2119.

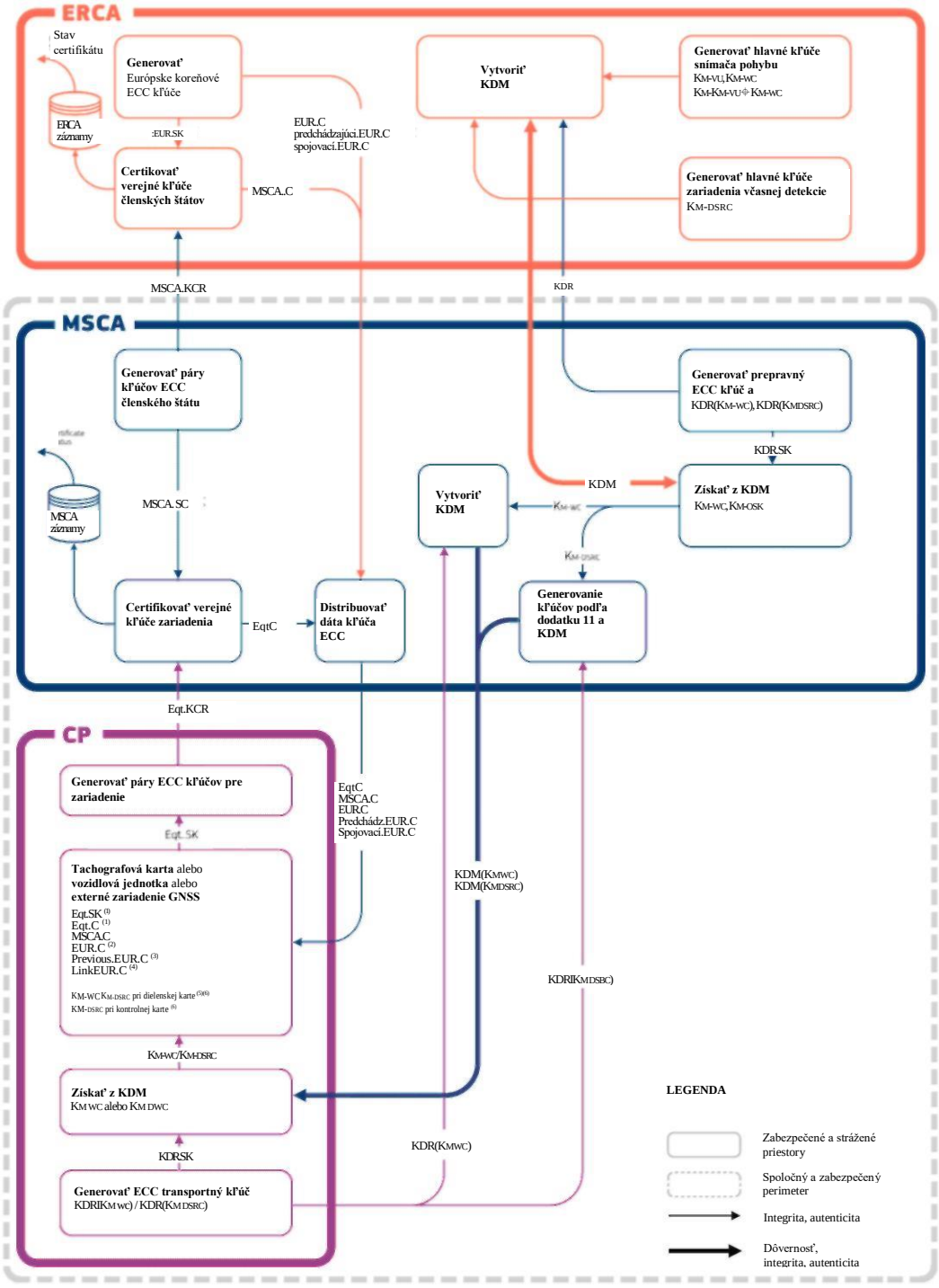
1.2 Názov a identifikácia tohto dokumentu

Tento dokument sa nazýva „Pravidlá postupu organizácie členského štátu (SK-MSA) týkajúce sa informačného systému inteligentných tachografov v Slovenskej republike” (SK-MSA-CP). Tieto

pravidlá certifikácie nemajú identifikátor objektu systému ASN.1. Takýto identifikátor nie je potrebný, pretože certifikáty využívané v systéme inteligentných tachografov neobsahujú odkaz na tieto pravidlá. Aktuálna verzia dokumentu je uvedená na začiatku tohto dokumentu.

1.3 Súčasti infraštruktúry PKI

Na nasledujúcom grafe (obr. 1) sú opísané jednotlivé súčasti infraštruktúry PKI Tachografov a infraštruktúry symetrických kľúčov. Na obr. 1 je tiež zobrazená výmena informácií medzi jednotlivými účastníkmi, konkrétne ER-CA, MSCA a personalizátormi komponentov systému (CP).



POZNÁMKY
1. Pre vozidlové jednotky a tachografové karty existujú dva certifikáty a príslušné kľúče, jeden pre vzájomnú autentizáciu (MA) a jeden pre podpisovanie (Sign).
2. Certifikát EUR používaný na generovanie certifikátu MSCA.C.
3. Certifikát EUR, ktorého platnosť priamo predchádza lehote platnosti EUR certifikátu v poznámke 2, ak existuje.
4. Certifikát prepojenia, ktorý spája EUR certifikáty uvedené v pozn. 2 a 3, a existuje.
5. Musia sa vložiť všetky kľúče KM-WC patriace ku kľúčom KM-VU, ktoré sa aktuálne používajú.
6. Musia sa vložiť všetky kľúče KM-DSBC, ktoré sa aktuálne používajú.

Obr. 1 Infraštruktúra PKI inteligentných tachografov a infraštruktúra symetrických kľúčov

Viac informácií o symetrických a asymetrických kľúčoch uvedených v tejto časti dokumentu nájdete v dodatku č. 11 časti B k nariadeniu Komisie (EÚ) č. 2016/799.

1.3.1 Certifikačné organizácie

1.3.1.1 Európska Certifikačná organizácia vydávajúca koreňové certifikáty (ERCA)

ERCA je Certifikačná organizácia vydávajúca koreňové certifikáty (CA), ktorá v infraštruktúre PKI vytvára a prideľuje certifikáty verejných kľúčov. Prevádzkuje nasledujúce služby pre súčasti systému:

službu registrácie, službu generovania certifikátov, službu šírenia certifikátov.

ERCA generuje páry koreňových kľúčov PKI a príslušné certifikáty spolu s certifikátmi prepojenia (link), aby bolo možné vytvoriť dôverné prepojenie medzi rôznymi koreňovými certifikátmi.

ERCA je tiež organizácia, ktorá na požiadanie vytvára, spravuje a distribuuje symetrické hlavné kľúče, t.j. hlavný kľúč snímača pohybu (Motion Sensor Master Key)– časť VU (K_{M-VU}), hlavný kľúč snímača pohybu - časť dielenskej karty (Workshop Card part) (K_{M-WC}) a hlavný kľúč DSRC (K_{M-DSRC}).

1.3.1.2 Certifikačná organizácia členského štátu - Slovenskej republiky (SK-CA)

SK-CA funguje ako Certifikačná organizácia podriadená organizácii ERCA. Vytvára a prideľuje certifikáty verejných kľúčov pre jednotlivé zariadenia. Z tohto dôvodu prevádzkuje služby registrácie, službu generovania certifikátov a službu šírenia certifikátov. Existujú dva typy párov kľúčov vydávaných CA a zodpovedajúcich certifikátov vydávaných CA: jeden na vydanie certifikátov VU a EGF, ktorý sa nazýva pár kľúčov MSCA_VU-EGF, a druhý na vydávanie certifikátov kariet, nazývaný pár kľúčov MSCA_Card. Organizácia SK-CA vyžaduje od ERCA iba certifikáty MSCA_Card SK-CA. Organizácia SK-CA od ERCA vyžaduje tiež symetrické hlavné kľúče a časti K_{M-WC} a K_{M-DSRC} distribuuje personalizátorom kariet.

1.3.2 Registračné organizácie

1.3.2.1 Organizácie vydávajúce karty pre tachografy (SK-CIA)

SK-CIA, ktorú ustanovila národná organizácia SK-MSA za subjekt vydávajúci karty (CIA), je zodpovedná za:

- overenie, či boli predložené všetky požadované dokumenty;
- overenie, či boli splnené všetky požiadavky na vydanie tachografovej karty, na ktorú sa vzťahuje nariadenie Európskeho parlamentu a Rady (EÚ) č. 165/2014, príloha IC k vykonávaciemu nariadeniu Komisie (EÚ) č. 2016/799 a všetky ostatné príslušné ustanovenia predpisov, pravidlá ERCA a tieto pravidlá SK-MSA;
- overenie, či tachografová karta už nebola žiadateľovi vydaná v inom členskom štáte EÚ;
- zabezpečenie toho, aby sa údaje zo žiadosti prenášali do SK-CP správne, v súlade s predloženými dokumentmi a požiadavkami týchto pravidiel;
- riadne informovanie všetkých používateľov systému o požiadavkách týchto pravidiel postupu;
- zabezpečenie toho, aby bol PIN dielenskej karty odovzdávaný iba určenému držiteľovi dielenskej karty prostredníctvom samostatného príjemcu pre dielenskú kartu (dielňa) a pre PIN (určený technik);
- okamžité informovanie SK-MSA a SK-CA o všetkých známych bezpečnostných rizikách a bezpečnostných incidentoch;

- SK MSA určila za organizáciu vydávajúcu karty (CIA) spoločnosť Alanata a.s., ktorá je označovaná ako SK-CIA.

1.3.2.2 SK-CA

Organizácia SK-CA v rámci svojej právomoci zabezpečuje, aby pred vydaním certifikátu, distribúciou symetrických kľúčov alebo šifrovaním údajov zariadenia došlo k riadnej registrácii personalizátorov kariet. Postup registrácie je podrobne uvedený v CPS.

1.3.3 Objednávatelia služieb

Jedinými objednávateľmi služby certifikácie verejných kľúčov MSCA sú personalizátori komponentov. Personalizátori komponentov systému sú zodpovední za personalizáciu:

- vozidlových jednotiek (VU)
- externých zariadení GNSS (EGF)
- snímačov pohybu (MoS)
- kariet tachografov: existujú štyri rôzne typy tachografových kariet: karty vodičov, firemné karty, dielenské karty a kontrolné karty.

V prípade Slovenska ide iba o personalizáciu kariet tachografov.

- Karty vodiča a dielenské karty majú dva páry kľúčov a zodpovedajúce certifikáty vydané MSCA_Card, menovite ide o
  - pár kľúčov a certifikát pre vzájomnú autentifikáciu s názvom Card_MA;
  - pár kľúčov a certifikát na podpisovanie s názvom Card_Sign.

- Dielenské karty obsahujú tiež K_{M-WC} a K_{M-DSRC} s dĺžkou kľúča pre všetky možné jednotky vozidla (VU) a použité šifrovacie schémy.

- Firemné karty a kontrolné karty majú pár kľúčov a zodpovedajúci certifikát pre potreby vzájomnej autentizácie vydaný organizáciou MSCA_Card.

- Kontrolné karty tiež obsahujú K_{M-DSRC} s dĺžkou kľúča pre všetky možné jednotky vozidla (VU) a použité šifrovacie schémy.

Personalizátori komponentov systému sú zodpovední za vybavenie zariadení príslušnými kľúčmi a certifikátmi.

1.3.3.1 Výrobcovia jednotiek vozidla (VU)

Netýka sa Slovenska.

1.3.3.2 Výrobcovia externých zariadení GNSS (EGF)

Netýka sa Slovenska.

1.3.3.3 Výrobcovia snímačov pohybu (MoS)

Netýka sa Slovenska

1.3.3.4 Personalizátor slovenských tachografových kariet (SK-CP)

- zaisťuje generovanie dvoch párov kľúčov kariet pre vzájomnú autentifikáciu a podpisovanie kariet vodičov a dielenských kariet;
- realizuje spracovanie žiadosti o certifikát u SK-CA_Card pre karty vodiča a dielenské karty;
- realizuje spracovanie žiadosti o K_{M-WC} a K_{M-DSRC} (iba dielenské karty);

- zaisťuje dostupnosť kľúčov a certifikátov na karte pre vzájomnú autentifikáciu a podpisovanie, párovanie MoS-VU a šifrovanie komunikácie DSRC a verifikáciu autentizačných údajov (iba dielenské karty);
- zabezpečuje generovanie párov kľúčov na kartách pre vzájomnú autentizáciu firemných a kontrolných kariet;
- realizuje proces podania žiadosti u organizácie SK-CA_Card pre firemné a kontrolné karty;
- podáva žiadosť o $K_{M\text{-}DSRC}$ (iba kontrolné karty);
- zaisťuje dostupnosť kľúčov a certifikátov na karte pre vzájomnú autentizáciu a dešifrovanie komunikácie DSRC a verifikáciu autentickosti údajov (iba kontrolné karty);
- Národná organizácia SK-MSA ustanovila za organizáciu realizujúcu personalizáciu kariet (CP) spoločnosť Alanata a.s., ktorá je označovaná ako SK-CP.

1.3.4 Závislé strany

Strany, ktoré sú závislé od certifikačných služieb organizácie SK-CA, sú predovšetkým orgány Slovenskej republiky, ktoré majú za úlohu uplatňovať pravidlá a predpisy týkajúce sa doby jázd a doby odpočinku, predstavované predovšetkým Policajným zborom SR a Národným inšpektorátom práce.
Certifikácia organizáciou SK-CA sa využíva v rámci systému na overovanie autenticity certifikátov zariadení, ktoré sa zasa využívajú na overovanie autenticity údajov stiahnutých z jednotiek vozidla a kariet vodičov.
Ďalšími priamo závislými stranami sú personalizátori, organizácie vydávajúce certifikáty (SK-CIA), vodiči, firmy a servisné dielne.

1.4 Používanie kľúčov a certifikátov

Organizácia SK-CA môže využívať svoje súkromné kľúče SK-CA iba na účely:

- podpísanie certifikátov zariadení, v súlade s prílohou IC dodatku 11
- podpisovanie žiadostí o podpis certifikátov (pozri časť 4.1.1)

Certifikáty vydané organizáciou SK-CA_Card sa použijú na verifikovanie certifikátov kariet, vydaných organizáciou SK-CA_Card.

Certifikáty Card_MA sa použijú na vzájomnú autentizáciu a odsúhlasenie prihlasovacích kľúčov medzi kartou a jednotkou vozidla.

Certifikáty Card_Sign sa použijú na verifikáciu autentickosti a integrity údajov stiahnutých z karty. Súkromný kľúč Card_Sign sa smie použiť iba na podpis údajov stiahnutých z karty.

1.5 Administrácia pravidiel

1.5.1 ERCA

Služba Európskej komisie zodpovedná za implementáciu pravidiel certifikácie na európskej úrovni a za zaistenie certifikácie kľúčov a službu distribúcie hlavných kľúčov do členských štátov EÚ sa označuje ako Európska Certifikačná organizácia vydávajúca koreňové certifikáty (ERCA).

Kontaktná adresa ERCA je:

Head of the Cyber and Digital Citizens' Security Unit E3
Directorate E - Space, Security and Migration
Joint Research Centre (TP 361)
European Commission
Via Enrico Fermi, 2749
I-21027 Ispra (VA)
Taliansko

Organizácia ERCA preveruje pravidlá vydávania certifikátov zo strany organizácií členských štátov (MSA), vrátane pravidiel vydávania certifikátov SK-MSA, či spĺňajú požiadavky definované organizáciou ERCA. Cieľom procesu preverovania je zaistiť porovnateľnú úroveň bezpečnosti v každom členskom štáte. ERCA archivuje správy z previerok uplatňovania pravidiel a zásad certifikácie MSA na účely referencií.
ERCA zaisťuje služby certifikácie kľúčov pre certifikačné organizácie členských štátov (MSCA) pridružené k zodpovednej organizácie členského štátu (MSA), iba ak výsledok preskúmania dodržiavania pravidiel certifikácie zo strany MSA dáva dostatočné dôvody na hodnotenie, že budú splnené požiadavky pravidiel ERCA na vydávanie certifikátov. Pokračovanie v poskytovaní služby certifikácie kľúčov zo strany ERCA pre MSCA závisí od včasného prijatia audítorských správ o MSA (pozri kapitolu 8.1), ktoré preukazujú, že MSCA si naďalej plnia svoje povinnosti stanovené v schválených pravidlách MSA pre certifikáciu.

1.5.2 Zodpovedná organizácia členského štátu EÚ v Slovenskej republike (SK-MSA)

Organizácia zodpovedná za tieto vnútroštátne pravidlá postupu (SK-MSA) je Ministerstvo dopravy Slovenskej republiky vystupujúce ako organizácia členského štátu (MSA), ktorého systém tachografov je označovaný ako SK-MSA. Do povinností SK-MSA patrí:

- Určovanie a dokumentovanie pravidiel certifikácie SK-MSA v súlade so všetkými požiadavkami vyplývajúcimi z pravidiel certifikácie ERCA a zaistenie ich schválenia zo strany ERCA. SK-MSA pripravuje pre ERCA verziu pravidiel certifikácie SK-MSA v anglickom jazyku a zaisťuje verziu v slovenskom jazyku.
- Schvaľovanie CPS SK-CA a konštatovanie ich súladu s týmito CP. Je možné splniť to spolu s auditmi súladu SK-CA (pozri kapitolu 8).
- Zistenie alebo zabezpečenie sprístupnenia SK-MSA-CP pre všetky zúčastnené organizácie.
- Zistenie toho, aby SK-CA mala požadované zdroje na prevádzku v súlade s pravidlami certifikácie.

Kontaktná adresa SK-MSA je:

Ministerstvo dopravy Slovenskej republiky
Námestie slobody č. 6

810 05 Bratislava
Slovenská republika

Telefón: +421 (2) 5949 4111

E-mail: info@mindop.sk

1.5.3 SK-CA

SK-MSA určuje spoločnosť Alanata a.s. na prevádzkovanie SK-CA, ktorá implementuje pravidlá certifikovania na Slovensku a zaisťuje službu certifikácie a distribúcie kľúčov personalizátorom kariet na Slovensku.

Kontaktná adresa SK-CA je:

Alanata a.s.
Einsteinova Business Center
Krasovského 14
851 01 Bratislava 5
Slovenská republika

Telefón: +421 (2) 502 67 111
Fax: +421 (2) 502 67 100
E-mail: info@alanata.sk

SK-CA dokumentuje svoju implementáciu pravidiel certifikácie SK-MSA prostredníctvom vyhlásenia o certifikačných postupoch (SK-CA CPS). SK-CA CPS je dokument organizácie SK-CA určujúci postup certifikácie, v ktorom sú uvedené podrobnosti uplatňovania pravidiel certifikácie SK-MSA pri každodennom manažmente tohto procesu. Dokument pripravila a vlastní organizácia SK-CA. Je s ním potrebné zaobchádzať ako s dôvernými informáciami s obmedzeným prístupom. SK-CA sprístupní obsah svojich CPS iba pre osoby, ktoré to nevyhnutne potrebujú pre svoju činnosť. Dokument SK-CA CPS sa musí riadiť, revidovať a upravovať podľa postupov riadenia dokumentov.
SK-CA sprístupní svoje vyhlásenia CPS organizácii SK-MSA. Organizácia SK-MSA je zodpovedná za zistenie toho, či SK-CA CPS spĺňa požiadavky pravidiel certifikácie SK-MSA. SK-CA na požiadanie sprístupní svoju verziu CPS tiež organizácii ERCA.
SK-CA vedie evidenciu svojej činnosti náležitým spôsobom tak, aby mohla preukázať plnenie požiadaviek certifikačných pravidiel organizácie SK-MSA, a zaistí sprístupnenie tejto evidencie organizácii SK-MSA, prípadne na vyžiadanie aj organizácii ERCA.
Sťažnosti zo strany personalizátorov komponentov na služby poskytované organizáciou SK-CA sa adresujú organizácii SK-MSA (kontaktná adresa pozri odsek 1.5.2).

V súlade s odsekmi 1.3.2.1 a 1.3.3.4 je ustanovenou organizáciou vydávajúcou karty pre Slovensko (ďalej len SK-CIA) a určenou organizáciou pre personalizáciu kariet v Slovenskej republike (ďalej len SK-CP):

Alanata a.s.
Einsteinova Business Center
Krasovského 14
851 01 Bratislava 5
Slovenská republika

Telefón: +421 (2) 502 67 111
Fax: +421 (2) 502 67 100
E-mail: info@alanata.sk

SK-CIA dokumentuje svoju implementáciu pravidiel certifikácie organizácie SK-MSA vo vyhlásení o „Postupoch certifikácie" (SK-CIA CPS).
SK-CP dokumentuje svoju implementáciu pravidiel certifikácie organizácie SK-MSA prostredníctvom vyhlásenia o „Postupoch certifikácie" (SK-CP CPS).

1.6 Definície a akronymy

Akronym	**Definícia**
AES	Pokročilý štandard šifrovania (Advanced Encryption Standard)
CP	Personalizátor komponentov
CP	Pravidlá certifikácie
CPS	Vyhlásenie o postupoch certifikácie
SK-CA	Slovenská Certifikačná organizácia členského štátu EÚ
SK-CIA	Slovenská organizácia vydávajúca kartu
SK-CP	Personalizátor slovenských kariet
SK-MSA	Slovenská organizácia členského štátu EÚ
SK-MSA-CP	Pravidlá certifikácie slovenskej organizácie členského štátu EÚ
DSRC	Vyhradená komunikácia na krátke vzdialenosti
CSR	Požiadavka na podpísanie certifikátu
EC	Eliptická krivka
EC	Európska komisia
ECC	Šifrovanie s využitím eliptickej krivky
EGF	Externé zariadenie GNSS
EA	Európska zodpovedná organizácia
ERCA	Európska organizácia pre vydávanie koreňových certifikátov
EU	Európska únia

GNSS	Globálny navigačný satelitný systém
HSM	Hardvérový bezpečnostný modul
ISMS	Systém manažmentu informačnej bezpečnosti
JRC	Spoločné výskumné stredisko
KDR	Požiadavka na distribúciu kľúčov
K_M	Hlavný kľúč snímača pohybu
K_{M-VU}	VU časť KM
K_{M-WC}	WC časť KM
K_{ID}	Identifikačný kľúč snímača pohybu
K_P	Párovací kľúč snímača pohybu
K_{M-DSRC}	Hlavný kľúč DSRC
LKM	Označená správa s kľúčom
MA	Vzájomná autentizácia
MoS	Snímač pohybu
MSA	Zodpovedná organizácia členského štátu
MSCA	Certifikačná organizácia členského štátu EÚ
MT SR	Ministerstvo dopravy Slovenskej republiky
NCP	Pravidlá normalizovaných certifikátov
PKI	Infraštruktúra verejných kľúčov
RFC	Žiadosť o pripomienky (Request for Comment)
RSA	Rivest, Shamir a Adleman
TC	Tachografová karta
VU	Jednotka vozidla
WC	Dielenská karta

Ďalšie definície možno nájsť v dokumentoch, na ktoré odkazujú certifikačné pravidlá SK-CA; pozri časť „referencie" v záverečnej časti tohto dokumentu.

2 Publikovanie a zodpovednosť za uchovávanie dokumentov

2.1 Depozitáre

- Všetky certifikáty pre zariadenia, ktoré vydala organizácia SK-CA, sa musia uchovávať v databáze SK-CA.

2.2 Zverejňovanie informácií o certifikácii

- SK-MSA zverejní tieto pravidlá certifikácie na webovej stránke www.digitalnytachograf.sk.
- Vyhlásenie o postupoch certifikácie SK-CA nebudú verejne dostupné, ale na požiadanie sa poskytnú relevantným subjektom.

2.3 Doba alebo frekvencia publikovania

- Informácie týkajúce sa zmien v týchto pravidlách sa zverejňujú podľa harmonogramu stanoveného v postupoch pre zmeny (novelizácie) uvedených v odseku 9.12 tohto dokumentu..

2.4 Riadenie prístupu k depozitárom

- Všetky informácie dostupné na webovej stránke SK-MSA majú prístup obmedzený len na čítanie. SK-CA určí zamestnancov, ktorí budú mať práva zápisu alebo úprav informácií v SK-CA CPS.
- Všetky informácie zverejnené na webovej stránke MSA budú dostupné prostredníctvom zabezpečeného internetového pripojenia.

3 Identifikácia a autentizácia

Táto kapitola opisuje realizáciu identifikácie a autentizácie (I&A) pri prvotnej žiadosti o certifikát, pri opakovanej žiadosti o certifikát a pri žiadosti o distribúciu symetrických kľúčov medzi SK-CA a ERCA. Identifikácia a autentizácia medzi organizáciou SK-CA a personalizátormi kariet je podrobne opísaná v SK-CA CPS.

3.1 Pomenovanie

3.1.1 Typy mien

3.1.1.1 Predmet certifikátu a vydavateľ certifikátu

Vydavateľ certifikátu a predmet certifikátu sú identifikované odkazmi na Certifikačnú organizáciu a držiteľa certifikátu. Vytvárajú sa spôsobom opísaným v dodatkoch č. 1 a 11 prílohy dokumentu CSM_136/CSM_141.

Entita (organizácia):

- SK-CA

Konštrukcia:

- Národný číselný kód (‘2D’ pre Slovensko)
- Národný znakový kód (53 4B20’, SK bez medzier, pre Slovensko)
- Sériové číslo kľúča
- Doplňujúce informácie
- Identifikátor certifikačnej organizácie (CA)

Certifikáty testovacích kľúčov, žiadosti o testovacie certifikáty, žiadosti o distribúciu testovacích kľúčov a správy s distribúciou testovacích kľúčov na účely skúšok interoperability musia obsahovať hodnoty „54 4B“ („TK“) v poli *doplňujúcich informácií*.

3.1.1.2 Žiadosti o distribúciu kľúčov a správa pre distribúciu kľúčov

Žiadosti o distribúciu kľúčov a správy s distribúciou kľúčov sa identifikujú podľa identifikátora kľúča efemérneho verejného kľúča generovaného každou MSCA, pozri odsek 4.2.1. Hodnota identifikátora kľúča sa určuje podľa odseku 3.1.1.1 s nasledujúcimi úpravami:
Entita:

- Sériové číslo kľúča: je jedinečné pre každú žiadajúcu entitu
- Doplňujúce informácie: ‘4B 52’ (“KR”, pre žiadosť o kľúč), pokiaľ nejde o žiadosť o testovacie kľúče KDR. V takomto prípade sa použije „54 4B“ („TK" pre testovací kľúč).

Konštrukcia:

- Národný číselný kód (‘28’ pre Slovensko)
- Národný znakový kód (53 4B 20’, SK bez medzier, pre Slovensko)
- Sériové číslo kľúča
- Doplňujúce informácie
- Identifikátor certifikačnej organizácie (CA)

Certifikáty testovacích kľúčov, žiadosti o testovacie certifikáty, žiadosti o distribúciu testovacích kľúčov a správy s distribúciou testovacích kľúčov na účely skúšok interoperability musia obsahovať hodnoty „54 4B“ („TK“) v poli *doplňujúcich informácií*.

3.2 Počiatočné overenie totožnosti

3.2.1 Metóda preukázania držby súkromného kľúča

Pri predkladaní žiadostí o podpísanie certifikátov (CSR) do ERCA je potrebný dôkaz o vlastníctve príslušného súkromného kľúča prostredníctvom interného podpisu, ako je uvedené v odseku 4.1.1. CSR môžu obsahovať aj vonkajší podpis preukazujúci pravosť správy. Vonkajší podpis sa vytvorí pomocou už certifikovaného súkromného kľúča uvedeného v žiadosti o podpísanie certifikátov.
Prostredníctvom overenia (realizovaného ručne spolu s SK-MSA/SK-CA), ak sa zhoduje kontrolný súčet (hash) vypočítaný na základe prijatej žiadosti o podpis certifikátu (CSR) s kontrolným súčtom (hashom) žiadosti CSR zaslanej od SK-CA (ako je opísané v ERCA CPS), sa preukáže ďalšia skutočnosť potvrdzujúca integritu, autenticitu a počiatočnú dôveru.

3.2.2 Autentizácia identity organizácie

Ako je uvedené v odseku 1.3 týchto pravidiel, účastníkmi infraštruktúry PKI a symetrických kľúčov inteligentného tachografu sú:

- jediná SK-MSA, uvedená v odseku 1.5.2 týchto pravidiel;
- jediná SK-CA, uvedená v odseku 1.5.3 týchto pravidiel;
- jediná SK-CIA, uvedená v odseku 1.3.2.1 týchto pravidiel;
- jediná SK-CP, uvedená v odseku 1.3.3.4 týchto pravidiel.

Pretože všetky tieto organizácie sú priamo vymenované a žiadna iná organizácia sa nemusí do systému inteligentných tachografov na Slovensku pripájať, nie je potrebné totožnosť týchto organizácií overovať.

3.2.3 Autentizácia identity jednotlivých subjektov

3.2.3.1 Pri podávaní žiadosti o kartu

SK-CIA zabezpečí, aby sa identifikačné doklady držiteľa karty a správnosť mien a súvisiacich údajov riadne preskúmali v rámci služby registrácie pri podávaní žiadosti o kartu. Ide predovšetkým o to, aby:

- SK-CIA informovala držiteľa karty o podmienkach využívania certifikátov;
- SK-CIA zaznamenala túto komunikáciu prostredníctvom prostriedkov trvalého uchovania informácií v ľahko zrozumiteľnom jazyku;
- SK-CIA zhromažďovala príslušné podklady z náležitých a autorizovaných zdrojov o totožnosti a akýchkoľvek špecifických atribútoch držiteľa karty. Predložené doklady môžu mať formu buď papierovej, alebo elektronickej dokumentácie. Overenie totožnosti držiteľa karty sa realizuje náležitými prostriedkami a v súlade s legislatívou príslušného štátu.
- ak je držiteľom karty fyzická osoba, SK-CIA porovná doklady totožnosti s dokladmi totožnosti uznávanými v danom štáte, napr. vodičským preukazom;
- ak je držiteľom karty fyzická osoba, ktorej identifikácia sa spája s právnickou osobou alebo organizačnou jednotkou (napr. dielňou), SK-CIA porovná doklad totožnosti držiteľa karty voči dokladu totožnosti uznávanému v danom štáte, napr. občianskemu preukazu, a dokladu, ktorý preukazuje, že držiteľ karty je skutočne spojený s právnickou osobou alebo organizačnou jednotkou;
- ak je držiteľ karty organizačná jednotka (napr. prepravná spoločnosť), SK-CIA porovná totožnosť držiteľa karty s platnou registráciou.

Tento postup je podrobnejšie opísaný vo vyhlásení SK-CIA o postupoch certifikácie.

3.2.3.2 Pri doručení karty

SK-CIA si pred vydaním tachografovej karty overí individuálnu totožnosť držiteľa karty:

- v prípade kariet vodiča, dielenských kariet alebo kontrolných kariet si SK-CIA overí totožnosť osoby, ktorá osobne preberá kartu tak, že skontroluje jej platný doklad totožnosti, ktorý obsahuje jej fotografiu. Osoba, ktorá kartu preberá, musí byť tá istá osoba, ako je držiteľ karty;
- v prípade firemných kariet spoločnosť, ktorá žiada o kartu, musí organizácii SK-CIA pred distribúciou karty oznámiť totožnosť osoby, ktorá v mene spoločnosti kartu preberá. Pri distribúcii si SK-CIA overí totožnosť tejto osoby prostredníctvom kontroly jej platných dokladov osobne.

Tento postup je podrobnejšie opísaný vo vyhlásení SK-CIA o postupoch certifikácie.

3.2.4 Overovanie právomocí

SK-CA vymedzí postup overovania právomocí vo svojom vyhlásení o postupoch certifikácie.

3.2.5 Kritériá na vzájomnú súčinnosť

Pri službách podpisovania certifikátov a distribúcie kľúčov, ktoré SK-CA zaisťuje pre systém inteligentných tachografov, nesmie byť SK-CA závislá od žiadnej externej certifikačnej organizácie, s výnimkou ERCA. Ak pri akejkoľvek inej službe alebo funkcii je SK-CA závislá od externej infraštruktúry PKI, pred podaním žiadosti o certifikačné služby sa vyžaduje preskúmanie a schválenie certifikačných postupov (CP), prípadne vyhlásenia o certifikačných postupoch (CPS) externého poskytovateľa certifikačných služieb zo strany SK-MSA.

3.3 Identifikácia a autentizácia pre žiadosti o obnovu kľúčov

Identifikácia a autentizácia pre žiadosti o obnovu kľúčov (pozri odseky 4.1.8 a 4.2.9) je rovnaká ako v prípadoch opísaných v odseku 3.2.

3.4 Identifikácia a autentizácia pri žiadosti o zrušenie

Na Slovensku neaplikovateľné.

4 Prevádzkové požiadavky na životný cyklus certifikátov, symetrických kľúčov a šifrovacích služieb

Táto kapitola opisuje formáty správ, kryptografické mechanizmy a postupy pri podávaní žiadostí o certifikáciu pre zariadenia, žiadostí o symetrické kľúče pre služby šifrovania údajov na kartách a v zariadeniach, pri ich distribúcii medzi SK-CA a personalizátormi komponentov, ako aj postupy pri podávaní žiadostí SK-CA o certifikáty, ich distribúciu a symetrické hlavné kľúče medzi ERCA a SK-CA.

4.1 Žiadosť o certifikát verejného kľúča SK-CA ERCA a jeho vydanie

Nasledujúce požiadavky sú úzko späté s príslušnou kapitolou pravidiel vydávania certifikátov ERCA 2. gen.

4.1.1 Žiadosti o podpísanie certifikátu

Žiadosti o podpísanie certifikátu môže predkladať iba SK-CA určená organizáciou SK-MSA prostredníctvom vyhlásenia o zhode (pozri odsek 1.5.2).
Žiadosť o podpísanie certifikátu (CSR) musí byť vo formáte TLV.

Dátový objekt	**Požiad.**	**Tag**
Autentizácia	c	'67'
ECC (CV) certifikátu	m	'7F 21'
Telo certifikátu	m	'7F 4E'
Identifikátor profilu certifikátu	m	'5F 29'
Odkaz na certifikačnú autoritu	m	'42'
Autorizácia držiteľa certifikátu	m	'5F 4C'
Verejný kľúč	m	'7F 49'
Štandardizované parametre domény OID	m	'06'
Verejný bod	m	'86'
Odkaz na držiteľa certifikátu	m	'5F 20'
Dátum nadobudnutia platnosti certifikátu	m	'5F 25'
Dátum skončenia platnosti certifikátu	m	'5F 24'
Vnútorný podpis	m	'5F 37'
Odkaz na certifikačnú autoritu vonkajšieho podpisu Signatár	c	'42'
Vonkajší podpis	c	'5F 37'

Tabuľka 1: Formát žiadosti o podpis certifikátu

m: povinné
c: podmienené

Autentizačný dátový objekt sa bude vyskytovať iba v prípade prítomnosti dátového objektu vonkajšieho podpisu.

Verzia profilu je identifikovaná identifikátorom profilu certifikátu. Verzia 1 uvedená v odseku 7.1 sa identifikuje hodnotou 00.

Odkaz na certifikačnú autoritu sa použije na informovanie ERCA o súkromnom kľúči ERCA, pri ktorom SK-CA predpokladá, že ho použije na podpísanie certifikátu. Hodnoty pre odkazy na certifikačnú autoritu sú uvedené v odseku 3.1. Na webovej stránke ERCA je vždy uvedený identifikátor koreňového kľúča ERCA, ktorý je k dispozícii na podpisovanie.

Autorizácia držiteľa certifikátu sa použije na identifikáciu typu certifikátu. Je zložený zo šiestich vyšších bajtov identifikátora (ID) aplikácie tachografu („FF 53 4D 52 44 54"), ku ktorým je pripojený typ zariadenia, pre ktoré je certifikát určený (Príloha IC, Dodatok 11, CSM_141). V prípade certifikátov MSCA sa typ zariadenia nastaví na „0E" (14 desiatkovo).

Verejný kľúč obsahuje dva dátové objekty:
- -Dátový objekt **parametre domény** odkazuje na štandardizované parametre domény, ktoré sa majú v certifikáte použiť pri verejnom kľúči. Musí obsahovať jeden z identifikátorov objektov uvedených v tabuľke 1 v dodatku 11 k prílohe IC.
- -Dátový objekt **Public Point** obsahuje verejný bod. Verejné body eliptickej krivky sa prepočítajú na oktetové reťazce, ako sa uvádza v norme ISO/IEC 18033-2. Použije sa nekomprimovaný formát kódovania (príloha IC, dodatok 11, CSM_143).

Odkaz na držiteľa certifikátu sa používa na identifikáciu verejného kľúča obsiahnutého v žiadosti o certifikát a vo výslednom certifikáte. Referencia držiteľa certifikátu musí byť jedinečná. Môže sa použiť na označenie tohto verejného kľúča v certifikátoch na úrovni zariadení (príloha IC, dodatok 11, CSM_144). Referenčné hodnoty držiteľa certifikátu sú uvedené v odseku 3.1.

Dátum nadobudnutia platnosti certifikátu uvádza počiatočný dátum a čas nadobudnutia platnosti certifikátu. **Dátum skončenia platnosti certifikátu** uvádza dátum a čas ukončenia platnosti certifikátu. Obidva dátové prvky sú typ TimeReal, špecifikované v dodatku 1 k prílohe IC. Upozorňujeme, že obdobie platnosti definované týmito dvoma dátovými prvkami je buď 17 rokov a 3 mesiace (v prípade certifikátu MSCA_VU-EGF), alebo 7 rokov a 1 mesiac (pre certifikáty MSCA_Card).

Telo certifikátu je samo podpísané prostredníctvom **vnútorného podpisu,** ktorý je overiteľný prostredníctvom verejného kľúča obsiahnutého v žiadosti o certifikát. Podpis bude zahŕňať zakódované telo certifikátu, vrátane značky (tagu) a dĺžky tela certifikátu. Algoritmus podpisu je ECDSA, ako je špecifikované v ISO/IEC 10116, s využitím hašovacieho algoritmu (kontrolného súčtu) viazaného na veľkosť verejného kľúča žiadosti o podpísanie certifikátu (CSR) tak, ako je to uvedené v prílohe IC dodatku 11, CSM_50. Formát podpisu musí byť jednoduchý tak, ako je to stanovené v ISO/IEC 18033-2.

Odkaz na certifikačnú autoritu vonkajšieho podpisu - signatára uvádza certifikačnú organizáciu členského štátu EÚ (MSCA), ktorá použila vonkajší podpis a príslušný kľúč. Musí byť prítomný iba v prípade, ak je k dispozícii vonkajší podpis. Možné hodnoty sú uvedené v odseku 3.1.

Vonkajší podpis nebude uvedený, ak SK-CA požiada o úvodný certifikát. Vonkajší podpis sa vyžaduje, ak SK-CA požiada o následný certifikát. V takom prípade sa žiadosť o podpísanie certifikátu podpíše navyše prostredníctvom vonkajšieho podpisu SK-CA s použitím jedného z jeho platných súkromných kľúčov SK-CA. Vonkajší podpis autentizuje žiadosť o certifikát. Pretože SK-CA je objednávateľom služby poskytovania certifikátov MSCA_Card i MSCA_VU-EGF, vonkajší podpis bude použitý s využitím súkromného kľúča zviazaného s certifikátom rovnakého typu..

Vonkajší podpis sa vytvorí tak, že bude pokrývať ECC (CV) kódovaný certifikát(vrátane značky (tagu) „7F 21“ certifikátu a jeho dĺžky) a pole s odkazom na certifikačnú autoritu signatára vonkajšieho podpisu (vrátane značky certifikátu „42“ a jeho dĺžky). Algoritmus podpisu je ECDSA, ako je špecifikované v ISO/IEC 10116, s využitím algoritmu kontrolného súčtu (hashovania) viazaného na veľkosť kľúča SK-CA použitého na podpisovanie, ako je to uvedené v prílohe IC dodatku 11, CSM_50. Formát podpisu musí byť jednoduchý tak, ako je to stanovené v ISO/IEC 18033-2.

SK-CA vypočíta a uloží kontrolný súčet (hash) pokrývajúci celú žiadosť o podpis CSR, s využitím algoritmu kontrolného súčtu viazaného na veľkosť kľúča podpisujúcej organizácie, ako je uvedené v prílohe IC dodatku 11, CSM_50. ERCA použije tento kontrolný súčet (hash) spolu s MSA/MSCA na manuálne overenie autenticity žiadosti CSR, pozri odsek 4.1.2.1.

4.1.2 Spracovanie žiadosti o certifikát

4.1.2.1 Overovanie obsahu žiadosti o podpis (CSR)

ERCA zaisťuje, aby žiadosť o podpis CSR, ktorá prichádza z ktorejkoľvek MSCA, bola úplná, presná a riadne schválená. Iba v takomto prípade ERCA certifikát MSCA podpíše.
Kontroly správnosti, úplnosti a autorizácie vykonávajú úradníci organizácie ERCA manuálne, prípadne automatizovane prostredníctvom registračnej služby organizácie ERCA. Ak je žiadosť riadna a úplná, povolia podpísanie certifikátu MSCA.

ERCA si pri každej žiadosti o podpis CSR overuje, či:

- sú prenosové médiá čitateľné; t.j. nepoškodené alebo neporušené;
- je formát CSR v súlade s tabuľkou 2;

- je žiadosť riadne schválená. Ak existuje vonkajší podpis, ERCA overí správnosť tohto podpisu. V každom prípade ERCA kontaktuje MSCA, ako je opísané v CPS ERCA, a overuje, či sa kontrolný súčet (hash) vypočítaný na základe prijatej žiadosti CSR zhoduje s kontrolným súčtom (hashom) na CSR zaslaným organizáciou MSCA;
-má MSCA nárok na požadovaný typ certifikátu;
-odkaz na certifikačnú autoritu uvedený v žiadosti uvádza koreňový súkromný kľúč ERCA, ktorý je aktuálne platný na podpisovanie certifikátov MSCA;
-je odkaz na držiteľa certifikátu jedinečný. V prípade MSCA je referenciou držiteľa certifikátu identifikátor kľúča certifikačnej autority (KID). Sériové číslo kľúča v tomto KID sa musí medzi jednotlivými kľúčmi od toho istého MSCA líšiť, čo robí KID jedinečným;
-sú parametre domény špecifikované v žiadosti uvedenej v tabuľke 1 prílohy IC, dodatok 11 a či stupeň týchto parametrov je zhodný so stupňom koreňového kľúča ERCA uvedeného v referenčnom čísle certifikačnej autority;
-ERCA necertifikovala v predchádzajúcom období verejný bod v žiadosti a či tento nebol v minulosti použitý ako efemérny kľúč pre distribúciu symetrických kľúčov (pozri oddiel 4.2.3) a ani na účely skúšky interoperability;
-sa verejný bod uvedený v žiadosti nachádza na krivke;
-sa dá pomocou verejného bodu a parametrov domény uvedených v žiadosti overiť vnútorný podpis . Týmto sa preukazuje, že MSCA vlastní súkromný kľúč naviazaný na verejný kľúč;
-je prítomný vonkajší podpis, ak nejde o žiadosť MSCA o počiatočný certifikát MSCA_VU-EGF alebo MSCA_Card
- sa overí vonkajší podpis, ak je k dispozícii, pomocou verejného bodu a parametrov domény v certifikáte MSCA, na ktorý je odkaz v poli podpisu „Odkaz na certifikačnú autoritu" pre vonkajší podpis. Navyše, či u tohto kľúča už neuplynula doba využívania súkromného kľúča.

Ak výsledok ktorejkoľvek z týchto kontrol bude negatívny, ERCA odmietne žiadosť o podpísanie CSR. ERCA pri každej žiadosti oznámi MSCA a zodpovednému MSA dôvody jej zamietnutia.

4.1.2.2 Generovanie, distribúcia a administrácia certifikátov

Ak sú výsledky všetkých kontrol pozitívne, ERCA podpíše certifikát, ako je opísané v odseku 4.1.3.
Do databázy ERCA sa pre každú prijatú žiadosť o podpísanie certifikátu zaznamenajú nasledujúce informácie:

-úplná žiadosť CSR prichádzajúca od daného MSCA;
-prípadný kompletný výsledný certifikát verejného kľúča;
-štandardizované parametre domény OID a verejný bod certifikovaného verejného kľúča;
-dátum nadobudnutia platnosti certifikátu a dátum uplynutia platnosti certifikátu ;
-odkaz na držiteľa certifikátu (pre identifikáciu verejného kľúča);
-kontrolný súčet binárnych dát certifikátu, ak existujú. Dĺžka kontrolného súčtu je viazaná na veľkosť kľúča podpisujúcej organizácie (signatára), ako je uvedené v prílohe IC dodatku 11, CSM_50;
-kontrolný súčet binárnych dát žiadosti CSR, pozri odsek 4.1.1;
-stav certifikátu „Platný“, ak je certifikát vydaný, alebo „Zamietnutý“ v prípade zamietnutia CSR;
-časová pečiatka.

Certifikáty odosielané do MSCA sú zapísané na prenosové médium v súlade s požiadavkami uvedenými v odseku 4.1.4. Každá kópia certifikátu zapísaná na prenosové médium sa následne overuje pomocou verejného kľúča ERCA. ERCA tiež zapíše na prenosové médium kópiu certifikátu verejného kľúča ERCA, ktorý sa môže použiť na overenie certifikátov (certifikátov) MSCA.
Po úspešnej distribúcii nového certifikátu do MSCA ERCA aktualizuje informácie o stave certifikátu v úložisku ERCA. Žiadne ďalšie oznamy sa nevykonávajú.
ERCA si ponecháva prenosové médium obsahujúce žiadosť CSR a archivuje ho vo svojich priestoroch s obmedzeným prístupom.
Cieľom ERCA je dokončiť operácie certifikácie verejného kľúča v rámci jedného pracovného dňa. Čas potrebný na to, aby ERCA dodala certifikát verejného kľúča do MSCA alebo aby rozdistribuovala symetrický kľúč, sa určí výhradne podľa času potrebného na správne vykonanie postupov ERCA. Zaručená je doba reakcie

a spracovania do jedného mesiaca. Pri žiadosti o certifikát zohľadnia príslušné organizácie členských štátov tento maximálny čas na reakciu a spracovanie žiadosti.

4.1.3 Certifikáty

Formát certifikátov verejného kľúča SK-CA je uvedený v odseku 7.1.

ERCA vytvorí podpis zahrňujúci kódované telo certifikátu, vrátane značky (tagu) a dĺžky. Algoritmom podpisu je ECDSA, podľa špecifikácie ISO/IEC 10116, s použitím algoritmu kontrolného súčtu naviazaného na veľkosť kľúča podpisujúcej organizácie, ako je uvedené v prílohe IC dodatku 11, CSM_50. Formát podpisu musí byť jednoduchý, ako je stanovené v ISO/IEC 18033-2.

4.1.4 Zasielanie žiadostí a odpovedí

Na prepravu žiadostí o podpis certifikátov a distribúciu certifikátov sa používajú CD-R médiá:

- Disky CD-R majú priemer 12 cm, nahrávajú sa v režime jednej relácie (formát ISO 9660: 1988).

Po predchádzajúcom súhlase ERCA sa môžu použiť aj iné spôsoby prepravy. Na účely testovania ERCA prijíma CSR a odosiela certifikáty ako prílohy e-mailov.
Na prenosové médium zapíše SK-CA tri kópie každej žiadosti o podpísanie certifikátu a odošle ho do ERCA. Tieto kópie musia byť vo formáte hexadecimálnom ASCII (súbor .txt), Base64 (súbor .pem) a binárnom formáte (súbor .bin).
ERCA zapíše na prenosové médium tri kópie každého certifikátu a odošle ho SK-CA. Tieto kópie sú vo formáte hexadecimálnom ASCII (súbor .txt), Base64 (súbor .pem) a binárnom formáte (súbor .bin)
Každá žiadosť o podpísanie certifikátu a samotný certifikát musia mať priloženú papierovú kópiu údajov vo formáte podľa šablóny definovanej v ERCA CPS. Ďalšia papierová kópia údajov bude uchovávaná v ERCA alebo SK-CA.
V oboch prípadoch, pri žiadosti CSR aj pri certifikátoch, si prenosové médiá a výtlačky odovzdávajú medzi sebou zamestnanci ERCA a kuriér SK-CA v stážených priestoroch ERCA.

4.1.5 Prevzatie certifikátu

Kuriér podpisuje prevzatie certifikátu pre SK-CA v priestoroch ERCA.
Po prevzatí certifikátu v priestoroch SK-CA musí SK-CA skontrolovať, či:

-je prenosové médium čitateľné; t. j. či nie je poškodené alebo neporušené;
-je formát certifikátu v súlade s tabuľkou 4 uvedenou v odseku 7.1;
-všetky hodnoty poľa certifikátu zodpovedajú hodnotám požadovaným v žiadosti CSR;
-je možné overiť podpis certifikátu pomocou verejného koreňového kľúča ERCA uvedeného v poli CAR.

Ak výsledok ktorejkoľvek z týchto kontrol bude negatívny, SK-CA zruší proces preberania a spojí sa s ERCA. Odmietnutie certifikátu sa riadi procedúrou na odvolanie certifikátu (pozri odsek 4.1.10)..

4.1.6 Použitie párov kľúčov a certifikátov

SK-CA bude využívať každý pár kľúčov a príslušné certifikáty v súlade s ustanoveniami uvedenými v odseku 6.2.

4.1.7 Obnovenie certifikátu

Obnovenie certifikátu, t.j. predĺženie doby platnosti existujúceho certifikátu, nie je dovolené.

4.1.8 Obnovenie certifikátu kľúča

Obnovenie certifikátu kľúča znamená podpísanie nového certifikátu SK-CA, ktorý nahradí existujúci certifikát.
4.1.8 Obnovenie certifikátu kľúča sa realizuje:

- Keď sa u SK-CA blíži ku koncu doba využívania (jedného z) jej súkromných kľúčov. V takomto prípade sa obnovenie certifikátu kľúča realizuje včas, aby sa zabezpečilo, že SK-CA bude pokračovať v činnosti aj po uplynutí tohto obdobia;
- po zrušení certifikátu.

Podanie žiadosti o certifikát, jeho spracovanie, vydanie, prevzatie a zverejnenie sú rovnaké ako pri počiatočnom páre kľúčov. SK-CA bude bezodkladne distribuovať personalizátorom komponentov potrebné kľúče a certifikáty spôsobom opísaným v SK-CA CPS.
Páry kľúčov SK-CA sa môžu pravidelne meniť. ERCA nestanovuje žiadne obmedzenia na počet certifikátov SK-CA, ktoré podpíše. SK-CA má dovolené požadovať viacnásobné certifikáty SK-CA toho istého typu, s prekrývajúcimi sa obdobiami platnosti, ak je to potrebné pre jej činnosť.

4.1.9 Úpravy certifikátov

4.1.9 Úpravy certifikátov nie sú povolené.

4.1.10 Zrušenie a pozastavenie platnosti certifikátu

4.1.10.1 Podmienky pre zrušenie certifikátu

Certifikáty SK-CA budú zrušené za nasledujúcich okolností:

- odmietnutie prevzatia novo vydaného certifikátu (pozri odsek 4.1.5);
- odkrytie alebo podozrenie na odkrytie súkromného kľúča SK-CA;
- strata súkromného kľúča SK-CA;
- ukončenie činnosti SK-CA;
- SK-MSA alebo SK-CA si neplnia povinnosti podľa nariadenia a pravidiel certifikácie ERCA.

4.1.10.2 Kto môže požiadať o zrušenie certifikátu

ERCA považuje za rozhodujúce žiadosti o zrušenie certifikátu, ktoré pochádzajú od nasledovných subjektov:

- zodpovedná organizácia EÚ;
- národné organizácie všetkých členských štátov EÚ;
- všetky uznané certifikačné autority členských štátov EÚ (MSCA);

Európska Certifikačná organizácia je oprávnená požadovať zrušenie akéhokoľvek certifikátu od certifikačnej autority členského štátu EÚ (MSCA).
Zodpovedná organizácia členského štátu (MSA) je oprávnená požadovať zrušenie certifikátov vydaných certifikačnými autoritami členského štátu EÚ (MSCA), ktoré sú uvedené v certifikačných pravidlách MSA.
Certifikačná autorita členského štátu EÚ (MSCA) je oprávnená požadovať zrušenie certifikátov, ktoré sama vydala.
ERCA zamietne žiadosti o zrušenie certifikátu pochádzajúce od akéhokoľvek iného subjektu.

4.1.10.3 Postup pri podávaní žiadosti o zrušenie certifikátu

Postup zrušenia certifikátu je opísaný v SK-CA CPS.

4.1.10.4 Lehota na zrušenie certifikátu

Lehota na zrušenie certifikátu je päť pracovných dní od vyskytnutia sa okolností podmieňujúcich zrušenie certifikátu, v rámci ktorej objednávateľ certifikátu podá žiadosť o jeho zrušenie.

4.1.10.5 Doba, v rámci ktorej ERCA realizuje žiadosť o zrušenie certifikátu

ERCA spracováva riadne, úplné a autorizované žiadosti o zrušenie certifikátov do troch pracovných dní od prijatia žiadosti.

4.1.10.6 Požiadavky na kontrolu zo strany závislých strán ohľadom zrušenia certifikátu

Závislé strany sú zodpovedné za kontrolu informácií o stave certifikátov publikovaných v úložisku ERCA.

4.1.10.7 Frekvencia vydávania certifikátov

Stav certifikátov verejných kľúčov ERCA a MSCA je možné zistiť on-line na adrese https://dtc.jrc.ec.europa.eu/. ERCA udržuje integritu informácií o stave rušenia certifikátov.
Informácie o stave certifikátov publikovaných v úložisku ERCA sa aktualizujú prvý pracovný deň každého týždňa.

4.1.10.8 Maximálna latencia pre CRL

Nevzťahuje sa.

4.1.10.9 On-line zrušenie certifikátu/dostupnosť kontroly stavu

Dostupnosť informácií o zrušení certifikátu/stavových informácií publikovaných v úložisku ERCA je zaručená iba počas bežnej pracovnej doby.

4.1.10.10 Požiadavky na on-line zrušenie certifikátu/kontrolu stavu

Nie sú stanovené.

4.1.10.11 Iné formy zrušenia publikovania, ktoré sú k dispozícii

Žiadne.

4.1.10.12 Osobitné požiadavky týkajúce sa odkrytia kľúčov

Odkrytie kľúčov je bezpečnostný incident, ktorý je potrebné spracovať.
Ak dôjde k odkrytiu kľúčov SK-CA (MSCA_Card.SK), alebo ak existuje podozrenie, že došlo k ich odkrytiu, SK-CA nahlási do 8 hodín tento incident do ERCA a SK-MSA.
Následné vyšetrovanie vedie SK-MSA a podnikne všetky potrebné kroky s cieľom znížiť potenciálne riziko zneužitia odkrytého kľúča.

4.1.10.13 Pozastavenie platnosti certifikátu

Pozastavenie platnosti certifikátu nie je povolené.

4.1.11 Služba informovania o stave certifikátu

Dostupnosť webovej stránky uvedenej v odseku 4.1.10.7 je zaručená počas bežnej pracovnej doby.
Zoznam informácií o stave certifikátu MSCA je tiež možné stiahnuť z tejto webovej stránky v bežnom formáte súborov (napr. CSV, Excel).

4.1.12 Ukončenie objednávania služby

Objednávanie služby podpisovania certifikátov od ERCA sa končí, ak sa organizácia SK-MSA rozhodne ukončiť činnosť SK-CA. SK-MSA túto zmenu oznámi ERCA ako zmenu pravidiel certifikácie SK-MSA.
V prípade ukončenia objednávania služby je zodpovednosť za rozhodnutie podať žiadosť o zrušenie certifikátu pre všetky platné certifikáty SK-CA, alebo o povolenie ukončenia platnosti všetkých certifikátov SK-CA u SK-MSA.

4.1.13 Úschova kľúčov u tretej strany a ich obnova

Uloženie kľúčov u tretej strany je výslovne zakázané, čo znamená, že súkromné kľúče SK-CA sa nikdy nebudú exportovať alebo uchovávať v akomkoľvek inom systéme okrem prevádzkových a záložných systémov SK-CA.

4.2 Aplikácia a distribúcia symetrického hlavného kľúča medzi ERCA a SK-CA

Nasledujúce požiadavky úzko súvisia s príslušnou kapitolou pravidiel certifikácie ERCA 2. gen.

4.2.1 Aplikácia hlavného kľúča

Ako je uvedené v prílohe 1C k nariadeniu EÚ č. 799/2016, dielenské karty musia byť vybavené hlavným kľúčom snímača pohybu - časť dielenská karta (KM-WC). Tento kľúč je potrebný na to, aby dielňa mohla spárovať snímač pohybu s jednotkou vozidla.
V prílohe 1C sa tiež uvádza, že kontrolné karty a dielenské karty musia byť vybavené hlavným kľúčom DSRC. Tento kľúč je potrebný na to, aby umožnil pracovníkovi kontroly dešifrovať správu prijatú z jednotky vozidla cez pripojenie DSRC a overiť jej autentickosť. Dielne potrebujú tento kľúč na overenie, či jednotka vozidla dokáže takéto správy odosielať.
Tieto hlavné kľúče generuje ERCA. Distribúciu týchto kľúčov môže požadovať SK-CA, ako je uvedené v pravidlách certifikácie ERCA.
Aby bolo možné tieto hlavné kľúče uložiť na príslušné karty, SK-CP musí mať tieto kľúče k dispozícii. Proces distribúcie týchto kľúčov na vysokej úrovni z ERCA do SK-CP (prostredníctvom SK-CA) je nasledujúci:

1. SK-CP podľa pravidiel certifikácie ERCA vygeneruje požiadavku na distribúciu kľúčov (KDR) pre hlavný kľúč, vrátane generovania páru efemérnych (dočasných) kľúčov pre odsúhlasenie kľúčov v ich hardvérovom bezpečnostnom module (HSM);
2. SK-CP odošle KDR do SK-CA;
3. SK-CA overuje správnosť KDR podľa odseku 4.2.2.1 pravidiel certifikácie ERCA;
4. SK-CA odošle KDR do ERCA prostredníctvom kuriéra, ako je uvedené v pravidlách certifikácie ERCA a vo vyhlásení ERCA CPS. SK-CA musí spĺňať všetky platné požiadavky uvedené v odseku 4.2.2 pravidiel certifikácie ERCA;
5. ERCA vytvorí správu pre distribúciu kľúčov (KDM), ako je uvedené v pravidlách certifikácie ERCA, a odošle ju späť do SK-CA;
6. SK-CA overí správnosť KDM podľa odseku 4.2.6 pravidiel certifikácie ERCA;
7. SK-CA odošle KDM do SK-CP;
8. SK-CP spracúva KDM, ako je uvedené v odseku 4.2.6 pravidiel certifikácie ERCA;

4.2.1.1 Požiadavky na distribúciu kľúčov

Požiadavky na distribúciu kľúčov môžu predkladať iba organizácie MSCA uznané ich národnými organizáciami MSA prostredníctvom vyhlásenia o zhode (pozri odsek 1.5.2).
KDR musí byť bo formáte TLV.

Dátový objekt	**Požadované**	**Tag**
Požiadavka na distribúciu kľúčov	m	‘A1’
Identifikátor profilu požiadavky	m	‘5F 29’
Autorizácia príjemcu správy	m	‘83’
Identifikátor kľúča	m	‘84’
Verejný kľúč (pre odsúhlasenie kľúča ECDH)	m	‘7F 49’
Štandardizované parametre domény OID	m	‘06’
Verejný bod	m	‘86’

Tabuľka 2: Formát požiadavky na distribúciu kľúčov

Verzia profilu sa identifikuje prostredníctvom **Identifikátora profilu požiadavky**. Verzia 1 uvedená v tabuľke 2 bude identifikovaná pomocou hodnoty ‘00’.

Autorizácia príjemcu správy sa používa na identifikáciu požadovaného symetrického kľúča. Pozostáva z reťazca, zloženého zo

- šiestich vyšších bajtov identifikátora (ID) aplikácie tachografu (‘FF 53 4D 52 44 54’),
- typu požadovaného kľúča (uvedené nižšie, 1 bajt),
- čísla verzie požadovaného hlavného kľúča (1 bajt),.

Na určenie typu požadovaného kľúča sa použijú nasledujúce hodnoty:

- ‘07’: KM, hlavný kľúč snímača pohybu
- ‘27’: KM-WC, dielenská časť hlavného kľúča snímača pohybu
- ‘67’: KM-VU, časť VU hlavného kľúča snímača pohybu
- ‘09’: KM-DSRC, hlavný kľúč DSRC

Identifikátor kľúča je jedinečný 8-bajtový oktetový reťazec, ktorý identifikuje verejný kľúč, ktorý sa nachádza v požiadavke na distribúciu (KDR) pri výmene kľúča ECDH, pozri odsek 4.2.3. Jeho hodnota sa určuje podľa odseku 3.1.1.2. Pretože MSCA používa pre každú požiadavku na distribúciu kľúčov iný pár efemérnych kľúčov, SK-CA môže použiť identifikátor kľúča na sledovanie efemérneho súkromného kľúča, ktorý sa použije na dešifrovanie určitej správy s distribúciou kľúčov po tom, ako dorazila do SK-CA. Z tohto dôvodu ERCA skopíruje identifikátor kľúča do správy s distribúciou kľúčov, pozri tabuľku 3.

Verejný kľúč obsahuje dva dátové prvky:

- Dátový prvok „Public Point" obsahuje verejný bod páru efemérnych kľúčov SK-CA, ktorý sa použije na odsúhlasenie kľúčov. SK-CA konvertuje verejný bod na oktetový reťazec podľa normy ISO/IEC 18033-2, pričom použije nekomprimovaný formát kódovania..
- Dátový prvok „Domain Parameters" obsahuje identifikátor objektu súboru štandardizovaných parametrov domény, ktoré sa použijú spolu s verejným bodom. Viac informácií nájdete v odseku 4.2.3.

SK-CA vypočíta a uchová kontrolný súčet (hash) za celú požiadavku na distribúciu (KDR), s využitím hašovacieho algoritmu zviazaného s veľkosťou požadovaného hlavného kľúča, ako je uvedené v prílohe IC dodatku 11, CSM_50. Tento kontrolný súčet (hash) ERCA použije na overenie autentickosti požiadavky KDR, pozri odsek 4.2.2.1.

4.2.2 Spracovanie hlavného kľúča aplikácie

4.2.2.1 Overenie obsahu KDR

Pred odoslaním požiadavky na distribúciu kľúčov do ERCA, prijatej od SK-CP, si musí SK-CA overiť, či:

- formát KDR spĺňa špecifikácie uvedené v odseku 4.2.1 pravidiel certifikácie ERCA;
- typ hlavného kľúča požadovaného v KDR je KM-WC alebo KDSRC;
- číslo verzie hlavného kľúča zodpovedá číslu (jednému z čísiel) verzie publikovaných ERCA;
- dočasný identifikátor verejného kľúča nebol predtým použitý ani na účely skúšky interoperability;
- sú dočasné parametre domény uvedené v žiadosti rovnaké ako parametre domény v súčasnosti používaných certifikátov SK-CA;
- nebol dočasný verejný bod v žiadosti certifikovaný SK-CA v certifikáte tachografovej karty. Tiež, či sa predtým nepoužil na distribúciu kľúčov, prípadne na skúšku interoperability;
- dočasný verejný bod uvedený v žiadosti sa nachádza na krivke uvedenej v žiadosti;
- Ak bude výsledok niektorej z týchto kontrol negatívny, SK-CA neodošle požiadavku KDR do ERCA, ale oznámi problém SK-CP. SK-CP potom vygeneruje novú požiadavku KDR.

Ak boli všetky kontroly úspešné, SK-CA vypočíta a uloží kontrolný súčet (hash) za celú požiadavku na distribúciu kľúčov (KDR) s využitím hašovacieho algoritmu viazaného na veľkosť požadovaného hlavného kľúča, ako je uvedené v prílohe 1C k nariadeniu EÚ 799/2016, dodatok 11, CSM_50. Tento kontrolný súčet (hash) použije ERCA na overenie autenticity požiadavky KDR, pozri oddiel 4.2.2.1 pravidiel certifikácie ERCA..
Následne SK-CA odošle požiadavku KDR do ERCA prostredníctvom kuriéra.

ERCA zaistí, aby žiadosť KDR prichádzajúca od MSCA bola kompletná, presná a riadne schválená. Iba v takom prípade ERCA vytvára správy s distribúciou kľúčov.
Kontroly správnosti, úplnosti a schválenia vykonávajú úradníci ERCA manuálne, prípadne automatizovane prostredníctvom registračnej služby ERCA. Ak je požiadavka správna a úplná, pracovníci ERCA môžu povoliť generovanie správy s distribúciou kľúčov prostredníctvom služby distribúcie kľúčov.
ERCA pri každej prijatej požiadavke KDR overí, či

- prenosové média sú čitateľné, t. j. či nie sú poškodené, alebo či sú neporušené;
- formát KDR zodpovedná tabuľke č. 2;
- je požiadavka náležite schválená. ERCA kontaktuje MSCA, ako je opísané vo vyhlásení CPS ERCA, a overuje, či sa kontrolný súčet (hash) vypočítaný na základe prijatej požiadavky KDR zhoduje s kontrolným súčtom (hashom) uvedeným v KDR, ktorý zapísala MSCA (pozri koniec odseku 4.2.1).;
- Certifikačná autorita členského štátu EÚ (MSCA) je oprávnená získať požadovaný typ hlavných kľúčov:
    - MSCA zodpovedná za vydávanie tachografových kariet bude oprávnená prijímať všetky platné verzie kľúčov KM-WC týkajúce sa použitého systému šifrovania a hlavný kľúč DSRC $K_{M\text{-}DSRC}$;
    - Certifikačné autority MSCA zodpovedné za vydávanie jednotiek vozidla (VU) budú oprávnené prevziať KM-VU časť a hlavný kľúč DSRC $K_{M\text{-}DSRC;}$
    - Certifikačné autority MSCA zodpovedné za vydávanie snímačov pohybu budú oprávnené prevziať všetky platné verzie KM týkajúce sa použitého systému šifrovania;

Vezmite na vedomie, že ak MSCA prevzala nielen $K_{M\text{-}WC,}$ ale aj $K_{M\text{-}VU}$ s platným systémom šifrovania, mohla by si aj sama generovať zodpovedajúci kľúč K_M. Organizácie MSCA to však nerobia, dokonca aj keď potrebujú kľúč KM na vydávanie snímačov pohybu. MSCA, ktorá potrebuje KM, požiada ERCA o distribúciu tohto kľúča.

- či daná MSCA v minulosti už nepožadovala daný typ a verziu hlavného kľúča. Ak áno, ERCA preskúma dôvod, prečo bola podaná žiadosť o prerozdelenie;
- či efemérny verejný kľúč uvedený v požiadavke MSCA nebol certifikovaný zo strany ERCA v minulosti, alebo či sa predtým nepoužil na distribúciu kľúčov, prípadne na skúšku interoperability;
- či sú parametre domény špecifikované v požiadavke uvedené v tabuľke 1 prílohy IC, dodatku 11 a úroveň týchto parametrov zodpovedá dĺžke požadovaného symetrického kľúča (pozri odsek 4.2.3, krok 2);
- verejný bod uvedený v žiadosti sa nachádza na krivke uvedenej v žiadosti.

Ak bude výsledok niektorej z týchto kontrol negatívny, ERCA odmietne požiadavku KDR. ERCA oznámi MSCA a MSA dôvod každého odmietnutia požiadavky.

4.2.2.2 Generovanie, distribúcia a administrácia správ KDM

Ak boli všetky kontroly úspešné, ERCA pokračuje v príprave správy pre distribúciu kľúčov určením symetrického kľúča, ktorý požaduje MSCA, a postupuje podľa krokov opísaných v odseku 4.2.3 (od 2. kroku)
Pre každú prijatú požiadavku na distribúciu kľúčov sa do databázy ERCA zapisujú nasledujúce informácie:

- kompletná požiadavka KDR prichádzajúca od MSCA;
- prípadná úplná výsledná správa pre distribúciu kľúčov;
- štandardizované parametre domény OID, dočasný verejný bod a identifikátor kľúča;
- typ kľúča a verzia hlavného kľúča;
- kontrolný súčet (hash) uvedený v správe pre distribúciu binárneho kľúča, ak bol vygenerovaný. Dĺžka kontrolného súčtu (hashu) je zviazaná s veľkosťou kľúča podpisujúcej autority, ako je uvedené v prílohe IC, dodatku 11, CSM_50;
- kontrolný súčet (hash) binárnych údajov požiadavky na distribúciu kľúčov (KDR), pozri odsek 4.2.1;
- stav „Distribuované“ v prípade, ak bol kľúč distribuovaný do MSCA alebo „Odmietnuté“ v prípade zamietnutia požiadavky KDR.;
- časová pečiatka.

ERCA si uschováva prenosové médiá s KDR a archivuje ich vo svojich strážených priestoroch.
Po vygenerovaní správy pre distribúciu kľúčov ju ERCA odošle do MSCA, ako je uvedené v odseku 4.2.5.
Cieľom ERCA je dokončiť distribúciu kľúčov v rámci jedného pracovného dňa. Zaručená doba spracovania požiadavky je jeden mesiac. Pri požiadavke na distribúciu kľúčov príslušné organizácie členských štátov MSCA musia zobrať do úvahy túto maximálnu dobu spracovania.

4.2.3 Ochrana dôvernosti a autenticity symetrických kľúčov

Ochrana dôvernosti a autenticity symetrických kľúčov distribuovaných z ERCA do jednotlivých MSCA je zabezpečená prostredníctvom schémy šifrovania využívajúcej integrovanú eliptickú krivku (ECIES). Táto schéma umožňuje odsúhlasenie šifrovacích a MAC kľúčov, ktoré sa využívajú na ochranu hlavných symetrických kľúčov pri distribúcii od ERCA do MSCA. V norme ISO/IEC 18033-2 bol štandardizovaný variant ECIES. Variant ECIES, ktorý sa využíva na distribúciu symetrických kľúčov ERCA, používa v súlade s dodatkom 11 prílohy IC nasledujúce kryptografické algoritmy:

- Funkcia derivácie kľúčov: KDF2, ako sa uvádza v norme ISO/IEC 18033-2;
- Algoritmus kódovej autentizácie správy: Algoritmus AES v režime CMAC, ako je uvedené v norme NIST, Špeciálna publikácia 800-38B;
- Symetrický šifrovací algoritmus: AES v režime reťazenia šifrovacích blokov (CBC), ako je uvedené v norme ISO/IEC 10116.

Na vysokej úrovni sa ECIES skladá z nasledujúcich krokov. Ďalšie podrobnosti pre jednotlivé kroky sú uvedené nižšie:

- MSCA vygeneruje jedinečný dočasný pár kľúčov ECC pre Diffie-Hellmanov algoritmus odsúhlasenia kľúčov a v žiadosti pre distribúciu kľúčov (KDR) odošle verejný kľúč do ERCA, pozri tabuľku 2.
- Podobným spôsobom ERCA generuje jedinečný pár dočasných kľúčov ECDH a využíva Diffie-Hellmanov algoritmus odsúhlasenia kľúčov, spolu s vlastným súkromným kľúčom a dočasným verejným kľúčom MSCA na odvodenie zdieľania utajovaných údajov.
- S využitím funkcie odvodenia kľúča, zdieľania utajovaných údajov a ďalších informácií uvedených nižšie ERCA odvodí šifrovací kľúč a kód overenia správy (MAC).
- Na šifrovanie symetrického kľúča, ktorý sa má distribuovať, vyžíva ERCA šifrovací kľúč.
- Na výpočet kódu overenia správy (MAC) pre zašifrovaný kľúč využíva ERCA MAC kľúč.

Krok 1
MSCA si na generovanie svojho dočasného verejného kľúča použitého pri Diffie-Hellmanovom algoritme odsúhlasenia kľúčov zvolí jeden zo štandardizovaných parametrov domény z tabuľky 1 uvedenej v prílohe IC dodatku 11. Úroveň zvolených parametrov domény musí zodpovedať dĺžke požadovaného symetrického kľúča, v súlade s CSM_50 uvedenej v dodatku 11. Generovanie dočasného páru kľúčov sa realizuje v HSM, ktorý spĺňa požiadavky uvedené v odseku 6.2. Dočasný súkromný kľúč nikdy neopustí HSM. Po vygenerovaní páru dočasných kľúčov MSCA skonvertuje verejný bod na oktetový reťazec, ako je uvedené v ISO/IEC 18033-2. Použije sa nekomprimovaný formát kódovania. MSCA zahrnie do požiadavky KDR, ktorú zasiela ERCA, OID zvolených štandardizovaných parametrov domény a oktetový reťazec predstavujúci verejný bod v KDR.

Krok 2
ERCA vygeneruje dvojicu efemérnych kľúčov pomocou štandardizovaných parametrov domény špecifikovaných v prijatej KDR. ERCA použije algoritmus ECKA-DH, ako je definované v norme ISO/IEC 18033-2, spolu s vlastným dočasným súkromným kľúčom a dočasným verejným kľúčom MSCA na odvodenie zdieľaného bodu (Kx, Ky). ERCA skontroluje, či tento bod nie je bodom v nekonečne. Ak áno, ERCA vygeneruje nový pár dočasných kľúčov a znova vykoná kontrolu. V opačnom prípade ERCA vytvorí zdieľanú utajovanú informáciu K prostredníctvom prevodu Kx na oktetový reťazec, ako je uvedené v norme ISO/IEC 18033-2. Generovanie páru dočasných kľúčov sa realizuje v hardvérovom bezpečnostnom module (HSM), ktorý spĺňa požiadavky uvedené v odseku 6.2. Dočasný súkromný kľúč nikdy neopustí HSM.

Krok 3
Na odvodenie šifrovacieho kľúča KENC a kľúča KMAC pre kódovanie overenia správy využíva ERCA funkciu odvodzovania kľúčov KDF2(x, l) definovanú v ISO/IEC 18033-2. Oktetový reťazec x bude rovný zdieľaným utajovaným údajom K z predchádzajúceho kroku. Funkcia kontrolného súčtu, ktorá je potrebná na vytvorenie inštancie funkcie KDF2 bude zviazaná s dĺžkou symetrického kľúča, ktorý sa má distribuovať tak, ako je opísané Dodatku č. 11 CSM_50.Výstupná dĺžka „l" sa rovná dĺžke výstupu z tejto funkcie kontrolného súčtu (hašovacej funkcie).
Ak „O" je výstup tejto funkcie odvodzovania kľúčov, potom sa kľúče na zašifrovanie a kľúče na výpočet kódu overenia správy (MAC) vytvoria ako

- K_{ENC} = prvé L oktety výstupu „O"

- K_{MAC} = posledné L oktety výstupu „O"

kde L je požadovaná dĺžka K_{ENC} a K_{MAC} v oktetoch , v súlade s dodatkom 11 CSM_50.

Krok 4
Ak je to potrebné (napr. pre 192 bytový kľúč), ERCA vloží symetrický kľúč, ktorý sa má distribuovať, s využitím 2. metódy vkladania definovanej v norme ISO/IEC 9797-1. ERCA následne zašifruje vložený kľúč pomocou algoritmu AES v režime zreťazenia šifrovaných blokov (CBC), ako je definované v norme ISO/IEC 10116, s využitím kľúča K_{ENC} s parametrom prekladania (interleave) m = 1 a inicializačným vektorom SV, ktorý obsahuje binárne nuly:

Zašifrovaný symetrický kľúč= AES-CBC (symetrický kľúč + prípadná „výplň", K_{ENC})

Krok 5
ERCA zreťazí zašifrovaný symetrický kľúč s reťazcom S, ktorý predstavuje zreťazenie hodnôt „Autorizácie príjemcu správy" a „Identifikátora kľúča", ktoré boli použité v správe o distribúcii kľúčov (pozri odsek 4.2.4)

S = Autorizácia príjemcu správy || Identifikátor kľúča

S využitím kľúča K_{MAC} potom ERCA vypočíta kód overenia správy (MAC) pre spojený reťazec šifrovaného symetrického kľúča a reťazca S s využitím algoritmu šifrovania AES v režime CMAC, ako je uvedené v špeciálnej publikácii NIST Special Publication 800-38B. Dĺžka kódu overenia správy (MAC) bude zviazaná s dĺžkou kľúčov relácie AES (session keys), ako je uvedené v dodatku 11 CSM_50.

MAC = AES-CMAC (zašifrovaný symetrický kľúč|| S, K_{MAC})

Akékoľvek operácie s dočasným súkromným kľúčom, so zdieľanými utajovanými údajmi a s derivovanými kľúčmi K_{ENC} a K_{MAC} sa budú realizovať v hardvérovom bezpečnostnom module (HSM), ktorý spĺňa požiadavky uvedené v odseku 6.2.
ERCA bude viesť evidenciu hodnôt S a MAC. Ako je opísané v oddiele 4.2.6, organizácie MSCA použijú tieto hodnoty na overenie pravosti správy pre distribúciu kľúčov.

4.2.4 Správy pre distribúciu kľúčov

Po spracovaní požiadaviek na hlavné kľúče (pozri odsek 4.2.2) ERCA vytvorí správu pre distribúciu kľúča, ako je uvedené tabuľke č. 3. Na dĺžku správy sa použijú pravidlá DER kódovania uvedené v norme (ISO/IEC 8825-1). Hodnoty sú uvedené vo zvyšnej časti tejto časti.

Dátový objekt	**Požadované**	**Tag**
Distribúcia kľúča	m	'A1'
Identifikátor profilu požiadavky	m	'5F 29'
Autorizácia príjemcu správy	m	'83'
Identifikátor kľúča páru dočasných kľúčov MSCA pre usporiadanie kľúčov ECDH	m	'84'
Verejný bod ERCA pre usporiadanie kľúčov ECDH	m	'86'
Zašifrovaný symetrický kľúč	m	'87'
MAC	m	'88'

Tabuľka 3: Formát správy s distribúciou kľúčov

Verzia profilu sa identifikuje prostredníctvom **Identifikátora profilu požiadavky**. Verzia 1 špecifikovaná v tabuľke 3 sa identifikuje hodnotou '00'.
Autorizácia príjemcu správy je totožná s dátovým prvkom autorizácie príjemcu správy uvedeným v požiadavke od MSCA na distribúciu KDR, pozri odsek 4.2.1.

Verejný bod obsahuje verejný bod páru dočasných kľúčov ERCA použitých na odsúhlasenie kľúčov, pozri odsek 4.2.3. ERCA s využitím nekomprimovaného formátu kódovania skonvertuje verejný bod na oktetový reťazec špecifikovaný v technickej príručke BSI TR-03111 .
Dátový prvok **Zašifrovaný symetrický kľúč** obsahuje výstup z kroku 4 v odseku 4.2.3.

Dátový prvok MAC obsahuje výstup z kroku 5 v odseku 4.2.3.
Po úspešnom vygenerovaní správy pre distribúciu kľúčov ERCA bezpečne zlikviduje v HSM svoj dočasný súkromný kľúč pre odsúhlasenie kľúčov, ako aj šifrovací kľúč K_{ENC} a kľúč K_{MAC} pre výpočet kódu overenia správy (MAC).
Správa pre distribúciu kľúčov bude doručená späť MSCA, ktorá vydala požiadavku KDR.

4.2.5 Komunikovanie požiadaviek a odpovedí

Na prenos požiadaviek na distribúciu kľúčov a správ pre distribúciu kľúčov by sa malo použiť médium typu CD-R:

- CD-R je 12 cm médium nahrávané v režime single-session (formát ISO 9660: 1988).

Iné spôsoby prepravy sa môžu použiť po predchádzajúcom odsúhlasení zo strany ERCA. ERCA pre potreby skúšok akceptuje požiadavky na distribúciu kľúčov a zasiela požiadavky a správy pre distribúciou kľúčov ako prílohy e-mailov.
MSCA musí nahrať na prenosové médium pre prenos do ERCA tri kópie každej žiadosti o distribúciu kľúčov. Tieto kópie musia byť v hexadecimálnom ASCII (súbor .txt), Base64 (súbor .pem) a v binárnom (súbor .bin) formáte.
ERCA pre odoslanie do MSCA zapíše na prenosové médium tri kópie každej správy pre distribúciu kľúčov. Tieto kópie musia byť v hexadecimálnom ASCII (súbor .txt), Base64 (súbor .pem) a v binárnom (súbor .bin) formáte.
Požiadavka KDR aj správa KDM musia mať ako prílohu papierovú kópiu údajov, formátovaných podľa predlohy definovanej vo vyhlásení ERCA CPS. Ďalšia papierová kópia údajov sa musí uchovávať u ERCA, prípadne MSCA.
Požiadavky KDR aj správy KDM, prenosové médiá a výtlačky si zamestnanci ERCA a kuriéri MSCA musia odovzdávať v strážených priestoroch JRC.

4.2.6 Prevzatie hlavného kľúča

Kuriér podpíše prevzatie správy pre distribúciu kľúčov v priestoroch ERCA. Po odovzdaní správy pre distribúciu kľúčov v priestoroch MSCA, musí MSCA skontrolovať, či:
- prenosové média sú čitateľné, t. j. či nie sú poškodené, alebo či sú neporušené;
- formát správy je v súlade s tabuľkou č. 3
- je správa hodnoverná. MSCA to urobí tak, že kontaktuje ERCA, ako je opísané vo vyhlásení o certifikačných postupoch ER-CA CPS, a overí si, či sa kód MAC v prijatej správe KDM zhoduje s kódom MAC v KDM odoslaným z ERCA;
- typ a verzia hlavného kľúča v správe sa zhodujú s požadovaným typom a verziou;
- verejný bod uvedený v správe je na krivke špecifikovanej v požiadavke na distribúciu kľúča, ktorú MSCA odoslala do ERCA.

Ak je výsledok niektorej z kontrol negatívny, MSCA proces preruší a kontaktuje ERCA.
Ak boli všetky kontroly úspešné, MSCA vykoná nasledovné:
- použije algoritmus ECKA-DH na odvodenie zdieľaného bodu (K_x, K_y) opísaného v kroku 3 v odseku 4.2.3, s využitím dočasného súkromného kľúča MSCA označeného identifikátorom obsiahnutým v správe a dočasného verejného kľúča od ERCA. MSCA si musí overiť, či sa zdieľaný bod nenachádza v nekonečne; ak áno, MSCA proces zruší a spojí sa s ERCA. V opačnom prípade MSCA vytvorí zdieľané utajované údaje K tak, že konvertuje K_x na oktetový reťazec špecifikovaný v Technickej príručke BSI TR-03111;
- odvodí kľúče K_{ENC} a K_{MAC} opísané v kroku 4 v odseku 4.2.3;

- overí si kód MAC vzťahujúci sa k zašifrovanému symetrickému kľúču spôsobom opísaným v kroku 5 v odseku 4.2.3. Ak bude výsledok overenia negatívny, MSCA proces preruší a kontaktuje ERCA;
- dešifruje symetrický kľúč spôsobom opísaným v kroku 4 v odseku 4.2.3. Ak má dešifrovaný kľúč „výplň", MSCA overí, či je správne. Ak bude výsledok overenia negatívny, MSCA proces preruší a kontaktuje ERCA.

Akékoľvek operácie s dočasným súkromným kľúčom, so zdieľanými utajovanými údajmi a derivovanými kľúčmi K_{ENC} a K_{MAC} sa budú realizovať v hardvérovom bezpečnostnom module (HSM), ktorý spĺňa požiadavky uvedené v odseku 6.2. Po úspešnom získaní hlavného kľúča alebo po prerušení procesu distribúcie kľúčov, pričom nebola iniciovaná obnova správy s distribuovaným kľúčom KDM (pozri odsek 4.2.8), MSCA v HSM bezpečne zlikviduje svoj dočasný súkromný kľúč použitý pre odsúhlasenie kľúčov, ako aj šifrovací kľúč K_{ENC} a kľúč K_{MAC} pre výpočet kódu overenia správy (MAC).
Pri komunikácii medzi SK-CA a SK-CP sú formáty správ, kryptografické mechanizmy a postupy pri podávaní žiadosti o distribúciu a pri distribúcii certifikátov pre zariadenia a pri distribúcii symetrických kľúčov pre karty uvedené vo vyhlásení o certifikačných postupoch SK-CA CPS.

4.2.7 Používanie hlavného kľúča

Každý hlavný kľúč musí MSCA používať v súlade s ustanoveniami uvedenými v odseku 6.2.

4.2.8 Obnovenie KDM

Obnovenie KDM znamená vydanie kópie existujúcej správy KDM pre MSCA bez zmeny dočasného verejného kľúča alebo akýchkoľvek iných informácií uvedených v KDM.
Obnovenie správy KDM sa môže realizovať iba vtedy, ak je pôvodné prenosové médium, ktoré MSCA prevzala, poškodené alebo porušené. Poškodenie alebo porušenie prenosového média sa považuje za bezpečnostný incident, ktorý sa musí nahlásiť do MSA a ERCA. Následne po takomto oznámení môže MSCA zaslať do ERCA požiadavku na obnovenie KDM s odvolaním sa na pôvodnú požiadavku na distribúciu kľúča. Tento postup je opísaný v certifikačných postupoch ERCA CPS.
ERCA akceptuje iba požiadavky na obnovenie KDM schválené MSCA, ktoré schválila MSA.
Poznámka: Ak MSCA potrebuje zaslať žiadosť o opätovnú distribúciu hlavného kľúča, ktorý už bol do MSCA úspešne distribuovaný, vygeneruje novú žiadosť o distribúciu kľúča pomocou novo vygenerovaného páru dočasných kľúčov. Takáto požiadavka môže viesť ERCA k iniciovaniu vyšetrovania možnosti ohrozenia dôvernosti šifrovacieho kľúča.

4.2.9 Použitie opätovne vydaného hlavného kľúča

Ak ERCA vygenerovala novú verziu hlavného kľúča, spôsobom uvedeným v odsekoch 9.2.1.2 a 9.2.2.2 dodatku č.11, dostupnosť nového kľúča bude uverejnená na webovej stránke ERCA, spolu s číslom verzie a dĺžkou kľúča.
Pre získanie novej verzie hlavného kľúča musí SK-CA zaslať novú požiadavku na distribúciu kľúča (KDR). Vyžiadanie nového hlavného kľúča je potrebné urobiť včas tak, aby sa kľúč (alebo odvodené kľúče alebo šifrované údaje pre snímače pohybu) mohol včas zabudovať do novo vydaných komponentov.
Aplikácia kľúča, jeho spracovanie, distribúcia a prevzatie sú rovnaké ako pri pôvodnom kľúči. Personalizátori kariet musia byť o tom bezodkladne informovaní spôsobom uvedeným vo vyhlásení o certifikačných postupoch SK-CA.

4.2.10 Oznámenie o ohrození dôvernosti symetrického kľúča

Ak SK-CA zistí, alebo bude informovaná o ohrození dôvernosti alebo o podozrení ohrozenia dôvernosti symetrického hlavného kľúča, oznámi to bez zbytočného odkladu ERCA a SK-MSA, najneskôr do 8 hodín od takéhoto zistenia. SK-CA v oznámení uvedie okolnosti, za ktorých došlo k ohrozeniu dôvernosti. Akékoľvek následné vyšetrovanie a možné kroky zo strany SK-MSA, prípadne SK-CA sa musia realizovať postupom uvedeným v pravidlách certifikácie SK-MSA. Výsledok vyšetrovania SK-MSA sa musí odoslať do ERCA.
Ak ERCA zistí, alebo jej bude oznámené ohrozenie dôvernosti alebo podozrenie na ohrozenie dôvernosti symetrického hlavného kľúča, oznámi to ERCA bez zbytočného odkladu a najneskôr do 8 hodín od zistenia

Európskej organizácii. Európske organizácie budú konať príslušným spôsobom. ERCA bude riešiť incident podľa definovaného postupu pre riešenie bezpečnostných incidentov.

4.2.11 Služba zverejňovania stavu hlavných kľúčov

Stav symetrických hlavných kľúčov je možné zistiť on-line na webovej stránke https://dtc.jrc.ec.europa.eu/. ERCA zabezpečí udržiavanie integrity stavových informácií.
Informácie o stave hlavných kľúčov publikovaných v úložisku ERCA sa aktualizujú v prvý pracovný deň každého týždňa.
Dostupnosť vyššie uvedenej webovej stránky je zaručená počas bežnej pracovnej doby.

4.2.12 Koniec poskytovania služby distribúcie kľúčov

Poskytovanie služby distribúcie kľúčov od ERCA bude ukončené, keď sa MSA rozhodne ukončiť činnosť MSCA. MSA túto zmenu oznámi ERCA ako zmenu pravidiel certifikovania v členskom štáte EÚ.
V prípade ukončenia poskytovania služby musí MSCA zaistiť bezpečnú likvidáciu všetkých kópií symetrických hlavných kľúčov, ktoré mala v držbe.

4.2.13 Úschova a obnova kľúčov

Úschova kľúčov je výslovne zakázaná, čo znamená, že symetrické hlavné kľúče sa nesmú exportovať ani ukladať v žiadnych iných systémoch, okrem produkčných a záložných systémov ERCA a MSCA.

4.3 Podávanie žiadosti o certifikát tachografovej karty a jeho vydanie

4.3.1 Podávanie žiadosti o certifikát

SK-CA vydá certifikát iba vtedy, ak je zodpovednej organizácii predložená riadna žiadosť o certifikát a ak boli v čase podania žiadosti splnené všetky požiadavky nariadenia (ES) č. 165/2014 a všetkých súvisiacich právnych predpisov a dohôd.

SK-CA bude akceptovať iba žiadosti o certifikát pre tachografové karty s platným typovým schválením, ako je opísané v Prílohe IC (kapitola 8).

Pre každú tachografovú kartu sa vygeneruje jedinečný pár kľúčov ECC označený ako Card_MA, ktorý sa bude sa používať na vzájomnú autentifikáciu. Pre každú kartu vodiča a každú dielenskú kartu sa navyše vygeneruje druhý jedinečný pár kľúčov ECC označený ako Card_Sign (používaný na podpisovanie údajov). Túto úlohu môžu riešiť výrobcovia kariet alebo personalizátori kariet, ako je to opísané v Dodatku 11 k Prílohe IC (odsek 9.1.5). Vždy, keď sa vygeneruje pár kľúčov pre kartu tachografu, strana, ktorá generuje kľúč, odošle verejný kľúč do SK-CA, aby získala zodpovedajúci certifikát karty podpísaný SK-CA. Súkromný kľúč sa bude využívať iba na karte tachografu. Požiadavky na certifikáciu kľúčov, ktoré závisia od prenosu súkromných kľúčov, nie sú povolené.

4.3.2 Požiadavky na certifikáciu

SK-CP môžu predkladať požiadavky na certifikáciu kľúčov (KCR) iba SK-CA.
Povinnosti SK-CP pri predkladaní požiadavky na certifikát karty sú:

- vytvoriť správu s požiadavkou na certifikáciu kľúčov (KCR) a zaslať ju do SK-CA. Formát a obsah KCR musia byť zhodné s certifikátom tachografovej karty, ktorú má SK-CA podpísať. Podpis KCR sa však musí dať overiť pomocou verejného kľúča obsiahnutého v KCR.
- KCR digitálne podpísať.

Formáty certifikátov a podrobnosti týkajúce sa generovania kľúčov sú uvedené v SK-CA CPS.

4.3.3 Vydávanie certifikátov

SK-CA v rámci svojich právomocí zabezpečí, aby pred vydaním certifikátu SK-CP u príslušných organizácií prebehla náležitá registrácia.
Generovanie kľúčov sa realizuje mimo SK-CA, SK-CA vydá certifikát pre SK-CP iba vtedy, ak sa na základe vopred dohodnutého postupu preukáže, že SK-CP vlastní príslušný súkromný kľúč. Súkromný kľúč by pri tom nemal opustiť zabezpečené prostredie generovania kľúčov.
SK-CA tiež zaistí, aby všetky údaje prichádzajúce z SK-CP boli úplné, presné a riadne schválené. Iba v takomto prípade SK-CA vydá alebo podpíše certifikát pre kartu.
Kontrola správnosti, úplnosti a autorizácie sa môže vykonávať automatizovaným spôsobom iba prostredníctvom systémov SK-CA spôsobom opísaným v SK-CA CPS.

V súlade s dodatkom 11 sú doby platnosti certifikátov pre karty Card_MA nasledovné:

- Pre karty vodičov: 5 rokov
- Pre podnikové karty: 5 rokov
- Pre kontrolné karty: 2 roky
- Pre dielenské karty: 1 rok

Doby platnosti certifikátov podpisov kariet Card_Sign sú nasledovné:

- Pre karty vodičov: 5 rokov a 1 mesiac
- Pre dielenské karty: 1 rok a 1 mesiac

Dátum nadobudnutia platnosti certifikátu musí uvádzať počiatočný dátum a dobu platnosti certifikátu. Je to dátum, kedy SK-CA vydala certifikát.
Certifikáty Card_MA a Card_Sign patriace k určitej karte vodiča alebo dielenskej karte musia mať rovnaký dátum nadobudnutia platnosti. Dátum nadobudnutia platnosti certifikátu kariet je rovnaký ako dátum nadobudnutia platnosti tachografových kariet, ako je zakódované v identifikácii EF.

Doba používania certifikátov Card_MA.SK a Card_Sign.SK je rovnaký ako doba platnosti príslušného certifikátu.

Formát certifikátov Card_MA a Card_Sign je opísaný v odseku 7.2.

Všetky certifikáty karty tachografu musia mať dobu platnosti stanovenú v súlade s dodatkom 11 k prílohe 1C Nariadenia EÚ č. 799/2016.

4.3.4 Akceptovanie certifikátu

SK-CP akceptuje certifikát iba vtedy, ak sa zhoduje s príslušnou požiadavkou na certifikát a ak je možné certifikát overiť voči certifikátu MSCA_Card vydaného SK-CA, ktorý obsahuje súkromný kľúč karty MSCA_Card.PK.

4.3.5 Používanie páru kľúčov a certifikátov

- SK-CP si zvolí úroveň šifrovania páru kľúčov karty rovnajúcu sa úrovni šifrovania páru kľúčov SK-CA použitých na podpísanie príslušného certifikátu karty.
- Karta tachografu bude používať svoj pár kľúčov Card_MA, skladajúci sa zo súkromného kľúča Card_MA.SK a verejného kľúča Card_MA.PK, výhradne na vzájomnú autentizáciu a odsúhlasenie kľúčov pri relácii voči jednotkám vozidla, ako je uvedené v prílohe IC dodatku 11.
- Karta vodiča alebo dielenská karta budú používať súkromný kľúč Card_Sign.SK zo svojho páru kľúčov Card_Sign výhradne na podpisovanie stiahnutých dátových súborov, ako je uvedené v dodatku 11. Zodpovedajúci verejný kľúč Card_Sign.PK sa použije výhradne na overenie podpisov vytvorených kartou.
- Páry kľúčov, symetrické kľúče a čísla pinov sa budú generovať a uchovávať v dôveryhodnom vyhradenom zariadení, ktoré:

- je certifikované na úroveň EAL 4 alebo vyššiu v súlade s normou ISO/IEC 15408 s využitím vhodného profilu ochrany; alebo
- spĺňa požiadavky uvedené v norme ISO/IEC 19790, úroveň 3; alebo
- spĺňa požiadavky stanovené v norme FIPS PUB 140-2 úroveň 3.

Najbežnejšou implementáciou takého dôveryhodného vyhradeného zariadenia na použitie v systéme PKI je hardvérový bezpečnostný modul (HSM).

- Operácie so súkromnými kľúčmi a operácie so symetrickými kľúčmi sa musia vykonávať interne v module HSM, kde sú použité kľúče uložené.
- Súkromné kľúče a symetrické kľúče budú používať pracovníci, ktorí pôsobia v dôveryhodných úlohách za minimálne dvojnásobnej kontroly a iba v rámci fyzicky bezpečného prostredia. Súkromné kľúče a symetrické kľúče sa nesmú spracúvať mimo HSM bez adekvátneho zašifrovania. Všetky prípady použitia súkromného kľúča a použitia symetrického kľúča sa musia evidovať.
- Po vydaní karty sa páry kľúčov a príslušné certifikáty danej tachografovej karty nesmú vymieňať ani obnovovať.
- Tachografové karty po vydaní obsahujú nasledujúce šifrovacie kľúče a certifikáty:
  - súkromný kľúč Card_MA a zodpovedajúci certifikát
  - u kariet vodičov a dielenských kariet je navyše: súkromný kľúč Card_Sign a zodpovedajúci certifikát
  - certifikát MSCA_Card obsahujúci verejný kľúč MSCA_Card.PK, ktorý sa použije na overenie certifikátov Card_MA a Card_Sign
  - certifikát EUR obsahujúci verejný kľúč EUR.PK, ktorý sa používa na overenie certifikátu MSCA_Card
  - certifikát EUR, ktorého doba platnosti priamo predchádza dobe platnosti certifikátu EUR, ak existuje, ktorý sa použije na overenie certifikátu MSCA_Card, .
  - ak existuje, certifikát prepojenia, ktoré spája tieto dva EUR certifikáty,
  - u dielenských kariet symetrické hlavné kľúče $K_{M\text{-}WC}$ a $K_{M\text{-}DSRC}$
  - u kontrolných kariet symetrický hlavný kľúč $K_{M\text{-}DSRC}$
- Okrem vyššie uvedených šifrovacích kľúčov a certifikátov musia tachografové karty obsahovať aj kľúče a certifikáty uvedené v prílohe IC dodatku 11 časti A, ktoré umožňujú týmto kartám interakciu s jednotkami vozidiel (VU) prvej generácie.

4.3.6 Obnovenie certifikátu

Obnovenie certifikátu, t. j. predĺženie doby platnosti existujúceho certifikátu, nie je povolené.

4.3.7 Opätovné zašifrovanie kľúča

Opätovné zašifrovanie kľúča nie je povolené. Po uplynutí platnosti certifikátu a po uplynutí doby používania dvojice kľúčov sa vydávajú nové tachografové karty.

4.3.8 Úpravy certifikátov

Úpravy certifikátov nie sú povolené.

4.3.9 Zrušenie a pozastavenie platnosti certifikátu

Zrušenie platnosti certifikátu tachografovej karty vydanej SK-CA sa nepredpokladá a požiadavka na zrušenie nebude zo strany SK-CA akceptovaná a spracovávaná.

4.3.10 Služby poskytovania informácii o stave certifikátu

Udržovanie informácií o stave certifikátov pre všetky vydané tachografové karty zaisťuje SK-CA. Tieto informácie nebudú zverejňované, ale na požiadanie budú sprístupnené oprávneným stranám.

4.3.11 Ukončenie poskytovania služby

Poskytovanie služby certifikácie zo strany SK-CA sa ukončí, keď sa personalizátor alebo výrobca karty rozhodne využívanie tejto služby ukončiť. Pritom môže uplynúť platnosť všetkých vydaných certifikátov tachografových kariet. Personalizátor karty alebo výrobca karty oznámi ukončenie služby SK-MSA a SK-CA. SK-MSA informuje SK-CIA o ukončení služby a následnom personalizátorovi kariet alebo výrobcoch kariet.

4.3.12 Úschova a obnovenie kľúčov

Úschova kľúčov je výslovne zakázaná, čo znamená, že súkromné kľúče Card_MA.SK a Card_Sign.SK sa nesmú exportovať alebo uchovávať na žiadnom inom mieste, okrem príslušnej tachografovej karty.

5 Prevádzkové priestory, manažment a prevádzkové kontroly

5.1 Bezpečnostné opatrenia týkajúce sa fyzickej bezpečnosti

- Služby generovania kľúčov a certifikátov SK-CA a zodpovedajúcich služieb personalizátora kariet sa môžu poskytovať iba v zabezpečených priestoroch chránených vymedzeným bezpečnostným perimetrom, vybavených vhodnými bezpečnostnými bariérami a kontrolami vstupu, aby sa zabránilo neoprávnenému vstupu do priestorov, poškodeniam zariadení a zasahovaniu do činnosti. Tieto priestory musia byť sledované strážnou službou a musia byť vybavené bezpečnostným výstražným systémom.
- Systémy SK-CA musia mať zaistené náležité napájanie energiami a klimatizáciu, pričom musí byť zaistená ich záloha.
- Systémy SK-CA a personalizátora kariet a pamäťové médiá používané na ukladanie dôverných informácií, ako sú pevné disky, smart karty a moduly HSM, musia byť chránené pred neoprávneným prístupom alebo použitím na iný ako určený účel, pred sprístupnením tretím osobám alebo poškodením zo strany nepovolaných osôb alebo chránené pred inými nebezpečenstvami (napr. požiar, voda).
- Záložné a inštalačné médiá musia byť uložené na oddelenom mieste, ktoré je fyzicky zabezpečené a chránené pred neoprávneným prístupom alebo použitím na iný ako určený účel, pred sprístupnením tretím osobám alebo poškodením zo strany nepovolaných osôb alebo chránené pred inými nebezpečenstvami (napr. požiar, voda).
- Musia byť implementované postupy likvidácie odpadov, aby sa zabránilo neoprávnenému použitiu dôverných údajov, prístupu k nim alebo ich zverejneniu.
- Musí byť zriadené miesto nachádzajúce sa mimo lokality prevádzky slúžiace na ukladanie kritických dát SK-CA a dát potrebných pre obnovenie prevádzky v havarijných prípadoch.

5.2 Bezpečnostné opatrenia týkajúce pracovných postupov

- SK-CA a personalizátor kariet musia mať implementované procedurálne opatrenia pre kontrolu, aby bola zaistená bezpečná prevádzka. Predovšetkým musí byť zaistené rozdelenie zodpovedností tak, aby pri kritických úlohách existovala kontrola viacerými osobami.
- Prístup do systémov SK-CA a zodpovedajúcich systémov personalizátora kariet musí byť obmedzený na jednotlivcov, ktorí sú vybavení náležitými oprávneniami, s obmedzením podľa princípu nevyhnutnosti pre ich prácu. Predovšetkým musia byť implementované opatrenia na obmedzenie prístupu:
    - Dôverné údaje musia byť pri uchovávaní chránené tak, aby sa zabezpečila ich integrita a dôvernosť;
    - Pri prenose údajov po nezabezpečených sieťach sa musia dôverné údaje chrániť tak, aby sa zabezpečila ich integrita a dôvernosť;
    - Zmazané dôverné údaje sa musia zlikvidovať trvalým spôsobom, napr. niekoľkonásobným spoľahlivým prepisom náhodnými údajmi.

- Systémy SK-CA a zodpovedajúce systémy personalizátora kariet musia umožňovať efektívnu administráciu a správu prístupových práv;
- Systémy SK-CA a zodpovedajúce systémy personalizátora kariet musia zaistiť, aby prístup k informáciám a funkciám aplikačného systému bol obmedzený iba na oprávnené osoby a musia byť zaistené dostatočné opatrenia počítačovej bezpečnosti umožňujúce oddelenie funkcií zviazaných s dôvernými údajmi. Predovšetkým musí byť obmedzené a prísne kontrolované používanie systémových pomocných programov (utilít). Prístup musí byť obmedzený tak, aby umožňoval prístup iba k zdrojom potrebným na realizáciu úloh pridelených používateľovi;
- Pred využívaním systémov SK-CA alebo príslušných systémov personalizátora kariet sa musia zamestnanci SK-CA a personalizátora identifikovať.
- Zamestnanci SK-CA a personalizátora karty sú zodpovední za svoje činnosti, ktoré sa musia zaznamenávať do denníkov udalostí, ako je to opísané v odseku 5.4;

- SK-CA a personalizátor kariet musia mať zavedený systém riadenia informačnej bezpečnosti (ISMS) založený na posudzovaní rizík pre všetky realizované operácie. Musia zaistiť, aby pravidlá ISMS riešili školenie personálu, previerky a funkcie jednotlivých pracovníkov. Implementácia ISMS musí byť v súlade s požiadavkami opísanými v ISO 27001.

5.3 Bezpečnostné opatrenia týkajúce sa personálu

- Povinnosti SK-CA je možné preniesť na externú špecializovanú spoločnosť alebo je možné na personál zmluvného partnera preniesť plnenie povinností SK-CA.
- Všetok zúčastnený personál SK-CA alebo zodpovedajúci personál personalizátora kariet musí byť riadne vyškolený a musí mať odborné znalosti, skúsenosti a kvalifikáciu potrebnú pre poskytovanie ponúkaných služieb a musí mať zodpovedajúce pracovné zaradenie. Týka sa to personálu zamestnávaného priamo, personálu špecializovanej spoločnosti, na ktorú boli prenesené úlohy, alebo personálu zmluvných partnerov.
- Pre školenie personálu musí byť vypracovaný plán školení opísaný v príslušných postupoch certifikácie CPS alebo v bezpečnostnej koncepcii.
- Vymenovávanie osôb do funkcií so zodpovednosťou ohľadom utajovaných skutočností sa musí riadiť v súlade s procesom previerok definovaným v príslušných postupoch certifikácie CPS alebo v bezpečnostnej koncepcii.
- Funkcie so zodpovednosťou ohľadom utajovaných skutočností, od ktorých závisí bezpečnosť prevádzky, musia byť v príslušnom CPS alebo bezpečnostnej koncepcii jasne identifikované. Tieto funkcie a s nimi súvisiace zodpovednosti musia byť zdokumentované v koncepcii pracovných funkcií alebo v porovnateľnom dokumente. Túto koncepciu funkcií je potrebné definovať z hľadiska oddelenia zodpovedností a čo najnižších privilégií. Žiadna jednotlivá osoba nesmie byť oprávnená súčasne vykonávať viac ako jednu z funkcií spojených so zodpovednosťou ohľadom utajovaných skutočností.

5.4 Postupy evidencie auditov

Všetky významné bezpečnostné udalosti v softvéri SK-CA alebo v súvisiacom softvéri personalizátora kariet sa automaticky označia časovou pečiatkou a zaznamenajú do systémových denníkov. Zahŕňa minimálne nasledujúce udalosti:

- Úspešné a neúspešné pokusy o vytvorenie, aktualizáciu, odstránenie alebo načítanie informácií o stave účtov zamestnancov alebo o nastavení alebo zrušení oprávnení v účte;
- Úspešné a neúspešné pokusy o nastavenie alebo zmenu spôsobu autentizácie (napr. heslo, biometrický, kryptografický certifikát), ktorá sa viaže k osobnému účtu;
- Úspešné a neúspešné pokusy o prihlásenie a odhlásenie z účtu;
- Úspešné a neúspešné pokusy o zmenu konfigurácie softvéru;
- Spustenie a zastavenie softvéru;
- Aktualizácie softvéru;
- Spustenie a vypnutie systému;

- Úspešné a neúspešné pokusy o pridanie alebo odobratie subjektu z registra objednávateľov služieb, pre ktorých SK-CA aktuálne poskytuje služby certifikácie kľúčov alebo pokusy o zmenu akýchkoľvek údajov u ktoréhokoľvek z objednávateľov alebo pokusy o získanie informácií z registra.;
- Úspešné a neúspešné pokusy spracovať požiadavku na podpísanie certifikátu alebo požiadavku na distribúciu kľúča;
- Úspešné a neúspešné pokusy podpísať certifikát alebo vygenerovať správu pre distribúciu kľúčov;
- Úspešné a neúspešné interakcie s databázou (databázami) obsahujúcimi údaje o (stave) vydaných certifikátov vrátane pokusov o pripojenie a operácií čítania, zápisu a aktualizácie alebo odstránenia záznamov;
- Úspešné a neúspešné pokusy o pripojenie alebo odpojenie od modulu HSM.
- Úspešné a neúspešné pokusy o autentizáciu používateľa modulu HSM.
- Úspešné a neúspešné pokusy o vygenerovanie alebo likvidáciu páru kľúčov alebo symetrického kľúča uloženého vo vnútri modulu HSM;
- Úspešné a neúspešné pokusy importovať kľúč do modulu HSM alebo ho z neho exportovať;
- Úspešné a neúspešné pokusy zmeniť stav životného cyklu u ľubovoľného páru kľúčov alebo pri symetrickom kľúči;
- Úspešné a neúspešné pokusy použiť súkromný kľúč alebo symetrický kľúč vo vnútri HSM na akýkoľvek účel.

Aby bolo možné preskúmať bezpečnostné incidenty, ak je to možné, musí systémový denník obsahovať informácie umožňujúce identifikáciu osoby alebo účtu, ktorý vykonal systémové úlohy.
Musí byť udržiavaná integrita protokolov udalostí systému a musí byť chránená pred neoprávneným prehliadaním, zmenou, vymazaním alebo likvidáciou. Denníky systémových udalostí sa musia zálohovať a uchovávať interne.

5.5 Archivácia evidencie

- Prehľad udalostí, ktoré sa majú archivovať, musí byť opísaný vo vnútorných postupoch a musí byť v súlade s príslušnými pravidlami a predpismi. SK-CA a personalizátori kariet musia implementovať náležité postupy archivácie evidencie. Musia byť zavedené postupy na zaistenie integrity, autentickosti a dôvernosti evidencie.
- Všetky archivované informácie majú neobmedzenú dobu archivácie.
- Je potrebné prijať opatrenia, ktoré zabezpečia, aby bol archív evidencie uchovávaný primeraným spôsobom, ktorý vylučuje stratu informácií.
- Udalosti uvedené v odseku 5.4 sa musia pravidelne kontrolovať z hľadiska ich integrity. Tieto kontroly sa vykonávajú minimálne raz ročne.

5.6 Zmena kľúčov

- SK-CA bude generovať nové páry kľúčov SK-CA podľa potreby. Po tom, ako SK-CA vygeneruje nový pár kľúčov, zašle požiadavku na opätovné certifikovanie kľúčov spôsobom opísaným v príslušnej časti pravidiel certifikácie ERCA a zašle kľúče personalizátorom komponentov spôsobom opísaným v odseku „obnova kľúčov" v kapitole 4 týchto pravidiel certifikácie.
- SK-CA musí zaistiť, aby nové kľúče boli generované v kontrolovaných podmienkach a v súlade s postupmi definovanými v týchto pravidlách certifikácie.

5.7 Obnova po havárii a ohrození dôvernosti kľúčov

- SK-CA a personalizátori kariet musia definovať postupy pre riešenie bezpečnostných incidentov a pri ohrození dôvernosti kľúčov v „Príručke postupov riešenia bezpečnostných incidentov", ktorá musí byť poskytnutá administrátorom systémov a audítorom.
- SK-CA a personalizátori kariet musia mať vypracovaný plán kontinuity činnosti, s podrobným opisom spôsobu, ako budú zaisťovať poskytovanie služieb v prípade incidentu, ktorý má dopad na bežný chod podniku. Po zistení incidentu sa prevádzka pozastaví až do doby, kým sa nestanoví úroveň ohrozenia

dôvernosti. SK-CA a personalizátori kariet tiež predpokladajú, že technologický pokrok spôsobí v priebehu času zastaranie ich IT systémov. V pláne kontinuity činnosti musia byť tiež stanovené opatrenia pre prípady zastaranosti technológie.

- V pláne zálohovania a obnovy musia byť riešené postupy zálohovania a obnovy všetkých dôležitých dát.
- Za havárie sa budú považovať nasledujúce incidenty:
  - ohrozenie dôvernosti alebo krádež súkromného kľúča (SK-CA_Card.SK,), prípadne symetrického hlavného kľúča ($K_{M\text{-}WC}$, $K_{M\text{-}DSRC}$);
  - strata súkromného kľúča (SK-CA_Card.SK) , prípadne symetrického hlavného kľúča ($K_{M\text{-}WC}$, $K_{M\text{-}DSRC}$);
  - porucha hardvéru IT.
- V prípade ohrozenia dôvernosti alebo odcudzenia súkromného kľúča SK-CA použitého na podpísanie certifikátov verejného kľúča tachografových kariet (SK-CA_Card.SK), SK-CA bezodkladne informuje SK-MSA, organizáciu vydávajúcu karty (CIA), dotknuté subjekty personalizátorov komponentov a ERCA. Všetky dotknuté strany musia v primeranej časovej lehote prijať náležité opatrenia.
- V prípade ohrozenia dôvernosti alebo odcudzenia jedného alebo viacerých symetrických hlavných kľúčov uložených u SK-CA, EA a ERCA pri novo určených ($K_{M\text{-}VU}$, $K_{M\text{-}WC}$, $K_{M\text{-}DSRC}$), musí SK-CA o tom ihneď informovať SK-MSA, ERCA a personalizátorov príslušných komponentov. Všetky dotknuté strany musia v primeranej časovej lehote prijať náležité opatrenia.
- Pri strate súkromných kľúčov SK-CA alebo symetrických hlavných kľúčov sa žiadna obnova kľúčov prakticky nevykonáva. Strate kľúčov sa preto musí predchádzať použitím viacerých záložných kópií príslušných kľúčov a hlavných kľúčov, ktoré sa musia pravidelne kontrolovať.
- Ochrana pred poruchami hardvéru IT sa zaisťuje prostredníctvom redundancie, t. j. dostupnosťou zdvojeného hardvéru IT.

5.8 Ukončenie poskytovania služby

- V prípade ukončenia činnosti SK-CA zo strany tejto vymenovanej organizácie, SK-MSA o tom informuje EA a ERCA a prípadne informuje EA a ERCA o novo vymenovanej SK-CA. SK-MSA musí zabezpečiť, aby bola neustále v prevádzke aspoň jedna SK-CA.
- V prípade ukončenia služby personalizátora karty musia byť o tom informované SK-CA, SK-MSA a SK-CIA a SK-MSA prípadne informuje EA a ERCA. SK-MSA musí zaistiť, aby neustále fungoval aspoň jeden personalizátor kariet. SK-MSA bude informovať SK-CIA, EA a ERCA o novo menovanom personalizátorovi kariet.

6 Technické bezpečnostné opatrenia

6.1 Generovanie a inštalácia párov kľúčov

- SK-CA a personalizátori kariet budú generovať súkromné kľúče v súlade s prílohou IC, dodatkom 11.
- Generovanie párov kľúčov a hlavných kľúčov musia realizovať vo fyzicky zabezpečených priestoroch osoby, ktoré zastávajú funkcie spojené s previerkou, kde je zaistená vzájomná kontrola minimálne dvoch osôb. Postup generovania kľúčov sa musí zdokumentovať.
- SK-CA musí mať v súlade s nariadením k dispozícii skúšobný systém SK-CA na účely skúšky interoperability. Skúšobný systém SK-CA musí predstavovať samostatný systém a musí mať vlastné súkromné kľúče SK-CA a symetrické hlavné kľúče. Skúšobný systém SK-CA musí byť schopný požiadať o podpis skúšobného certifikátu a distribuovať symetrické skúšobné kľúče s využitím procesov opísaných v tomto dokumente a pravidlách certifikácie ERCA. Skúšobný systém SK-CA musí byť tiež schopný na požiadanie personalizátorov komponentov podpísať skúšobné certifikáty zariadení a distribuovať skúšobné symetrické kľúče a zašifrované údaje snímačov pohybu jednotlivým personalizátorom komponentov.

6.2 Ochrana súkromných kľúčov a ochranné opatrenia pre kryptografické moduly

- SK-CA a SK-CP - personalizátori kariet musia zachovávať dôvernosť, integritu a dostupnosť súkromných kľúčov a symetrických kľúčov spôsobom opísaným v tejto časti pokynov.
- Súkromné kľúče a symetrické kľúče sa musia generovať a využívať výhradne v „hardvérovom bezpečnostnom module" (HSM) alebo na tachografovej karte. SK-CP preto musí žiadať, importovať a uchovávať všetky hlavné kľúče výhradne v module HSM alebo na čipovej karte. V oboch prípadoch musí modul HSM:
    - byť certifikovaný na úrovni EAL 4 alebo vyššej v súlade s normou ISO/IEC 15408 s využitím náležitého profilu ochrany; alebo
    - spĺňať požiadavky uvedené v norme ISO/IEC 19790 úroveň 3; alebo
    - spĺňať požiadavky uvedené vo FIPS PUB 140-2 úroveň 3; alebo
    - ponúkať ekvivalentnú úroveň bezpečnosti podľa porovnateľných vnútroštátnych alebo medzinárodne uznávaných hodnotiacich kritérií pre bezpečnosť IT.

  V prípade generovania páru kľúčov na karte sa na generovanie kľúčov vzťahuje certifikácia bezpečnosti karty podľa spoločných kritérií. Na generovanie párov kľúčov sa musia použiť verejne špecifikované a náležité kryptografické algoritmy. Operácie so súkromnými kľúčmi a operácie so symetrickým kľúčom sa vykonávajú výhradne interne v module HSM alebo na čipovej karte, kde sa použité kľúče uchovávajú. Vyššie uvedené požiadavky sa vzťahujú iba na produkčné kľúče. Kľúče používané na skúšku interoperability sa môžu generovať a používať mimo modulu HSM.
- SK-CA a personalizátori kariet SK-CP môžu používať súkromné kľúče a symetrické kľúče iba v rámci fyzicky zabezpečených priestorov prostredníctvom osôb, ktoré zastávajú funkcie spojené s previerkou, kde je zaistená vzájomná kontrola minimálne dvoch osôb. Všetky prípady použitia súkromných kľúčov a symetrického hlavného kľúča sa musia evidovať.
- SK-CA a personalizátori kariet SK-CP musia zálohovať, uchovávať a čítať súkromné kľúče a symetrické kľúče iba prostredníctvom osôb ktoré zastávajú funkcie spojené s previerkou, kde je zaistená vzájomná kontrola minimálne dvoch osôb a vo fyzicky zabezpečených priestoroch.
- Záložné kópie súkromných kľúčov a symetrických kľúčov SK-CA a personalizátorov kariet podliehajú rovnakej úrovni bezpečnostných kontrol ako kľúče, ktoré sa aktuálne využívajú.
- Jedna záložná kópia každého súkromného kľúča a hlavného kľúča SK-CA sa musí uchovávať mimo lokalitu SK-CA.
- Import a export súkromného kľúča sa môže realizovať iba na účely zálohovania a prečítania kľúča.
- Import a export symetrického kľúča je iba na účely zálohovania a prečítania kľúča. SK-CA má dovolené exportovať $K_{M\text{-}VU}$ a $K_{M\text{-}WC}$ v zašifrovanej podobe v prípade požiadavky na distribuovanie platných kľúčov zo strany personalizátora komponentov prostredníctvom osôb, ktoré zastávajú funkcie spojené s previerkou, kde je zaistená vzájomná kontrola minimálne dvoch osôb.
- Na konci životného cyklu súkromného kľúča SK-CA alebo symetrického hlavného kľúča (podľa špecifikácie v SK-CA CPS) sa musia všetky kópie kľúča zničiť tak, aby sa nedali obnoviť.
- Ak dôjde k ohrozeniu dôvernosti súkromných a symetrických kľúčov musia sa deaktivovať a zlikvidovať. Kľúče budú zlikvidované po tom, ako bolo preskúmané ohrozenie ich dôvernosti a bolo prijaté rozhodnutie o ich deaktivácii.
- Likvidácia súkromných kľúčov a hlavných kľúčov sa realizuje prostredníctvom funkcie modulu HSM likvidácie kľúčov. Musia sa tiež zlikvidovať aj záložné kópie kľúčov, u ktorých došlo k ohrozeniu ich dôvernosti.

6.3 Ostatné aspekty manažmentu párov kľúčov

- Certifikáty verejného kľúča SK-CA, a teda verejné kľúče, majú neobmedzenú lehotu archivácie.
- Lehota platnosti všetkých certifikátov SK-CA musí byť v súlade s dodatkom 1 prílohy IC.
- V zmysle prílohy IC, dodatku č. 11 je lehota využívania súkromných kľúčov SK-CA dva roky. Lehota využívania súkromného kľúča začína dňom nadobudnutia platnosti príslušného certifikátu. SK-CA nesmie po uplynutí lehoty využívania súkromného kľúča tento kľúč použiť.

6.4 Aktivačné údaje

- Súkromné kľúče, prípadne symetrické hlavné kľúče SK-CA, uložené v module HSM, sa budú aktivovať pre použitie, ak sa všetky osoby, ktoré majú ku kľúču prístup, autentizovali v module HSM. Autentizácia sa realizuje prostredníctvom náležitých prostriedkov (napr. prístupových fráz, autentizačných predmetov (tokenov)).
- Dĺžka trvania relácie overenia totožnosti nesmie byť neobmedzená.
- Na aktiváciu samotného softvéru SK-CA sa použije overenie totožnosti používateľa pomocou náležitého prostriedku (napr. pomocou prístupovej frázy).

6.5 Opatrenia počítačovej bezpečnosti

- Personalizátor kariet SK-CA musí špecifikovať a odsúhlasiť pracovné postupy a špecifické technické bezpečnostné opatrenia pre manažment svojich počítačových systémov. Tieto postupy zaručujú, že bude vždy dodržaná požadovaná úroveň bezpečnosti. Pracovné postupy a technické bezpečnostné opatrenia musia byť opísané v interných dokumentoch, prípadne v bezpečnostných koncepciách. Počítačové systémy musia byť usporiadané a spravované v súlade s týmito pracovnými postupmi, postupmi uvedenými v bezpečnostných koncepciách a osvedčenými postupmi pre centrá dôveryhodnosti a pre dôveryhodné počítačové spracovanie.

6.6 Bezpečnostné opatrenia týkajúce sa životného cyklu

- SK-CA a personalizátori kariet musia vo fáze návrhu a špecifikácie požiadaviek vykonať analýzu bezpečnosti, aby bolo zaistené, že bezpečnosť bude súčasťou ich systémov.
- Musí sa zachovať oddelenie systému schválenia (alebo pred produkcie) a systému produkcie certifikátov. Pracovné postupy pre realizáciu zmien a manažment bezpečnosti musia zaručovať udržiavanie požadovanej úrovne bezpečnosti v Systéme produkcie.
- Pracovné postupy pre realizáciu zmien musia byť zdokumentované a využívať sa pre vydávanie, úpravy a (mimoriadne) opravy softvéru pri akomkoľvek prevádzkovom softvéri.

6.7 Bezpečnostné opatrenia týkajúce sa počítačovej siete

SK-CA a personalizátori kariet musia navrhnúť a implementovať architektúru svojej siete tak, aby bolo možné efektívne obmedziť prístup z internetu do ich vnútornej siete a prístup z internej siete do systémov certifikačnej autority a súvisiacich systémov personalizátora kariet;

6.8 Používanie časovej pečiatky

Čas a dátum udalosti musí byť súčasťou každého záznamu auditu. Dokument SK-CA CPS a súvisiace dokumenty /CPS personalizátora kariet musia definovať, akým spôsobom sa synchronizuje a overuje časová informácia.

7 Certifikát, profily CRL a OCSP

7.1 Profil certifikátu

Všetky certifikáty musia mať profil uvedený v prílohe IC dodatkoch 11 a 1:

Dátový objekt	Požiad.	ID poľa	Tag	Dĺžka (v bajtoch)	ASN.1 dátový typ
Certifikát ECC (CV)	m	C	'7F 21'	var	
Telo certifikátu	m	B	'7F 4E'	var	
Identifikátor profilu certifikátu	m	CPI	'5F 29'	'01'	INTEGER (0…255)
Odkaz na certifikačnú autoritu	m	CAR	'42'	'08'	Identifikátor kľúča
Autorizácia držiteľa certifikátu	m	CHA	'5F 4C'	'07'	Autorizácia držiteľa certifikátu
Verejný kľúč	m	PK	'7F 49'	var	
Štandardizované parametre domény OID	m	DP	'06'	var	IDENTIFIKÁTOR OBJEKTU
Verejný bod	m	PP	'86'	var	OKTETOVÝ REŤAZEC
Odkaz na držiteľa certifikátu	m	CHR	'5F 20'	'08'	Identifikátor kľúča
Dátum nadobudnutia platnosti certifikátu	m	CEfD	'5F 25'	'04'	TimeReal
Dátum uplynutia platnosti certifikátu	m	CExD	'5F 24'	'04'	TimeReal
Podpis certifikátu ECC	m	S	'5F 37'	var	OKTETOVÝ REŤAZEC

Tabuľka 4: Profil certifikátu

Algoritmus sa označuje prostredníctvom štandardizovaného identifikátora doménových parametrov OID, ako je uvedené v tabuľke 1 dodatku č.11 prílohy IC. Možnosti sú nasledujúce:

Názov	Označ. identifikátora objektu	Hodnota identifikátora objektu
NIST P-256	secp256r1	1.2.840.10045.3.1.7
BrainpoolP256r1	brainpoolP256r1	1.3.36.3.3.2.8.1.1.7
NIST P-384	secp384r1	1.3.132.0.34
BrainpoolP384r1	BrainpoolP384r1	1.3.36.3.3.2.8.1.1.11

Tabuľka 5: Povolené štandardizované parametre domény OID

7.2 Formát certifikátu (úroveň zariadenia)

Certifikáty úrovne zariadení pre inteligentný tachografový systém sú podľa noriem ISO/IEC 7816-4 a 7816-8 predstavované ECC certifikátmi verejných kľúčov, spolu s niektorými osobitnými požiadavkami:

- „kartou overiteľné" (CV):

Certifikáty je možné počas overovania interpretovať na čipovej karte (operácia VERIFY CERTIFICATE).

- „samoopisné":

Pre kódovanie dátových štruktúr ASN.1s a dátových objektov vo vnútri certifikátov sa musí použiť kódovanie „Distinguished Encoding Rules (DER)" v súlade s normou ISO 8825-1. Výsledkom je nasledujúca štruktúra TLV:

- Tag: Tag sa kóduje pomocou jedného alebo dvoch oktetov a indikuje obsah.
- Dĺžka: Dĺžka je kódovaná ako celé číslo bez znamienka v jednom, dvoch alebo troch oktetoch, čoho výsledkom je maximálna dĺžka 65535 oktetov. Je potrebné použiť minimálny počet oktetov.

- Hodnota: Hodnota sa kóduje oktetmi od nuly až po niekoľko oktetov.

Vydaný certifikát zariadenia má variabilnú dĺžku. Formáty certifikátov zariadení pre tachografové karty (Card_MA.C a Card_Sign.C) je nasledovný:

Pole	**Tag**	**Dĺžka**	**Hodnota**	**Poznámky**
C	‘7F 21’	var		ECC certifikát
B	‘7F 4E’	var		Telo ECC certifikátu
CPI	‘5F 29’	‘01’	‘00’	Identifikátor profilu certifikátu
CAR	‘42’	‘08’	CertificationAuthori-tyKID	Odkaz na certifikačnú organizáciu; verejný kľúč na overenie podpisu (zodpovedá CHR v MSCA_Card. C)
nationNumeric		*1 bajt*	*‘2D‘ pre Slovensko*	Číselný kód krajiny pre Slovensko: -13 (‘0x2D’)
nationAlpha		*3 bajty*	IA5String ’ 53 4B 20’ pre Slovensko	Abecedný kód krajiny– IA5 reťazec s dĺžkou 3 bajty: pre Slovensko ‚SK’ a jedna medzera
keySerialNumber		*1 bajt*		*Sériové číslo kľúča INTEGER (0…255)*
additionalInfo		*2 bajty*	- nepoužité: ‘FF FF’ - pre TC: ‘54 43‘ - pre VU: ‘56 55‘	Doplnková informácia týkajúca sa SK-CA
caIdentifier		*1 bajt*	*‘01’*	*Identifikátor na rozlíšenie medzi identifikátormi CA kľúčov – hodnota: ‘0x01’*
CHA	‘5F 4C’	‘07’		Autorizácia držiteľa certifikátu
tachographAppli-cationID		6 *bajtov*	*- Tachografová karta a VU:* *‘FF 53 4D 52 44 54’* *- EGF:* ‘FF 44 54 45 47 4D‘	6 prvých bajtov identifikátora aplikácie (AID) („SMRDT“) („DTEGM“)
equipmentType		1 *bajt*	’01’, ’02’, ’03’, 04’, ’06’, ’08’, ’11’, ’12’ or ’13’	S registrovaným certifikátom zodpovedajúcim typu zariadenia: - Tachografové karty: - karta vodiča: ‘0x01‘ - dielenská karta: ‘0x02‘ - kontrolná karta: ‘0x03‘ - podniková karta: ‘0x04‘ - podpis karty vodiča: ‘0x11‘ - podpis dielenskej karty: ‘0x12‘
PK	‘7F 49’	var		Verejný kľúč
DP	‘06’	var	definovaný identifikátor objektu	Parameter domény; ID objektu pre odkaz na štandardizované parametre domény
PP	‘86’	var	OKTETOVÝ REŤAZEC	Verejný bod (1); konvertovaný na oktetový reťazec (nekomprimovaný formát)
CHR	‘5F 20’	‘08’	ExtendedSerialNumber alebo CertificateRequestID	Držiteľ certifikátu. Odkaz na verejný kľúč uvedený v certifikáte
serialNumber		*4 bajty*	INTEGER (0..232-1)	Jedinečné sériové číslo certifikátu

				žiadosť na uvedeného výrobcu / personalizátora a mesiac alebo jedinečné sériové číslo zariadenia uvedeného výrobcu, typ zariadenia, mesiac a rok.
monthYear		*2 bajty*	BCDString	Mesiac a rok žiadosti o certifikát alebo výroby zariadenia, zakódované v BCD kóde (2 číslice pre mesiac, posledné dve číslice pre rok)
type		*1 bajt*	EquipmentType (‘01‘, ‘02‘, ‘03‘, ‘04‘, ‘06‘, ‘08‘) or ‘FF‘	Typ zariadenia: - v prípade rozšíreného sériového čísla: Typ zariadenia: - karta vodiča: ‘0x01‘ - dielenská karta: ‘0x02‘ - kontrolná karta: ‘0x03‘ - podniková karta: ‘0x04‘ - v prípade požiadavky na certifikát ID: ‘0xFF‘
manufacturerCode		*1 bajt*		Číselný kód výrobcu typovo schváleného zariadenia
CEfD	‘5F 25’	‘04’	TimeReal	Dátum nadobudnutia platnosti certifikátu, dátum a čas lehoty platnosti certifikátu (zodpovedá dátumu vygenerovania certifikátu)
CExD	‘5F 24’	‘04’	TimeReal	Dátum uplynutia platnosti certifikátu Koncový dátum a čas lehoty platnosti certifikátu
S	‘5F 37’	var		Podpis ECC certifikátu (2) ECDSA podpis vzťahujúci sa na telo certifikátu v jednoduchom formáte

Tabuľka 6: Formát certifikátu inteligentného tachografu pre úroveň zariadenia

Komentár:

(1) Verejné body na eliptických krivkách sa konvertujú na oktetové reťazce s použitím nekomprimovaného formátu kódovania, ako je podrobne opísané v TR-03111. Na šifrovanie bodu na eliptickej krivke sa musia vykonať overovania uvedené v TR-03111.

Nekomprimované kódovanie PU bodu $P=(x_P, y_P)$:

PU=C||X||Y, s

C=0x04

$X=FE2OS(x_P)$

$Y=FE2OS(y_P)$

Dekódovanie:

P=(OS2FE(X),OS2FE(Y))

Overenie:

Musí sa preukázať, že bod P sa skutočne nachádza na eliptickej krivke:

$$y_p^2 = x_p^3 + ax_p + b$$

(2) Podpis certifikátu sa generuje na základe zakódovaného tela certifikátu, vrátane tagu a dĺžky tela certifikátu. Podľa DSS sa musí na podpis použiť algoritmus ECDSA s využitím algoritmu kontrolného súčtu (hash), ktorý je naviazaný na dĺžku kľúča podpisujúcej entity. Formát podpisu je obyčajný text, ako sa uvádza v TR-03111.

Podpis (r,s), vygenerovaný ako podpis ECDSA zakódovaný systémom DER s hodnotou 0x30 b1 0x02 b2 (vr)0x02 b3 (vs) sa musí formátovať ako OKTETOVÝ REŤAZEC R||S, t. j. ako spojenie oktetového reťazca R=I2OS(r,l) a reťazca S=I2OS(s,l) s dĺžkou l=[$\log_{256}$n] s výslednou pevnou dĺžkou 21 oktetov.

7.3 Profil CRL

Nebude publikovaný žiadny profil CRL.

7.4 Profil OCSP

Nepoužije sa žiadny profil OCSP.

8 Audit dodržiavania legislatívy a iné hodnotenia

8.1 Frekvencia alebo okolnosti hodnotenia

- Úplný a formálny audit činnosti SK-CA, SK-CIA a SK-CP sa vykonáva na príkaz SK-MSA. Pri audite sa zisťuje, či sa dodržiavajú požiadavky týchto pravidiel certifikácie a pravidiel ERCA. SK-MSA musí vykonať prvý audit do 12 mesiacov od začatia činností, na ktoré sa vzťahujú schválené pravidlá certifikácie SK-MSA.
- Pred začiatkom prevádzky, na ktorú sa vzťahujú pravidlá certifikácie SK-MSA, musí SK-MSA vykonať predprevádzkové posúdenie s cieľom preukázať, že je organizácia je schopná fungovať v súlade s požiadavkami uvedenými v pravidlách certifikácie SK-MSA.
- Ak sa pri audite nepreukáže žiadny nesúlad s predpismi, nasledujúci audit sa vykoná do 12 až 24 mesiacov. Ak sa pri audite zistí nedodržiavanie predpisov, do 12 mesiacov sa vykoná následný audit, aby sa overilo, či boli porušenia odstránené.
- V prípade vážneho bezpečnostného incidentu sa musí vykonať mimoriadny audit do 6 mesiacov od zistenia incidentu. Za vážne incidenty sa v tejto súvislosti považujú strata integrity alebo dôvernosti súkromných, prípadne symetrických kľúčov. Takýto audit sa zameria na okolnosti a následné opatrenia súvisiace s incidentom. Mimoriadny audit po bezpečnostnom incidente nemá vplyv na bežnú frekvenciu auditov opísaných v bode 8.1
- SK-MSA predkladá správy o výsledkoch auditov a audítorské správy v anglickom jazyku do ERCA. V audítorských správach musia byť definované všetky nápravné opatrenia, vrátane harmonogramu realizácie, ktoré sú potrebné na splnenie záväzkov SK-MSA

8.2 Identita/kvalifikácia hodnotiteľa

- Audit vykonáva nezávislý audítor.
- Každá osoba, ktorá bola vybratá alebo navrhnutá na vykonanie auditu dodržiavania predpisov v SK-CA alebo u personalizátora kariet, musí byť najskôr schválená SK-MSA.
- Mená audítorov, ktorí vykonajú audity, sa zaregistrujú. Títo audítori musia spĺňať nasledujúce požiadavky:

    - Etické správanie - dôveryhodnosť, jednotnosť a dôvernosť, ohľadom ich vzťahu k auditovaným subjektom a zaobchádzania s ich informáciami a dátami;

- Spravodlivá prezentácia - zistenia, závery a správy z auditu sú pravdivé a presne opisujú všetky činnosti vykonané počas auditu;
- Profesionálny prístup - audítor musí mať vysokú úroveň odbornosti a odbornej spôsobilosti a efektívne využívať svoje skúsenosti, ktoré získal vďaka dlhoročnej praxi v odbore informačných technológií, infraštruktúre PKI a súvisiacich technických normách a predpisoch.
- Dobrá povesť- SK-MSA poskytne potvrdenie o bezchybnom správaní.

- Audítor musí mať rozsiahle vedomosti a pokiaľ možno musí byť akreditovaný v oblastiach:

  - Vykonávania auditov bezpečnosti informačných systémov;
  - PKI a šifrovacích technológií;
  - Prevádzkovania softvéru PKI;
  - Príslušných pravidiel a nariadení Európskej komisie.

8.3 Vzťah hodnotiteľa k hodnotenému subjektu

Audítor musí byť nezávislý a nesmie byť prepojený na SK-CA alebo personalizátorov kariet.

8.4 Oblasti, ktoré hodnotenie pokrýva

- Audit organizácie SK-CA alebo personalizátora kariet sa vzťahuje na dodržiavanie certifikačných pravidiel ERCA, certifikačných pravidiel SK-MSA, CPS SK-CA a CPS alebo podobných dokumentov u personalizátora kariet pre inteligentné tachografy 2. generácie, ako aj súvisiacich metód a pracovných postupov zdokumentovaných organizáciou SK-CA alebo personalizátorom kariet.
- Predmetom auditu dodržiavania predpisov bude implementácia technických, procedurálnych a personálnych pracovných postupov opísaných v týchto dokumentoch. Audity sa zameriavajú na niektoré z nasledujúcich oblastí:

  - Identifikácia a autentizácia;
  - Prevádzkové funkcie/služby;
  - Bezpečnostné opatrenia v oblasti fyzickej bezpečnosti, bezpečnosti pracovných postupov a personálnej bezpečnosti;
  - Bezpečnostné opatrenia v technickej oblasti;
  - Postupy riešenia bezpečnostných incidentov.

- Prostredníctvom vyhodnotenia protokolov z auditu je potrebné určiť, či sa nevyskytujú nedostatky v bezpečnosti systémov organizácie SK-CA alebo u personalizátorov kariet. Zistené (možné) nedostatky sa musia odstrániť. O posúdení audítorskej správy a vyhodnotených možných nedostatkoch je potrebné urobiť zápis.
- V prípade mimoriadneho auditu iniciovaného vážnym bezpečnostným incidentom sa audit zameria na procesy a technické opatrenia týkajúce sa bezpečnostného incidentu.

8.5 Opatrenia prijaté v dôsledku nedostatkov

Ak audítor zistí nedostatky vedúce k neplneniu predpisov, SK-CA alebo personalizátor kariet okamžite prijme nápravné opatrenia. Po realizácii nápravných opatrení sa vykoná následný audit do 12 mesiacov.

8.6 Oznamovanie výsledkov

- Nezávislý audítor oznámi auditovanému subjektu (SK-CA alebo personalizátorovi kariet) a SK-MSA úplné výsledky auditu dodržiavania predpisov v slovenskom a anglickom jazyku. SK-MSA zašle organizácii ERCA správu o audite SK-CA zahŕňajúcu príslušné výsledky auditu. Táto správa zahŕňa minimálne počet zistených odchýlok od stanovených predpisov a povahu každej odchýlky. Dátum prijatia správy o audite sa uverejní na webovej stránke ERCA.

- Na žiadosť ERCA jej SK-MSA zašle úplné výsledky auditov dodržiavania predpisov všetkých vyžiadaných subjektov.

9 Ostatné právne a obchodné záležitosti

9.1 Poplatky

Poplatky za symetrické kľúče, šifrovacie služby a certifikáty sa vypočítavajú výhradne na základe skutočných nákladov SK-CA na poskytovanie potrebných služieb.

9.2 Finančná zodpovednosť

Bez ustanovení.

9.3 Dôvernosť obchodných informácií

Ako dôverné informácie sa rozumejú:

- osobné údaje (napr. zamestnancov SK-CA, personalizátora kariet alebo predstaviteľov ERCA);
- súkromné kľúče;
- symetrické hlavné kľúče;
- údaje vo vlastníctve spoločnosti alebo údaje výrobcu;
- dôvody zrušenia certifikátu;
- záznamy z auditov (okrem prípadov, kde sa prístup požaduje zo zákona, na základe predpisov, certifikačných pravidiel alebo stanov vyhlásenia o postupoch certifikácie);
- podrobná dokumentácia manažmentu PKI;
- správy z auditov vykonaných internými alebo externými audítormi.

Dôverné informácie sa nesmú zverejniť s výnimkou prípadov vyžadovaných zákonom.

9.4 Ochrana osobných údajov

V systéme SK-CA sa budú spracovávať a ukladať výhradne osobné údaje predstaviteľov ERCA, SK-CA a personalizátora komponentov.
S týmito údajmi sa bude nakladať v súlade so Všeobecným nariadením o ochrane údajov 2016/679, zákonom č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov.

9.5 Práva duševného vlastníctva

Ministerstvo dopravy Slovenskej republiky má plné vlastnícke práva k softvéru SK-CA tak, ako je uvedené v príslušných zmluvách.

9.6 Vyhlásenia a záruky

SK-CA sa bude riadiť certifikačnými pravidlami ERCA, certifikačnými pravidlami uvedenými v tomto dokumente a v dokumente CPS.

9.7 Odmietnutie záruky

SK-CA odmietne všetky záruky a záväzky akéhokoľvek typu, vrátane akejkoľvek záruky obchodovateľnosti, akejkoľvek záruky vhodnosti na konkrétny účel a akejkoľvek záruky presnosti poskytnutých informácií (okrem

prípadov, kedy pochádzajú z autorizovaného zdroja) a ďalej odmieta zodpovednosť za nedbanlivosť a nedostatočnú starostlivosť zo strany objednávateľov služieb a závislých strán.

9.8 Obmedzenie zodpovednosti za škodu

Ministerstvo dopravy Slovenskej republiky nezodpovedá za akékoľvek škody:

- z dôvodu vojny, prírodných katastrof alebo skutočnosti mimo jeho dosahu;
- ktoré vznikli v dobe od zmeny stavu certifikátu do ďalšieho plánovaného vydania informácií o stave certifikátu;
- z dôvodu neoprávneného používania certifikátov vydaných SK-CA a používania certifikátov nad rámec predpísaného použitia definovaného v týchto certifikačných pravidlách a vo vyhlásení CPS SK-CA;
- spôsobené podvodným alebo nedbanlivým používaním certifikátov príp. informácií o stave certifikátov vydaných SK-CA.

Ministerstvo dopravy Slovenskej republiky odmieta zodpovednosť akéhokoľvek druhu za akékoľvek plnenie, náhradu škody alebo iný nárok alebo povinnosť vyplývajúcu z úmyselného porušenia práva, zmluvných vzťahov alebo z iného dôvodu v súvislosti s akoukoľvek službou spojenou s vydaním, používaním alebo závislosťou od:

- akéhokoľvek certifikátu vydaného SK-CA, alebo s ním spojenými verejnými príp. súkromnými kľúčovými pármi, používanými objednávateľom služieb alebo závislou stranou;
- akéhokoľvek symetrického kľúča distribuovaného SK-CA, používaného objednávateľom služieb alebo závislou stranou;
- akejkoľvek šifrovacej služby poskytovanej SK-CA a využívanej objednávateľom služieb alebo závislou stranou.

Vydávanie certifikátov, symetrických kľúčov a šifrovacích služieb zo strany SK-CA neznamená, že sa Ministerstvo dopravy Slovenskej republiky alebo SK-CA stáva zástupcom, dôverníkom, opatrovníkom alebo iným predstaviteľom žiadateľov alebo závislých strán, alebo iných osôb využívajúcich systém riadenia kľúčov Smart Tachograph.
Objednávatelia služby a závislé strany nemajú nárok na náhradu škody v dôsledku nenáležitého alebo nezákonného využívania tohto systému manažmentu kľúčov.
SK-CA okrem toho nie je sprostredkovateľom transakcií medzi objednávateľmi služieb a závislými stranami.
Sťažnosti voči SK-CA sa obmedzujú na preukázanie, že postupoval spôsobom, ktorý nie je v súlade s týmito certifikačnými pravidlami a pravidlami vyhlásenia o postupoch certifikácie SK-CA.

9.9 Náhrada škody

Bez ustanovení.

9.10 Doba platnosti a ukončenie

Tieto pravidlá certifikácie SK-MSA sú platné od okamihu uvedenia SK-CA do prevádzky. Sú platné až do ďalšieho oznámenia.
Platnosť týchto pravidiel certifikácie SK-MSA sa končí, keď organizácia SK-CA zastaví svoju činnosť alebo keď SK-MSA oznámi, že tieto pravidlá certifikácie už nie sú platné, napr. pretože začala platiť nová verzia certifikačných pravidiel.

9.11 Individuálne oznámenia a komunikácia s účastníkmi

Úradné oznámenia a komunikácia s účastníkmi systému riadenia kľúčov inteligentných tachografov musia byť v písomnej forme a vzťahujú sa na ne evidenčné postupy platné pre korešpondenciu v rámci MT SR.

Oznámenia o rozdelení alebo zlúčení podnikov môžu mať za následok zmeny v rozsahu, správe, prípadne prevádzke SK-CA. V takomto prípade môže byť tiež potrebné upraviť certifikačné pravidlá SK-MSA a dokument SK-CA CPS. Zmeny v týchto dokumentoch sa realizujú spôsobom, ktorý je v súlade s požiadavkami na administratívu uvedenými v odseku 9.12 tohto dokumentu.

9.12 Novelizácie dokumentov

Za vydanie týchto certifikačných pravidiel SK-MSA je zodpovedná SK-MSA. SK-MSA môže tieto pravidlá revidovať, ak to bude považovať za potrebné.
Postup pri navrhovaní zmien a postup schvaľovania týchto certifikačných pravidiel SK-MSA je nasledovný:

1. Pripomienky alebo žiadosti o zmeny v týchto certifikačných pravidlách SK-MSA sa adresujú SK-MSA. Takéto oznámenie musí obsahovať opis pripomienky alebo požadovanej zmeny, odôvodnenie a kontaktné informácie osoby, ktorá predkladá pripomienky alebo žiada zmenu.
2. SK-CA schváli, schváli s úpravami alebo odmietne pripomienky alebo navrhovanú zmenu po skončení lehoty na predkladanie pripomienok. Možnosti SK-CA ohľadom navrhovaných zmien posudzuje SK-MSA. Rozhodovanie o navrhovaných zmenách je v právomoci SK-CA a SK-MSA.
3. Dokument SK-CA „Vyhlásenie o certifikačných postupoch" nie je verejné, avšak je možné ho na vyžiadanie relevantnej zúčastnenej strany sprístupniť.
4. Aktualizované certifikačné pravidlá SK-MSA budú predložené do ERCA na odsúhlasenie.
5. Nová verzia týchto certifikačných pravidiel SK-MSA s informáciami týkajúcimi sa zmien bude publikovaná na webovej stránke SK-MSA www.digitalnytachograf.sk až po ich schválení zo strany ERCA.

Každá zmena v týchto certifikačných pravidiel SK-MSA musí byť sprevádzaná zvýšením čísla verzie dokumentu. Jedinými zmenami, ktoré sa môžu v pravidlách certifikácie a v CPS urobiť bez zmeny čísla verzie dokumentu, sú redakčné alebo typografické opravy.
SK-CA môže zmeniť kontaktné údaje uvedené v odseku 1.5 prostredníctvom notifikácie SK-MSA a ERCA, avšak bez zmeny čísla verzie dokumentu. Všetky ostatné zmeny certifikačných pravidiel (CP) sa vykonávajú v súlade s postupmi pre novelizáciu uvedenými v tejto časti dokumentu.
Všetky relevantné zmeny certifikačných pravidiel SK-MSA sa riadnym spôsobom premietnu do príslušného dokumentu SK-CA CPS.

9.13 Riešenie sporov

Akékoľvek spory súvisiace s manažmentom kľúčov a certifikátov pre digitálny tachografový systém medzi SK-CA a organizáciou alebo jednotlivcami mimo Ministerstva dopravy Slovenskej republiky sa budú riešiť prostredníctvom náležitého mechanizmu riešenia sporov. Ak je to možné, spor sa bude riešiť rokovaním. Spory, ktoré sa nevyriešia rokovaním, sa budú riešiť rozhodcovským konaním sprostredkovaným SK-MSA .

9.14 Rozhodné právo

Presadzovanie, výklad, interpretácia a platnosť týchto certifikačných pravidiel SK-MSA sa riadia slovenskými a európskymi predpismi.

9.15 Dodržiavanie platnej legislatívy

Tieto certifikačné pravidlá spĺňajú nariadenie Európskeho parlamentu a Rady (EÚ) č. 165/2014 a vykonávacie nariadenie Komisie (EÚ) č. 2016/799. V prípade nezrovnalostí medzi týmto dokumentom a nariadením alebo vykonávacím nariadením, majú prednosť menované nariadenia.

9.16 Rôzne ustanovenia

Bez ustanovení.

9.17 Ostatné ustanovenia

Bez ustanovení.

10 Referencie

(NIST), N. I. (2005). Special Publication 800-38B: Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication.
(NIST), N. I. (July 2013). FIPS PUB 186-4: Digital Signature Standard (DSS).
(NIST), N. I. (May 25, 2001). FIPS PUB 140-2, Security requirements for cryptographic modules.
National Policy of Authority of the Member State SK-MSA for The Information System of Digital Tachograph System in Slovak Republic, Version 1.1. Ministry of Transport and Construction of the Slovak Republic.
Commission Implementing Regulation (EU) 2016/799, including Annex 1c and all Appendices, especially Appendix 11. Official Journal of the European Union L 139, including ref. 3.
Commission Implementing Regulation (EU) 2018/502, amending Implementing Regulation (EU) 2016/799. Official Journal of the European Union L 85.
SK-CA Certification Practice Statement Smart Tachograph, Version 1.0.
Implementing Rules for Commission Decision C(2006) 3602 of 16.8.2006 concerning the security of information systems used by the European Commission.
ISO/IEC 10116, Information technology – Security techniques – Modes of operation of an n-bit block cipher. Third edition.
ISO/IEC 15408-1, -2 and -3, Information technology — Security techniques — Evaluation criteria for IT security Parts 1, 2 and 3, third edition.
ISO/IEC 18033-2, Information technology — Security techniques — Encryption algorithms — Part 2: Asymmetric ciphers, first edition.
ISO/IEC 19790, Information technology — Security techniques — Security requirements for cryptographic modules, second edition.
ISO/IEC 27001, Information technology — Security techniques — Information security management systems — Requirements. Second edition.
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.
ISO/IEC 9797-1, Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher. Second edition.
JRC. Smart Tachograph - Equipment Interoperability Test Specification.
JRC. Smart Tachograph - ERCA Certification Practice Statement.
Marjo Geers, D. B. (June 2018). Smart Tachograph - European Root Certificate Policy and Symmetric Key Infrastructure Policy, Version 1.0. JRC.
Regulation (EU) No 165/2014. Official Journal of the European Union L60: European Parliament and the Council.
RFC 2119, Key words for use in RFCs to Indicate Requirement Levels.
RFC 3647, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.

11 Zoznam tabuliek