PŘÍLOHA G

Resortní politika certifikačních orgánů pro systém Digitální tachograf v České republice ("Národní certifikační politika")

1. Národní certifikační politika pro Karty DT první generace

Resortní politika certifikačních orgánů

pro systém

Digitální tachograf

v České republice

Správa klíčů, certifikátů a zařízení

(Registrace, generace klíčů, vydávání certifikátů, personalizace, distribuce, použití a ukončení životnosti)

pro

1. orgán členského státu (CZA)

2. orgán pro vydávání karet (CZCIA)

3. certifikační orgán členského státu (CZCA)

4. organizace pro personalizaci karet (CZCP)

Systém digitální tachograf v silniční dopravě -

certifikační politika pro Českou republiku

1 Úvod

Tento dokument představuje resortní politiku certifikačních orgánů České republiky pro systém digitální tachograf.

Tato resortní politika certifikačních orgánů České republiky je vydána na základě a v souladu s:

Nařízením Rady o systému digitálního tachografu (Council Regulation of the Digital Tachograph System) č. 3821/85, ve znění Nařízení (ES) č. 2135/98

Nařízením Komise (Commission Regulation) č. 1360/2002

Systémem digitálních tachografů - Evropskou Root politikou (Verze 2.0 – Zvláštní vydání I. 04.131).

1.1 Odpovědné organizace

Za tuto resortní politiku certifikačních orgánů odpovídá orgán členského státu (**CZA**), kterým je Ministerstvo dopravy České republiky.

Adresa:

Ministerstvo dopravy České republiky

nábřeží L. Svobody 12/1222

110 15 Praha 1

Pověřeným orgánem pro vydávání karet (**CZCIA**) je Ministerstvo dopravy České republiky.

Adresa:

Ministerstvo dopravy České republiky

nábřeží L. Svobody 12/1222

110 15 Praha 1

Jmenovaným certifikačním orgánem členského státu (**CZCA**) je Ministerstvo dopravy České republiky.

Adresa:

Ministerstvo dopravy České republiky

nábřeží L. Svobody 12/1222

110 15 Praha 1

Jmenovanou organizací pro personalizaci karet (**CZCP**) je Ministerstvo dopravy České republiky.

Adresa:

Ministerstvo dopravy České republiky

nábřeží L. Svobody 12/1222

110 15 Praha 1

CZCA nebo CZCP mohou uzavřít subdodavatelské smlouvy na části svých činností se subdodavateli a podřízenými institucemi. Využití subdodavatelských firem nesnižuje všeobecnou odpovědnost CZCA nebo CZCP.

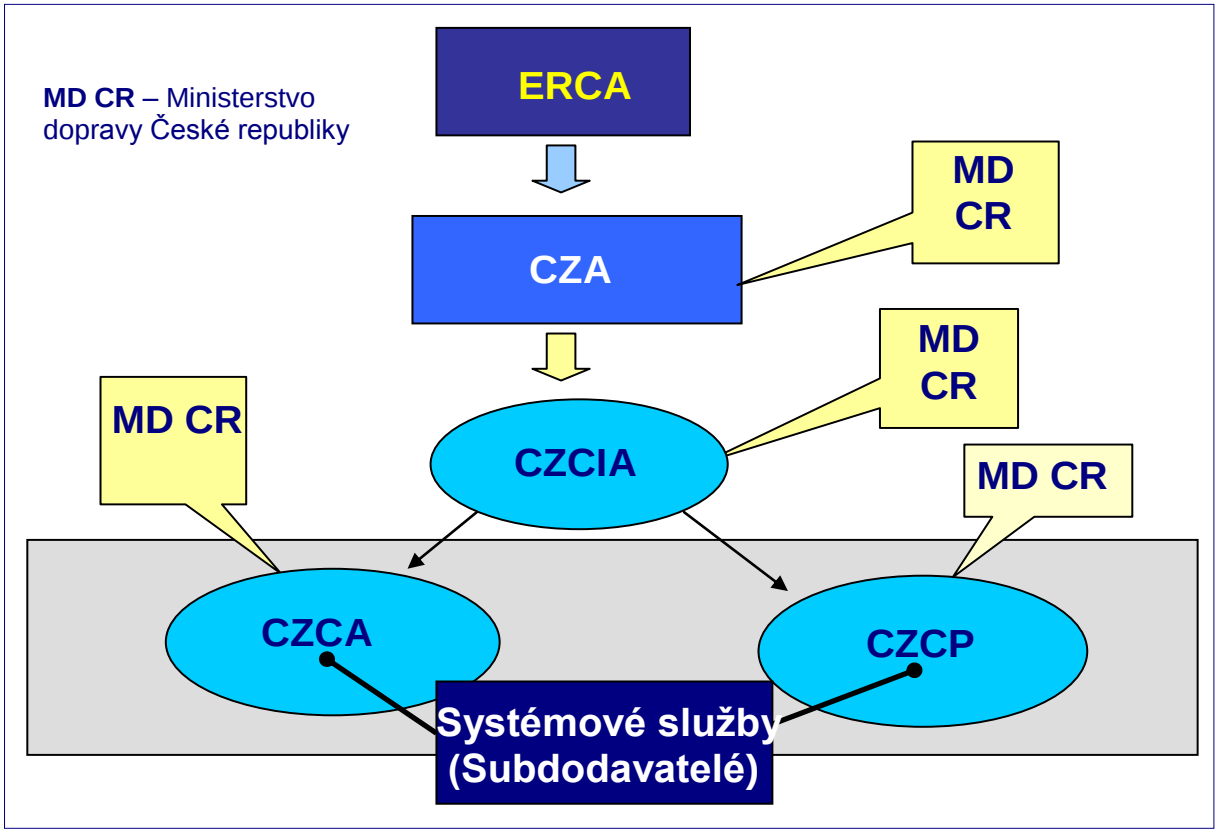


Diagram 1: Struktura odpovědných organizací

1.2 Schválení

Tato resortní politika certifikačních orgánů České republiky je schválena komisí, jmenovitě <name>, <date>.

1.3 Dostupnost a Telefonického kontaktní údaje

Resortní politika certifikačních orgánů České republiky je veřejně přístupná na informačních stránkách Ministerstva dopravy České republiky - http://www.mdcr.cz.

Dotazy související s resortní politikou certifikačních orgánů České republiky je možno adresovat na Ministerstvo dopravy České republiky.

Adresa:

nábřeží L. Svobody 12/1222

110 15 Praha 1

2 Rámec působnosti

[r2.1]

Tato resortní politika certifikačních orgánů České republiky platí pouze pro provádění úkolů v rámci Nařízení (ES) č. 3821/85, ve znění Nařízení (ES) č. 2135/98.

[r2.2]

CZA a CZCA zajišťuje, aby certifikáty vydané a klíče vygenerované CZCA byly používány pouze pro účely stanovené v Nařízení (ES) č. 3821/85, ve znění Nařízení (ES) č. 2135/98 v rámci systému jejich jednotlivých oprávnění a v rámci příslušných platných ustanovení.

[r2.3]

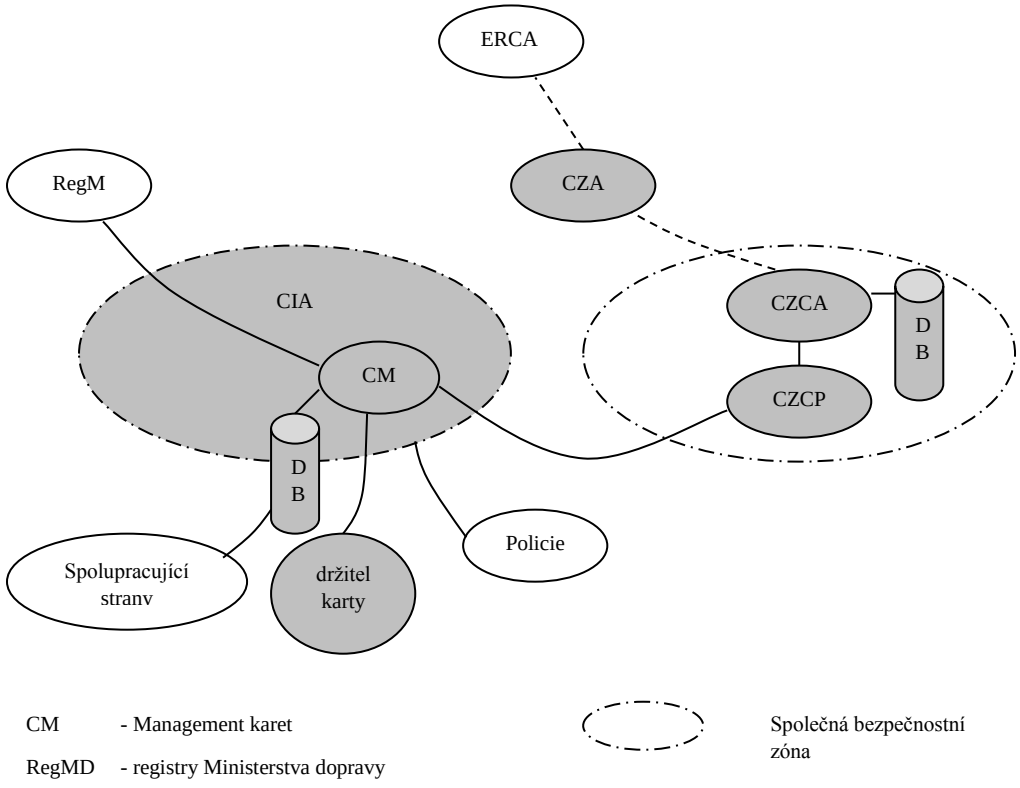
Rámec resortní politiky certifikačních orgánů České republiky je vyznačen šedou barvou v diagramu na obr. 1, který zachycuje strukturu tachografového systému v ČR a vazby v něm zúčastněných subjektů.

[r2.4]

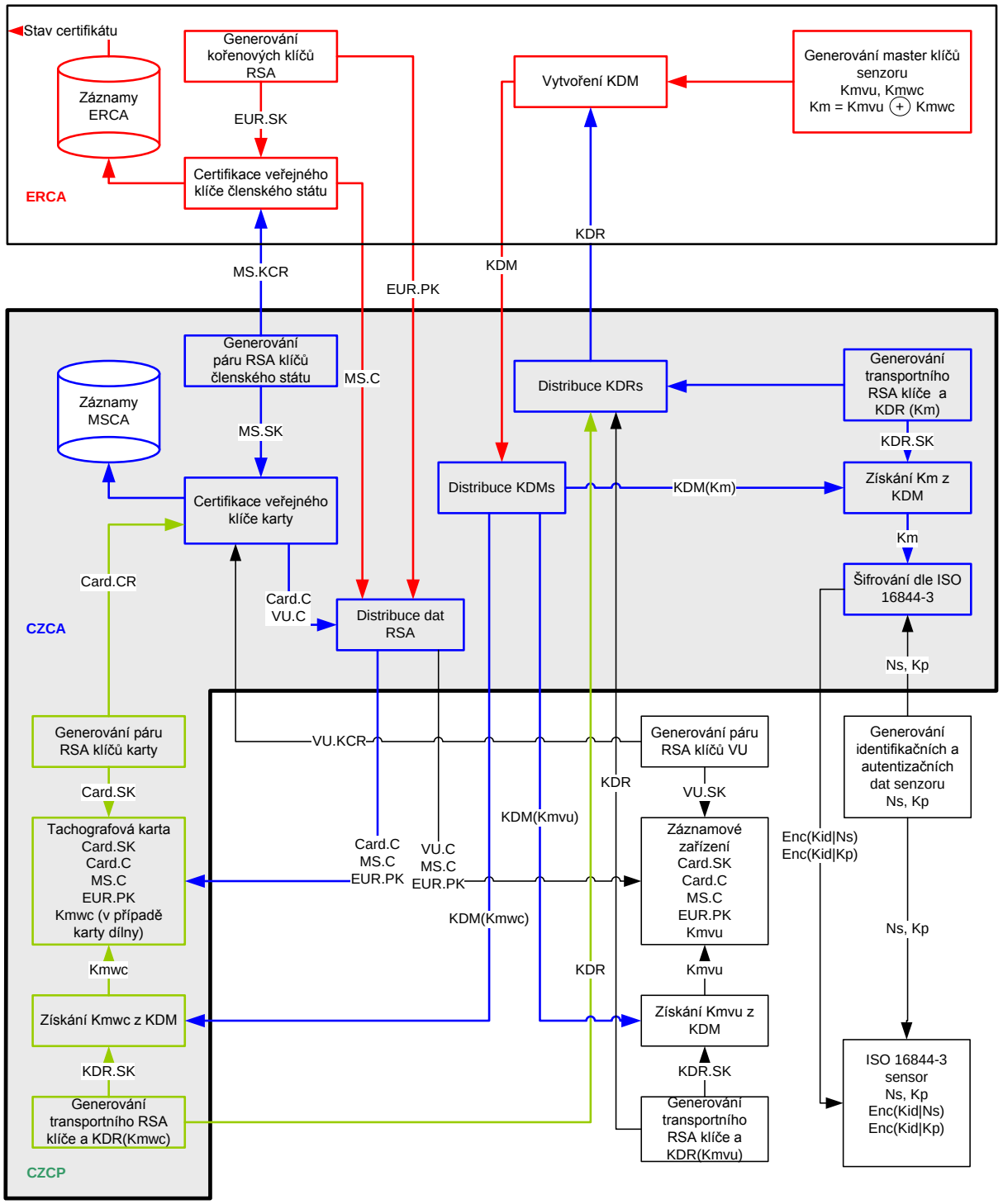
Procesní model systému vychází ze schématu uvedeného na obr. 2.

Poznámka:

V České republice neexistuje výrobce záznamových zařízení a senzorů. Proto se tato resortní politika certifikačních orgánů České republiky zaměřuje pouze na správu klíčů a certifikátů týkajících se tachografových karet.



Obr. 1 Zjednodušené schéma tachografového systému České republiky



Obr. 2 Popis správy klíčů dle přílohy 1(B)

3 Všeobecná ustanovení

3.1 Povinnosti

Tato část popisuje povinnosti úřadů, kterých se týká provádění Nařízení (ES) č. 3821/85, ve znění Nařízení (ES) č. 2135/98, při činnostech dle této resortní politiky certifikačních orgánů České republiky.

[r3.1]

CZA:

a) plní úkoly v koordinaci s ostatními členskými státy,

b) je odpovědná za návrh a provádění certifikační politiky pro Českou republiku a zajišťuje její schválení Komisí,

c) jmenuje CZCA,

d) jmenuje CZCP nebo zadá tyto úkoly externímu subdodavateli služeb,

e) může provádět a organizovat inspekci CZCA, CZCP, CZCIA, výrobců a dalších externích poskytovatelů služeb, pokud je to nutné,

f) zajišťuje, aby CZCA obdržela všechny informace nutné pro její práci,

g) schvaluje Specifikaci běžných postupů (Practice Statement) CZCA a dalších externích poskytovatelů služeb, pokud je to nutné,

h) zajišťuje, aby resortní politika certifikačních orgánů České republiky byla zpřístupněna všem zainteresovaným úřadům,

i) okamžitě informuje ERCA nebo jednu z jejích oprávněných agentur o všech událostech týkajících se bezpečnosti související s výrobou, personalizací a použitím jejich zařízení i klíčů a certifikátů v nich integrovaných.

[r3.2]

CZCA:

a) dodržuje požadavky stanovené Nařízením (ES) č. 3821/85, ve znění Nařízení (ES) č. 2135/98, souvisejícími právními ustanoveními, základní politikou (the Root Policy) a touto resortní politikou certifikačních orgánů České republiky,

b) navrhuje Specifikaci běžných postupů (Practice Statement), ve kterém je vysvětlena metoda implementace politiky CA, Root politiky a právních ustanovení,

c) po personální a materiální stránce zajišťuje plnění odpovídajících úkolů,

d) je odpovědná za správné provedení úkolů i v případě, že tyto úkoly nebo jejich části jsou zadány subdodavatelským poskytovatelům služeb. v tomto případě se musí ujistit, že tito subdodavatelé dodržují při své činnosti příslušné požadavky politiky CA a PS,

e) okamžitě informuje CZA nebo jednu ze svých oprávněných agentur o všech událostech týkajících se bezpečnosti, souvisejících s výrobou, personalizací a použitím jejich vybavení i klíčů a certifikátů v nich integrovaných.

[r3.3]

CZCIA:

a) zajistí, aby aplikační data byla dodána CZCA a CZCP s úplnými daty podle požadavků CZCA,

b) informuje odpovídajícím způsobem všechny uživatele o požadavcích resortní politiky,

c) prověřuje, zda jsou dány všechny nezbytné předpoklady pro vydání karty,

d) zajišťuje, aby PIN karty dílny byl předán pouze držiteli dané karty dílny, kterému je určen,

e) okamžitě informuje CZA a CZCA nebo jednu z jejích oprávněných agentur o všech událostech vztahujících se k bezpečnosti systému.

[r3.4]

CZCP:

a) plní v rámci své činnosti úkoly dle požadavků Nařízení (ES) č. 3821/85, ve znění Nařízení (ES) č. 2135/98, souvisejících právních předpisy, Root politiky a této resortní politiky certifikačních orgánů České republiky i PS CZCA,

b) podepisuje – pokud jedná s externím dodavatelem služeb – smlouvu s CZA, ve které se zavazuje plnit své povinnosti podle odstavce a),

c) doporučuje CZA vhodné postupy při provádění činností,

d) povoluje činnost agenturám s oprávněním od CZA,

e) okamžitě informuje CZCA nebo jednu z jejích oprávněných agentur o všech událostech souvisejících s bezpečností výroby, personalizace a použití jejich vybavení i klíčů a certifikátů v nich integrovaných.

[r3.5]

Držitel karty/Žadatel:

je povinen:

a) předkládat v žádosti pravdivé osobní údaje,

b) předkládat pravdivé informace týkající se jemu přidělených karet a typů karet v okamžiku odevzdání žádosti,

c) odpovídajícím způsobem zajistit, že vydaná karta bude používána pro stanovené účely, a zabránit jejímu zneužití,

d) zajistit, aby byl vlastníkem jediné platné karty řidiče,

e) nepoužívat poškozené karty nebo karty s prošlou platností,

f) informovat odpovědné úřady o ztrátě, krádeži, poškození nebo zneužití karty a příslušného privátního klíče.

[r3.6]

Výrobci vozových jednotek a výrobci senzorů pohybu musí obzvláště zajistit, že

a) splňují požadavky stanovené Nařízením (ES) č. 3821/85, ve znění Nařízení (ES) č. 2135/98, ostatními právními předpisy, resortní politikou certifikačních orgánů České republiky, a to dle nejlepšího vědomí a podle odpovídajícího současného technologického pokroku,

aa) že integrované klíče a certifikáty nebo ty klíče a certifikáty, které budou integrovány v jimi vyrobeném vybavení, mohou být použity pouze pro odpovídající účely v rámci Nařízení (ES) č. 3821/85, ve znění Nařízení (ES) č. 2135/98,

ab) učiní opatření, aby zajistili důvěrnost privátních i tajných klíčů během celého výrobního procesu a také během celého servisního období vybavení,

b) poskytnou CZA jména všech externích subdodavatelských poskytovatelů služeb s odpovědností za výrobu a personalizaci jejich vybavení, kdykoli to bude požadováno, a zavážou je povinností plnit odpovídající požadavky. Pokud výrobce přesune své úkoly na jiný subjekt, jeho práva a povinnosti zůstávají tímto nedotčeny,

c) okamžitě budou informovat CZA nebo jí pověřený orgán o všech událostech souvisejících s bezpečností výroby, personalizací a použitím jejich vybavení, jakož i klíčů a certifikátů v nich integrovaných,

d) umožní CZA nebo jí pověřenému orgánu hodnotit praktické provádění jejích povinností,

e) v rámci možností vyloučí, aby klíče a certifikáty, které mají k dispozici, nebyly zaváděny do zařízení bez typového schválení.

3.2 Zvláštní ustanovení

[r3.7]

CZCA stejně jako poskytovatelé služeb jím oprávnění plní úkoly v souladu s příslušnými právními předpisy, obzvláště s Nařízením (ES) č. 3821/85, ve znění Nařízení (ES) č. 2135/98 a národními předpisy přijatými pro jejich provádění. Právní předpisy zmíněné v této části nepředstavují úplný výčet.

[r3.8]

Ochrana dat

CZCA zajistí v rámci své působnosti, že budou dodržována ustanovení zákona č.101/2000 Sb., o ochraně osobních údajů, a další příslušná ustanovení o ochraně dat v souvislosti se zacházením s osobními daty.

Použité pojmy „důvěryhodný“, „privátní“ a „tajný“ je nutné vykládat pouze v souladu s účelem této politiky a nejsou totožné s pojmy, uvedenými ve zvláštních právních předpisech nebo v mezinárodních smlouvách (např. v zákoně č. 148/1998 Sb., o ochraně utajovaných skutečností a o změně některých zákonů, ve znění pozdějších předpisů).

4 Specifikace běžných postupů (dále jen „PS“) CZCA

r4.1]

CZCA navrhuje a udržuje PS, který ukazuje ve formě konkrétních opatření, jak je zajišťováno dodržování této resortní politiky certifikačních orgánů České republiky, Root politiky a právních ustanovení souvisejících s prací CZCA v činnosti CZCA. PS se skládá z přehledu, který ukazuje, jakým způsobem jsou požadavky politiky implementovány v PS.

[r4.2]

PS musí poskytnout jména všech externích poskytovatelů služeb CZCA, specifikovat jejich konkrétní úkoly, jakož i vysvětlit, jaké požadavky CZCA musí být poskytovateli služeb dodržovány.

[r4.3]

PS musí vysvětlit, jakým způsobem plní CZCA své povinnosti ohledně informačního managementu.

[r4.4]

Revizní proces musí být popsán v dokumentech PS, což má zajistit, aby PS vždy odpovídala současnému právnímu stavu a vývoji technologií a trvajícím podmínkám u CZCA a u jeho externích poskytovatelů služeb.

[r4.5]

CZCA předá svůj PS CZA ke schválení. Významné změny v PS rovněž vyžadují schválení CZA. CZCA odpovídá za to, že CZA je vždy poskytnuta poslední verze PS CZCA.

[r4.6]

Veřejná část PS může být kromě v PS popsána i v implementačním konceptu.

[r4.7]

PS obsahuje seznam událostí, které mohou vést ke znehodnocení klíčů. Se seznamem musí být zacházeno s náležitou opatrností.

5 Management karet a vybavení

[r5.1]

CZCA zajišťuje podle instrukcí CZA a zároveň v rámci své odpovědnosti, že certifikáty jím vydané a tajné klíče jím dodané jsou integrovány a implementovány v souladu s jejich zamýšleným účelem pouze v kartách záznamového zařízení a v záznamovém zařízení, které splňuje požadavky Nařízení (ES) č. 3821/85, ve znění Nařízení (ES) č. 2135/98.

[r5.2]

CZCA odmítne dodat klíče a certifikáty, pokud je riziko, že tyto klíče a certifikáty budou zneužity.

[r5.3]

CZCIA garantuje dodržování aplikačních a dodacích postupů pro karty v záznamovém zařízení, definovaných CZA podle instrukcí Nařízení (ES) č. 3821/85, ve znění Nařízení (ES) č. 2135/98.

[r5.4]

CZCIA zajišťuje v rámci své úřední pravomoci, že vydávání náhradních karet a obnovení karet se uskuteční pouze podle podmínek zmíněných v Nařízení (ES) č. 3821/85, ve znění Nařízení (ES) č. 2135/98 a že předepsané časové limity budou dodrženy.

[r5.5]

CZCP zajišťuje, že karty pro záznamová zařízení jsou personalizovány podle instrukcí Nařízení (ES) č. 3821/85, ve znění Nařízení (ES) č. 2135/98. Musí být respektována integrita vstupních dat.

[r5.6]

CZCA, CZCP a výrobci zajišťují v rámci svých úkolů, že privátní a tajné klíče jsou uskladněny a používány v zabezpečeném výrobním prostředí. Jestliže musí být tyto klíče přenášeny (ve shodě s požadavky Nařízení (ES) č. 3821/85, ve znění Nařízení (ES) č. 2135/98), musí být zajištěna jejich důvěrnost.

[r5.7]

CZCIA zpřístupní odpovídající data centrálnímu registru Ministerstva vnitra a spolupracujícím stranám takovým způsobem, aby bylo zjistitelné, komu byla která karta vydána.

[r5.8]

CZCIA zajistí, že personalizované karty budou bezpečně dodávány v časové lhůtě dané Nařízením (ES) č. 3821/85, ve znění Nařízení (ES) č. 2135/98 a že budou doručeny/předány jejich držitelům/uživatelům. Předběžnou podmínkou pro vydávání personalizovaných karet držiteli/uživateli je, že byl osobně identifikován při žádosti i předání karty. v případě, že karta není vystavena na fyzickou osobu, žadatel a příjemce karty musí být schopen prokázat svou identitu.

[r5.9]

CZCP zajišťuje, že karty dílny jsou poskytovány s PIN podle instrukcí Nařízení (ES) č. 3821/85, ve znění Nařízení (ES) č. 2135/98.

[r5.10]

PIN je generován systémem zabezpečeným proti neautorizovanému přístupu. Systém zabraňuje možnosti přiřadit PIN kartě dílny po jejím vydání. Po generování je PIN vytištěn v uzavřené PINové obálce na on-line tiskárně a doručen osobě do vlastních rukou, pro níž byla odpovídající karta dílny vyrobena. Systém použitý pro generování PINu a tisk PINové obálky musí splňovat požadavky stanovené v normě FIPS 140-2 (nebo 140-1) úroveň 3 (nebo vyšší) nebo ITSEC E3, nebo záruky dle dokumentu Common Criteria úroveň EAL4 nebo ekvivalentní IT bezpečnostní kritéria nebo doložitelné záruky požadované úrovně bezpečnosti.

[r5.11]

Každá PINová obálka musí být dodána odděleně od personalizované karty a může být doručena poštou.

[r5.12]

Oprava PIN nesmí být možná.

6 Management klíčů v rámci CZCA

Tato sekce obsahuje požadavky pro zacházení s následujícím klíčovým materiálem CZCA (zkratky eventuálně používané v Nařízení (ES) č. 3821/85, ve znění Nařízení (ES) č. 2135/98 jsou uvedeny v závorkách):

- veřejný klíč (public key) of the Root CA (EUR.PK),
- pár klíčů CZCA (MS.SK, MS.PK),
- symetrické klíče pro senzory vzdálenosti a pohybu (Km, Kmwc, Kmvu),
- pokud je to požadováno, přepravní klíče pro komunikaci s Root CA a
- pokud je to vyžadováno, exkluzivní přepravní klíče CZCA.

CZCA zajišťuje v rámci svého pole působnosti důvěrnost a integritu všech neveřejných generovaných klíčů, používaných a/nebo uskladněných u něj a efektivně zabraňuje jakémukoli zneužití těchto klíčů. Pro tento účel musí využít vhodný technický systém, který splňuje jeden z následujících požadavků:

- FIPS 140-2 (nebo 140-1) úroveň 3 nebo vyšší [FIPS],
- CEN Workshop Agreement 14176-2 [CEN],
- certifikaci podle EAL 4 nebo vyšší v souladu s ISO 15408 [CC] k úrovni E3 nebo vyšší [ITSEC] založenou na ochraně profilu a bezpečnostních instrukcích ("SecurityTargets"), což zahrnuje požadavky této resortní politiky certifikačních orgánů České republiky – založené na všeobecné analýze rizik – jakož i strukturální a netechnická bezpečnostní opatření,
- bezpečnostní kritéria, která poskytují rovnocennou úroveň zabezpečení.

Stejným způsobem, musí být prokázáno, že tyto systémy jsou provozovány v odpovídajícím způsobem zabezpečeném operačním prostředí u CZCA.

CZCA podepíše certifikáty zařízení výhradně v rámci stejného zařízení, používaného k uložení privátních klíčů členského státu.

6.1 Veřejný klíč (Public key) bezpečnostní certifikační politiky (ERCA.PK)

[r6.1]

CZCA zajišťuje, že integrita a dostupnost klíče ERCA.PK je garantována v jeho běžné činnosti.

[r6.2]

CZCP a výrobci zajistí, že ERCA.PK je integrován ve všech kartách a záznamových zařízeních (VU), v rámci jejich úřední pravomoci.

6.2 Pár klíčů (Key pair) vlastněný CZCA (MS.SK, MS.PK)

[r6.3]

CZCA bude vlastnit různé páry klíčů pro výrobu certifikátů pro záznamová zařízení (neomezená platnost) a jiné pro tachografové karty (omezená platnost).

[r6.4]

CZCA zajistí, aby MS.SK byl používán výhradně pro podepisování certifikátů pro karty v záznamových zařízeních, pro podepisování certifikátů záznamových zařízení (VU) a pro vydání požadavku na certifikaci klíče ERCA. Toto obzvláště zahrnuje utajení privátního klíče MS.SK.

[r6.5]

Výroba páru klíčů CZCA se může uskutečnit pouze s aktivní účastí nejméně dvou různých osob v CZCA. Jeden z těchto jedinců musí převzít funkci správce CA, druhý má jinou funkci, jak je popsáno v politice CA.

[r6.6]

CZCA by si měl nechat – v rámci instrukcí Root politiky – odpovídající počet náhradních párů klíčů s odpovídajícími certifikáty, aby provedl rychlou výměnu klíče v případě nedostupnosti pravého klíče, a to i bez aktivní účasti root CA. Pokud je k dispozici několik párů klíčů, pak musí CZCA zajistit, že jen ten správný klíč se používá celou dobu.

[r6.7]

Každý privátní klíč MS.SK by měl být používán maximálně 2 roky. Po uplynutí doby používání musí být zničen CZCA takovým způsobem, že nebude možné žádné další budoucí použití nebo zneužití.

[r6.8]

Doba platnosti veřejného klíče členského státu MS.PK je neomezená.

[r6.9]

CZCA musí efektivně chránit všechny privátní klíče, jakož i náhradní klíče před zneužitím, úpravou a neoprávněným přístupem za použití technických a organizačních prostředků.

[r6.10]

CZCA efektivně omezuje přístup k MS.SK jedinou osobou, implementací vhodných technicko-organizačních opatření.

[r6.11]

Není dovolen depozit (key escrow) privátního klíče, včetně privátních klíčů zařízení.

[r6.12]

PS CZCA by mělo obsahovat explicitní postupy v případě, že je MS.SK znehodnocen (zkompromitován) nebo potenciálně znehodnocen. Tyto postupy by měly také obsahovat instrukce pro externí poskytovatele služeb a informace držitelům karty a výrobcům zařízení. v případě, že klíče EUR.SK, MS.SK, Km, Kmwc, Kmvu jsou znehodnoceny nebo potenciálně znehodnoceny, CZA a Root CA musí být okamžitě informovány. v ostatních případech znehodnocení klíčů nebo potenciálního znehodnocení klíčů budou přijata vhodná opatření a informace budou podány zainteresovaným institucím.

[r6.13]

CZCA zajišťuje ve spolupráci s Root CA, že vlastní platný pár klíčů (MS.SK, MS.PK) s odpovídajícím certifikátem ve kterémkoli časovém okamžiku.

[r6.14]

CZCA předá MSA veřejné klíče pro certifikaci ERCA s použitím protokolu požadavku na certifikaci klíče (KCR), popsaného v příloze a Evropské Root politiky digitálních tachografů - Digital Tachograph System European Root Policy.

[r6.15]

CZCA rozeznává ERCA veřejný klíč v distribučním formátu popsaném v příloze B Evropské Root politiky digitálních tachografů - Digital Tachograph System European Root Policy.

[r6.16]

CZCA používá pro přepravu klíčů a certifikátů fyzická média popsaná v příloze C Evropské Root politiky digitálních tachografů - Digital Tachograph System European Root Policy.

6.3 Symetrické klíče pro karty dílny a senzory vzdáleností a pohybu (Km, Kmwc, Kmvu)

[r6.17]

Pokud vyvstane potřeba, CZCA si vyžádá od Root CA klíče k senzorům vzdálenosti a pohybu Km, Kmwc a Kmvu. Ustanovení Root CA pro požadavek a dodání těchto klíčů mezi Root CA a CZCA se musejí dodržovat.

[r6.18]

CZCA zajistí za využití vhodných prostředků, že klíče Kmwc a Kmvu budou předány pouze určenému příjemci a zabezpečí jejich doručení adresátovi vhodnými prostředky. CZA kontroluje bezpečnostní opatření CZCA. CZCA zajistí, aby klíč Km nebyl předán.

[r6.19]

V případě, že jeden z klíčů Kmwc nebo Kmvu je znehodnocen nebo potenciálně znehodnocen, CZCA musí okamžitě informovat CZA a Root CA.

[r6.20]

CZCA požaduje master klíče pohybových senzorů od ERCA, s využitím protokolu o požadavku na distribuci klíče (KDR) popsaném v příloze D ERCA politiky.

6.4 Přepravní klíče Root CA

[r6.21]

V případě, že Root CA chce dát CZCA kryptografické klíče pro zabezpečení vzájemné komunikace, jejich integrita musí být efektivně chráněna CZCA a musí být zabráněno jakémukoli zneužití klíčů.

6.5 Exkluzivní přepravní klíče CZCA

[r6.22]

V případě, že CZCA chce dát pro zajištění vzájemné komunikace kryptografické klíče svým komunikačním partnerům (personalizačním agenturám, výrobcům zařízení …), ochrana dat a jejich důvěrnost a integrita musí být efektivně chráněna CZCA a musí být efektivně zabráněno jejich zneužití. CZCA požaduje po svých komunikačních partnerech, aby splňovali odpovídající bezpečnostní opatření pro ochranu klíčů v rámci jejich pravomocí.

7 Key (klíčový) management klíčů pro asymetrické karty a vybavení

Tato část obsahuje požadavky pro generování a zacházení s asymetrickými kryptografickými klíči pro karty v záznamových zařízeních a pro záznamová zařízení, jakož i s odpovídajícími certifikáty. Požadavky pro symetrické klíče Km, Kmwc a Kmvu mohou být nalezeny v části 6.3.

7.1 Všeobecné požadavky, záznam

[r7.1]

CZA, CZCA, CZCP a výrobci zajišťují v rámci své působnosti, že zprovoznění, zašifrování a personalizace karet a záznamového zařízení se uskuteční ve výrobním prostředí se zvláštním zabezpečením. Tento přístup k těmto oblastem musí být efektivně utajený a kontrolovaný. Správa těchto systémů musí vyžadovat přítomnost alespoň 2 zodpovědných osob. Každý přístup a vstup do systémů, jakož i do všech činností jimi prováděných musí být zaznamenán takovým způsobem, aby nebyla možná neoprávněná modifikace těchto záznamů a aby byla zajištěna dostupnost, důvěrnost a integrita záznamu, a to i tehdy, pokud byl kompromitován klíč.

[r7.2]

CZA, CZCA, CZCP a výrobci zajišťují v rámci jejich pravomoci, že informace jako jsou privátní klíče atd., nezbytné pro bezpečnostní účely, jsou chráněny v celém průběhu zavádění do provozu, šifrování a personalizace karet a záznamového zařízení podle požadavků Nařízení (ES) č. 3821/85, ve znění Nařízení (ES) č. 2135/98 a resortní politiky certifikačních orgánů České republiky.

[r7.3]

CZA požaduje po všech externích poskytovatelích služeb, aby prováděli přijaté úkoly naprosto odděleně od jejich ostatních aktivit. Toto je obzvláště platné, pokud poskytovatel služeb převezme úkoly pro CA jiných členských států. CZA požaduje po všech externích poskytovatelích služeb, aby zaznamenávali své aktivity podle [r7.1] takovým způsobem, aby záznam nemohl být pozměněn a aby povolili CZA získat přehled záznamů, pokud to bude vyžadovat.

[r7.4]

Záznamy vytvořené v průběhu personalizace karet a záznamového zařízení musejí umožnit přiřazení jednotlivých úkonů k příslušnému číslu karty/zařízení, jakož i odpovídajícímu certifikátu.

7.2 Generování klíčů

[r7.5]

CZA, CZCA, CZCP a výrobci zajišťují v rámci své působnosti, že generace klíčů se uskuteční ve výrobním prostředí se zvláštním zabezpečením, což obzvláště garantuje utajení

odpovídajících privátních klíčů. Pro vybavení, které bude pro tyto účely použito, jsou platné stejné požadavky jako pro vybavení využívané CZCA pro generování párů klíčů.

[r7.6]

CZA, CZCA, CZCP a výrobci zajistí v rámci své působnosti, že privátní klíče jsou trvale vymazány z paměti systémů pro generaci klíčů a personalizaci okamžitě po jejich integraci do příslušných karet nebo zařízení, pokud se generace klíče neprovede přímo v čipu.

[r7.7]

CZCA zajistí v rámci své odpovědnosti, že duplikace klíče bude pokud možno vyloučena.

[r7.8]

Generování klíčů je povoleno pro vytváření zásob (stock-building) (“Batch process”), pokud je zajištěno technicko-organizačními prostředky, že zneužití uložených párů klíčů je zabráněno. Zásoba klíčů nepřesáhne výrobní kvótu na jeden měsíc.

7.3 Žádost o klíč

[r7.9]

CZA, CZCA, CZCP a výrobci zajistí v rámci své působnosti, že odpovídající klíče mohou být výhradně používány pro jejich stanovené účely podle Nařízení (ES) č. 3821/85, ve znění Nařízení (ES) č. 2135/98. Toto obzvláště zahrnuje, že neexistují žádné kopie těchto klíčů mimo zabezpečenou oblast karet pro záznamová zařízení a záznamového zařízení po uskutečnění procesu personalizace.

[r7.10]

CZCP, CIA zajistí v rámci své působnosti, že budou dodány jen takové karty, jejichž optická a logická personalizace se vztahuje správně na držitele karty.

[r7.11]

Privátní klíče členského státu mohou být zálohovány pro potřeby obnovení klíče (key recovery procedure). Přístup k těmto procedurám vyžaduje alespoň dvojitou kontrolu.

[r7.12]

CZA, CZCA, CZCP a výrobci zajistí v rámci své působnosti, že privátní klíče nemohou být znovu použity po vypršení platnosti funkčního období karet pro záznamová zařízení nebo záznamového zařízení.

8 Management certifikátů (Certificate management)

Tato sekce obsahuje požadavky ohledně výroby a aplikace certifikátů vytvořených CZCA během životního cyklu příslušných karet pro záznamová zařízení nebo záznamového zařízení.

8.1 Registrace

[r8.1]

CZCIA zajistí v rámci své pravomoci, že bude provedena správná registrace u zodpovědných orgánů, než bude certifikát vydán.

[r8.2]

Zde musí CZCP obzvláště zajistit, že registrační data umožňují jasné přiřazení "Certificate Holder Reference" (reference držitele certifikátu) podle požadavku CSM_017 z dodatku 11 přílohy (B) Nařízení (ES) č. 3821/85, ve znění Nařízení (ES) č. 2135/98.

[r8.3]

Pokud generování klíče probíhá mimo bezpečnostní zónu CZCA, CZCA vydá požadovaný certifikát, jen pokud žadatel prokáže předem dohodnutým způsobem, že je vlastníkem odpovídajícího privátního klíče. Během tohoto období by privátní klíč neměl opustit zabezpečené prostředí generátoru klíčů.

8.2 Vydávání certifikátu

[r8.4]

CZCA vydá certifikát, když je předána správná žádost o certifikát odpovědnému orgánu a když byly v době žádosti dodrženy všechny požadavky Nařízení (ES) č. 3821/85, ve znění Nařízení (ES) č. 2135/98 a všechny další související právní ustanovení a dohody. v případě automatizovaného procesu musí být dokonale zabráněno vydání certifikátu manuálním zásahem do systému.

[r8.5]

CZCA zajistí v rámci své působnosti, že certifikáty jím vydané budou doručeny pouze žadateli.

[r8.6]

CZCA vydá certifikáty jenom pro zařízení a karty, pro které bylo vydáno schválení typu komponentů a toto schválení je stále platné.

[r8.7]

Požadavky na certifikaci klíčů závislých na přípravě privátních klíčů nejsou povoleny.

[r8.8]

CZCIA udržuje a zpřístupňuje informace o statusu certifikátu.

8.3 Platnost certifikátu

[r8.9]

Období platnosti certifikátů vydaných CZCA by nemělo překročit maximální dobu užívání příslušných karet a/nebo zařízení. Certifikáty pro:

- karty řidiče ne více než 5 let
- karty dílny (servisu) ne více než 1 rok,
- kontrolní karty ne více než 5 let,
- karty podniku (vozidla) ne více než 5 let,

jak je vypočteno z období, po které jsou odpovídající karty platné.

Certifikáty pro dopravní prostředky mají platnost na dobu neurčitou.

8.4 Obsah a formát certifikátů

[r8.10]

Obsah a formáty certifikátů vydaných CZCA splňují požadavky Nařízení (ES) č. 3821/85, ve znění Nařízení (ES) č. 2135/98, obzvláště specifikace zmíněné v dodatku 11 přílohy i (B).

CZCA podepisuje všechny certifikáty jím vydané svým privátním podpisovým klíčem. CZA zajistí, že klíčový identifikátor (Key Identifier) (KID) a modul (n) klíčů předaných ERCA pro certifikaci a pro distribuci klíčů pro pohybové senzory jsou jedinečné v rámci působnosti CZCA.

8.5 Informační povinnosti CZCA

[r8.11]

CZCA přenese veškerá data o certifikátech CZCP a výrobcům tak, aby certifikáty, zařízení i karty i držitelé karet byli vzájemně propojeni.

[r8.12]

Pokud dotazující se orgány prokáží oprávněný zájem o zvláštní neveřejné informace o fungování CZCA nebo jeho externích smluvních partnerů a žádná pravidla nebo bezpečnostní předpoklady nestojí proti dodání těchto informací, CZCA informace zpřístupní co nejrychleji v souladu s CZA.

[r8.13]

Operační koncept CZCA musí být brán za důvěrný. Informace v něm obsažené mohou být k nahlédnutí po dohodě s CZA v CZCA, pokud je prokázaný oprávněný zájem a pokud je důvěrnost informací také odpovídajícím způsobem chráněna u příjemce.

9 Zabezpečení IT

9.1 Systém managementu zabezpečení IT (ISMS)

[r9.1]

CZCA a, pokud je to nutné, všichni oprávnění poskytovatelé služeb zřídí vhodný systém zabezpečení IT (IT Security Management System) (ISMS), který neustále garantuje bezpečnost IT pro veškerou práci vztahující se k úkolům CZCA. Je vhodné, aby tento systém zabezpečení vycházel z požadavků ISO 17799.

[r9.2]

CZCA zajistí, že stanovení ochranných požadavků je prováděno pro všechny IT systémy a informace vztahující se k CZCA.

[r9.3]

Musí být vytvořen bezpečnostní koncept pro práci CZCA. Tento koncept musí být přizpůsoben operačnímu konceptu (pojetí).

[r9.4]

Návrh a zavedení operačního konceptu jsou součástí managementu zabezpečení IT.

9.2 Speciální požadavky bezpečnostního konceptu

Následující část shrnuje skutečnosti, kterým se musí věnovat zvláštní pozornost v rámci bezpečnostního konceptu. Není tím však míněn úplný výčet skutečností.

[r9.5]

CZCA zajistí, že pouze důvěryhodné a dostatečně kvalifikované osoby jsou pověřeny stanovenými úkoly. Toto se vztahuje rovněž na personál externích smluvních partnerů.

[r9.6]

IT systémy implementované pro práci CZCA a, pokud je to nutné, i pro práci externích poskytovatelů služeb musí být obsluhovány takovým způsobem, aby bylo v nejvyšší možné míře zabráněno možným škodám způsobeným viry a jinými zákeřnými kódy (šiframi) a aby byly minimalizovány možné následky škod a narušení. Systémy musí mít efektivní vstupní kontrolu a musí obzvláště efektivně využívat funkční koncepty popsané v této politice a v doprovodných bezpečnostních a operačních konceptech.

[r9.7]

Spuštění systémů, které obsahují privátní podpisový klíč CZCA nebo tajné symetrické klíče Kmvu, Kmwc nebo Km se může uskutečnit pouze ve spolupráci dvou osob, které musí být v systému předem ověřeny.

[r9.8]

CZCA by měl pro své úkoly zavádět důvěryhodné systémy a software, které jsou efektivně chráněny používáním vhodných prostředků proti neoprávněným úpravám. Pokud je použit speciálně vyvinutý software nebo hardware, musí být vyvíjen zvlášť pečlivě s ohledem na implementaci bezpečnostních funkcí.

[r9.9]

Sítě zavedené v rámci CZCA a data zde uložená a zpracovaná musí být chráněna proti vnější intervenci za použití ochranného mechanismu (jako např. Firewalls).

[r9.10]

Všechny akce a procesy související s bezpečností IT systému používaného pro práci CZCA musí být zaznamenány takovým způsobem, aby mohl být s dostatečnou jistotou nalezen odpovídající čas a osoba. To zahrnuje alespoň:

- vytvoření uživatelské oblasti (účtů),
- všechny požadavky na transakce (účet žadatele, typ, status (úspěšný/neúspěšný), důvody selhání, …),
- Instalace a aktualizace softwaru,
- úpravy hardwaru,
- ukončení činnosti systému a znovuzahájení (restart),
- přístup do evidence a archívů.

[r9.11]

Záznamy by měly být chráněny proti úpravám a neoprávněnému přístupu. Měly by být pravidelně a příležitostně hodnoceny a analyzovány.

[r9.12]

Zaznamenaná data by měla být zachována alespoň 7 let takovým způsobem, aby bylo v jakémkoli okamžiku v rámci tohoto časového období možné vyhodnocení dat.

[r9.13]

CZCA navrhuje nouzový plán, ve kterém je stanoven průběh akce v případě vážné nouze, jako je zneužití klíče nebo ztráta příslušných dat a/nebo selhání IT systému.

[r9.14]

CZCA garantuje úspěšnou strukturální a fyzickou ochranu svých dat a IT systémů. Toto zahrnuje obzvláště dostatečnou přístupovou ochranu pro oblasti citlivé na bezpečnost. Oblasti,

kde jsou generovány, uloženy a zpracovávány privátní a tajné klíče, musejí být chráněny zvláštními prostředky.

9.3 Oddělení funkcí

[r9.15]

Koncepty nastavení funkcí by měly zabránit jednotlivým osobám obejít předběžná bezpečnostní opatření CZCA. Pro tyto účely jsou přidělena jednotlivým funkcím omezená práva a povinnosti jednotlivě. Přesná organizace závisí na konkrétním běhu událostí v CZCA a zůstává rezervována pro operační koncept CZCA. Minimálně musí být zřízeny následující funkce:

- CZCA – řídící funkce (NR)
- CA administrátor (CAA)
- Správce systému (SysA)
- Vedoucí bezpečnosti IT (IT Security Officer) (ISSO)

Každá funkce by měla být obsazena alespoň jednou osobou a musí být určen alespoň jeden zástupce (představitel). Žádná osoba nesmí přijmout víc než jednu z těchto funkcí zároveň. Nositelé funkce musejí být spolehlivě prověřeni IT systémy CZCA.

[r9.16]

NR funkce spočívá v následujícím:

- Je zodpovědný za bezpečné a hladké fungování CZCA jako organizace.
- Je představitelem organizace a oprávněn dávat instrukce v rámci organizace CZCA.
- Není přímo zapojen v implementaci obchodních procesů, ale je zodpovědný za dodržování a hodnocení bezpečnostních opatření společně s celkovým řízením CZCA.
- Přijímá zodpovědnost za řízení změn - Change Management.

[r9.17]

Funkce CAA zahrnuje:

- bezpečné provádění procesů klíčového managementu - Key Management Processes,
- generování, certifikaci, správu a vymazávání asymetrických klíčů CZCA, jakož i symetrických klíčů, které jsou používány pro zakódování dat záznamových zařízení a/nebo workshop karet.

[r9.18]

Funkce SysA spočívá v následujícím:

- Je zodpovědný za hladké fungování složek technické sítě DCA. To zahrnuje např. prvky Firewall, VPN složky a kabely. Přizpůsobení Firewall a VPN gateway (bráně) jsou povolené pouze na principu ‘foureyes-principle’.

[r9.19]

Funkce ISSO zahrnuje:

- detailní přezkušování bezpečnosti všech obchodních procesů a ohodnocení bezpečnostních opatření,
- přezkoušení všech ostatních funkcí, implementace bezpečnostní politiky, managementu změn a/nebo implementace obchodních procesů a instrukcí v rámci organizace CZCA,
- zodpovědnost za provádění auditů, které musejí být uskutečňovány pravidelně v rámci organizace DCA,
- zodpovědnost za návrh a udržování bezpečnostního konceptu,
- Účast na generaci klíče členského státu.

[r9.20]
Pokud CZCA přesune části svých úkolů na externí poskytovatele služeb, měl by navrhnout funkční koncept odpovídající jejich povinnostem.

10 Konec činnosti CZCA

10.1 Přesun odpovědnosti CZCA

CZA činí rozhodnutí týkající se přesunu zodpovědnosti CZCA. CZA musí určit nový CZCA pro stejnou činnost. Aby byl proveden tento přesun, musejí být splněny následující body:

[r10.1]
CZA zajistí, že přesun úkolů a povinností na nový CZCA se uskuteční vhodným způsobem plně v souladu s právními předpisy a resortní politikou.

[r10.2]
Starý CZCA musí přesunout všechny dostupné CZCA klíče na nový CZCA. Metoda je určena CZA.

[r10.3]
Všechny typy kopií klíčů, které mohou být spojovány se starým CZCA nebo které nemohou být předány, musejí být zničeny.

11 Auditní činnosti (Operation audits)

11.1 CZCA

[r11.1]
CZA zajistí provedení pravidelných a příležitostných nezávislých auditů činnosti CZCA. Vhodný audit by se měl uskutečnit alespoň jednou ročně. CZA může pověřit tímto úkolem externí poskytovatele služeb. v době auditu činnosti CZCA musejí být především ověřeny soulad běžné činnosti s odpovídajícími právními ustanoveními, CZCA politika, jakož i běžný operační koncept a běžný koncept zabezpečení IT. Externí poskytovatelé služeb pověření CZCA musejí být, pokud je to nutné, zahrnuti v auditu.

[r11.2]

CZA zajistí, že bezpečnost činnosti CZCA není dotčena probíhajícím auditem. Obzvláště pak zajistí, že výsledky těchto auditů nejsou k dispozici žádné neoprávněné osobě. Vyžaduje se, aby externí poskytovatelé služeb zachovávali tajemství, pokud je to nutné.

[r11.3]

CZA zahrne výsledky hodnocení do zprávy, která určí opravné akce, včetně časového rozvrhu jejich implementace, požadovaného ke splnění povinností CZA. Zpráva bude poskytnuta společnosti ERCA.

[r11.4]

Pokud hodnocení ukáží nesrovnalosti nebo neshody ve fungování CZCA, pak CZA sdělí CZCA, aby tyto napravila. CZCA okamžitě podá zprávu o zahájení a závěru těchto opatření. CZA může zajistit nezávislé zhodnocení úspěchu těchto opatření.

11.2 CZCP a výrobci

[r11.5]

Dodržování bezpečnostních směrnic a obzvláště resortní politiky certifikačních orgánů České republiky musí být prokázáno:

- Certifikátem vydaným CZA nebo autoritou pověřenou CZA nejméně jednou ročně.

Výrobce a/nebo CZCP nese náklady.

[r11.6]

Příležitostné audity v souladu s Nařízení (ES) č. 3821/85, ve znění Nařízení (ES) č. 2135/98 mohou být kdykoli vyžadovány CZA a CZCA. Pokud se najdou nezvyklosti, pak nese náklady výrobce a /nebo CZCP. Jinak nese náklady kontrolní orgán, z jehož podnětu byly audity uskutečněny.

12 Úpravy a přizpůsobení politiky CZCA

[r12.1]

Žádosti o úpravy politiky CZCA musejí být adresovány na CZA, který je zodpovědný za přijetí vhodných opatření v nejbližším časovém období.

[r12.2]

Jediné změny, které mohou být provedeny v resortní politice certifikačních orgánů České republiky bez oznámení, jsou:

a) vydavatelské a typografické opravy

b) změny v Telefonických kontaktních údajích

13 Přizpůsobení se ERCA politice

Požadavky na českou politiku CA jsou formulovány v politice ERCA § 5.3. Níže uvedená tabulka poskytuje vztah mezi požadavky, jak jsou formulovány v ERCA politice a požadavky resortní politiky certifikačních orgánů České republiky.

položka	odkaz v politice ERCA	Požadavky	odkaz v CZCA politice
1	§ 5.3.1	Politika MSA určí jednotky pověřené činností.	§ 1.1 Zodpovědné organizace
2	§ 5.3.2	MSCA páry klíčů pro certifikaci klíčů zařízení a pro distribuci klíčů pro pohybové senzory budou generovány a uloženy v rámci zařízení, které buď: _ má oprávnění plnit požadavky stanovené v FIPS 140-2 (nebo FIPS 140-1) úroveň 3 nebo vyšší [10]; _ má oprávnění být shodný s požadavky stanovenými v CEN Workshop Agreement 14167-2 [11]; _ je důvěryhodným systémem, který je zajištěn na EAL4 nebo vyšší v souladu s ISO 15408 [12]; na úroveň E3 nebo vyšší v ITSEC [13]; nebo odpovídající bezpečnostní kritéria. Tato hodnocení budou k ochrannému profilu nebo bezpečnostnímu účelu, _ je předveden k poskytování (is demonstrated to provide an)	§ 6 Klíčový management v rámci CZCA (odstavec 2)
3	§ 5.3.3	Generace páru klíčů členského státu se uskuteční ve fyzicky zabezpečeném prostředí personálem na věrných postech, za alespoň dvojité kontroly.	§ 6 Klíčový management v rámci CZCA (odstavec 3) § 6.2 Pár klíčů CZCA (MS.SK, MS.PK) [r6.5] § 6.2 Pár klíčů CZCA (MS.SK, MS.PK) [r6.10] § 7.3 Žádost o klíče [r7.9] § 9.2 Speciální požadavky bezpečnostního konceptu [r9.7]

položka	odkaz v politice ERCA	Požadavky	odkaz v CZCA politice
4	§ 5.3.4	Páry klíčů členského státu budou používány po dobu maximálně dvou let, přičemž toto období začíná běžet certifikací ERCA.	§ 6.2 Pár klíčů CZCA (MS.SK, MS.PK) [r6.7]
5	§ 5.3.5	Generace párů klíčů pro nový členský stát bude brát v úvahu měsíční lhůtu požadovanou pro certifikaci ERCA.	§ 6.2 Pár klíčů CZCA (MS.SK, MS.PK) [r6.13]
6	§ 5.3.6	MSA odevzdá MSCA veřejné klíče pro certifikaci ERCA pomocí protokolu požadavku na certifikaci klíče (KCR), popsaného v příloze A.	§ 6.2 Pár klíčů CZCA (MS.SK, MS.PK) [r6.14]
7	§ 5.3.7	MSA bude od ERCA vyžadovat master klíče pro pohybové senzory pomocí protokolu o požadavku na distribuci klíče (KDR) popsaného v příloze D.	§ 6.3 Symetrické klíče pro workshop karty a senzory vzdálenosti a pohybu (Km, Kmwc, Kmvu) [r6.20]
8	§ 5.3.8	MSA uzná veřejný klíč ERCA v distribučním formátu popsaném v příloze B.	§ 6.2 Pár klíčů CZCA (MS.SK, MS.PK) [r6.15]
9	§ 5.3.9	MSA použije pro přepravu klíče a certifikátu fyzická média popsaná v příloze C	§ 6.2 Pár klíčů CZCA (MS.SK, MS.PK) [r6.16]
10	§ 5.3.10	MSA zajistí, že identifikátor klíče (KID) a modul (*n*) klíčů předložených ERCA pro certifikaci jsou unikátní v rámci působnosti MSCA.	§ 8.4 Obsah a formát certifikátů [r8.9]
11	§ 5.3.11	MSA zajistí, že klíče, jejichž platnost vypršela, nejsou používány k žádnému účelu. Privátní klíč členského státu bude buď: zničen, tak aby privátní klíč nemohl být znovu zprovozněn nebo uchován způsobem zabraňujícím jeho užívání.	§ 6.2 Pár klíčů CZCA (MS.SK, MS.PK) [r6.7]
12	§ 5.3.12	MSA zajistí, že klíč k zařízení RSA je generován, přepravován a vkládán do zařízení takovým způsobem, aby byla uchována jejich důvěrnost a integrita. Pro tyto účely MSA:	§ 7.1 Všeobecné požadavky, záznam [r7.1] § 7.2 Generace klíčů [r7.5]

položka	odkaz v politice ERCA	Požadavky	odkaz v CZCA politice
		- zajistí, aby byly splněny jakékoli příslušné předpisy dané bezpečnostní certifikací zařízení, - zajistí, aby se jak generace tak vložení (pokud není onboard) uskutečnily ve fyzicky zabezpečeném prostředí, - pokud generace klíče nebyla pokryta bezpečnostní certifikací zařízení, zajistí, aby byly použity určené a vhodné algoritmy pro generaci kryptografického klíče, Poslední dva z těchto požadavků na generaci budou splněny generací klíčů pro vybavení v rámci zařízení, které buď: a) má oprávnění plnit požadavky určené v FIPS 140-2 (or FIPS 140-1) úroveň 3 nebo vyšší [9]; b) má oprávnění být v souladu s požadavky stanovenými v CEN Workshop Agreement 14167-2 [10]; c) je oprávněným systémem, který je zajištěn na EAL4 nebo vyšší v souladu s ISO 15408 [11]; na úroveň E3 nebo vyšší v ITSEC [12]; nebo odpovídající bezpečnostní kritéria. Tato ohodnocení budou k profilu ochrany nebo bezpečnostnímu plánu; d) prokáže, že poskytuje odpovídající úroveň zabezpečení.	
13	§ 5.3.13	MSA zajistí důvěrnost, integritu a dostupnost privátního klíče, generovaného, uloženého a používaného pod kontrolou politiky MSA.	§ 5 Management karet a vybavení [r5.6] § 6 Klíčový management v rámci CZCA (odstavec 2) § 7.1 Všeobecné požadavky, záznam [r7.2]
14	§ 5.3.14	MSA zabrání neoprávněnému použití privátních klíčů generovaných, uložených a používaných pod kontrolou politiky MSA.	§ 6 Klíčový management v rámci CZCA (odstavec 2) § 6.2 Pár klíčů CZCA

položka	odkaz v politice ERCA	Požadavky	odkaz v CZCA politice
			(MS.SK, MS.PK) [r6.9] § 7.2 Generace klíčů [r7.8]
15	§ 5.3.15	Privátní klíče členského státu mohou být podpořeny použitím procedury obnovení klíče, vyžadující alespoň dvojitou kontrolu.	§ 7.3 Aplikace klíčů [r7.11]
16	§ 5.3.16	Požadavky na certifikaci klíče, které závisí na přepravě privátních klíčů, nejsou povoleny.	§ 8.2 Vydávání certifikátů [r8.7]
17	§ 5.3.17	Uložení klíče u třetí osoby (Key escrow) je přísně zakázáno.	§ 6.2 Pár klíčů CZCA (MS.SK, MS.PK) [r6.11]
18	§ 5.3.18	MSA zabrání neoprávněnému použití klíčů pro senzory pohybu.	§ 6.3 Symetrické klíče pro workshop karty a senzory vzdálenosti a pohybu (Km, Kmwc, Kmvu) [r6.18]
19	§ 5.3.19	MSA zajistí, že master klíč pro pohybové senzory (Km) je používán pouze k zašifrování dat pro senzor pohybu pro účely výrobců senzorů pohybu. Data určená k zašifrování jsou definována v ISO / IEC 16844-3 standard [7].	§ 6 Klíčový management v rámci CZCA (odstavec 2)
20	§ 5.3.20	Master klíč pro senzory pohybu (Km) nikdy neopustí bezpečné a kontrolované prostředí MSA.	§ 6.3 Symetrické klíče pro workshop karty a senzory vzdálenosti a pohybu (Km, Kmwc, Kmvu) [r6.18]
21	§ 5.3.21	MSA doručí klíč k pohybovým senzorům workshop karet (KmWC) personalizátorovi komponentů (v případě služby personalizace karty), s využitím odpovídajících prostředků zabezpečení, výhradně pro účely vložení do workshop karet.	§ 6.3 Symetrické klíče pro workshop karty a senzory vzdálenosti a pohybu (Km, Kmwc, Kmvu) [r6.18]
22	§ 5.3.22	MSA doručí klíč pro senzor pohybu dopravních prostředků (KmVU) personalizátorovi komponentů (v tomto případě výrobci dopravních prostředků),	§ 6.3 Symetrické klíče pro workshop karty a senzory vzdálenosti a pohybu (Km, Kmwc,

položka	odkaz v politice ERCA	Požadavky	odkaz v CZCA politice
		s využitím odpovídajících prostředků zabezpečení, výhradně pro účely vložení do dopravních prostředků.	Kmvu) [r6.18]
23	§ 5.3.23	MSA bude udržovat důvěrnost, integritu a dostupnost svých kopií klíčů k senzorům pohybu.	§ 6 Klíčový management v rámci CZCA (odstavec 2)
24	§ 5.3.24	MSA zajistí, že kopie klíčů k pohybovým senzorům jsou uloženy v rámci zařízení, které buď: a) má oprávnění splňovat požadavky určené v FIPS 140-2 (nebo FIPS 140-1) úroveň 3 nebo vyšší [9]; b) je důvěryhodným systémem, který je zajištěn na EAL4 nebo vyšší v souladu s ISO 15408 [11]; na úroveň E3 nebo vyšší v ITSEC [12]; nebo ekvivalentní bezpečnostní kritéria. Tato hodnocení budou k ochrannému profilu nebo bezpečnostnímu účelu.	§ 6 Klíčový management v rámci CZCA (odstavec 2)
25	§ 5.3.25	MSA bude vlastnit různé páry klíčů členského státu pro ochranu certifikátů veřejných klíčů pro výrobu dopravních prostředků a vybavení s tachografovými kartami.	§ 6.2 Pár klíčů CZCA (MS.SK, MS.PK) [r6.3] § 7.3 Aplikace klíčů [r7.9]
26	§ 5.3.26	MSA zajistí dostupnost své služby certifikace veřejného klíče pro zařízení.	§ 6.2 Pár klíčů CZCA (MS.SK, MS.PK) [r6.6]
27	§ 5.3.27	MSA bude používat privátní klíče členského státu pouze pro: a) výrobu certifikátů pro klíče vybavení z přílohy I(B) s využitím digitálního podpisového algoritmu ISO / IEC 9796-2, jak je popsán v příloze I(B) dodatek 11 Běžné bezpečnostní mechanismy (*Common Security Mechanism)* [6]; b) výrobu požadavku na certifikaci klíče ERCA, jak je popsáno v příloze A; c) vydávání seznamů rušených certifikátů, pokud je tato metoda používána pro poskytování certifikátu.	§ 6.2 Pár klíčů CZCA (MS.SK, MS.PK) [r6.4]
28	§ 5.3.28	MSA podepíše certifikáty pro vybavení ve stejném zařízení, jaké bylo použito	§ 6 Klíčový management v rámci

položka	odkaz v politice ERCA	Požadavky	odkaz v CZCA politice
		pro uložení privátních klíčů členského státu (viz 5.3.2).	CZCA (odstavec 4)
29	§ 5.3.29	V rámci své působnosti, MSA zajistí, že veřejné klíče pro vybavení budou identifikovány unikátním klíčovým identifikátorem, který splňuje předpisy přílohy 1(B) [6].	§ 8.4 Obsah a formáty certifikátů [r8.9]
30	§ 5.3.30	Pokud generace a certifikace klíče není provedena ve stejném fyzicky zabezpečeném prostředí, protokol o požadavku na certifikaci klíče bude poskytovat důkaz o původu a integritě požadavků na certifikaci, aniž by byl odhalen privátní klíč.	§ 8 Registrace [r8.3]
31	§ 5.3.31	MSA bude udržovat a zpřístupňovat informace o statusu certifikátu.	§ 8.2 Vydávání certifikátů [r8.8]
32	§ 5.3.32	Platnost certifikátu tachografové karty bude stejná jako platnost tachografové karty.	§ 8.3 Platnost certifikátu [r8.9]
33	§ 5.3.33	MSA zabrání vložení certifikátů s neurčitou platností do tachografových karet.	§ 8.3 Platnost certifikátu [r8.9]
34	§ 5.3.34	MSA může povolit vložení certifikátů členského státu s neurčitou platností do přepravních prostředků.	§ 8.3 Platnost certifikátu [r8.9]
35	§ 5.3.35	MSA zajistí, že uživatelé karet jsou identifikováni na určitém stupni procesu vydávání karet.	§ 5 Management karet a vybavení [r5.8] § 7.3 Aplikace klíče [r7.10]
36	§ 5.3.36	MSA zajistí, že ERCA je informován bez odkladu o ztrátě, krádeži nebo potenciálnímu znehodnocení jakéhokoli klíče MSA.	§ 6.2 Pár klíčů CZCA (MS.SK, MS.PK) [r6.12]
37	§ 5.3.37	MSA bude implementovat odpovídající mechanismy pro znovu zprovoznění při katastrofě, které nezávisí na čase odezvy ERCA	§ 6.2 Pár klíčů CZCA (MS.SK, MS.PK) [r6.6] § 9 Bezpečnost IT [r9.13]
38	§ 5.3.38	MSA zavede systém managementu zabezpečení informací (ISMS) založený na zvážení rizik pro všechny operace,	§ 9.1 IT Systém bezpečnostního managementu (ISMS)

položka	odkaz v politice ERCA	Požadavky	odkaz v CZCA politice
		kterých se to týká.	[r9.1]
39	§ 5.3.39	MSA zajistí, že politiky se odrazí v proškolení personálu, vyčištění (clearance) a funkcích.	§ 9.2 Speciální požadavky bezpečnostního konceptu [r9.5] § 9.3 Rozdělení funkcí [r9.15]
40	§ 5.3.40	MSA zajistí, že budou zachovávány příslušné záznamy certifikačních operací.	§ 8.4 Obsah a formáty certifikátů [r8.10] § 9 IT Zabezpečení [r9.10] [r9.11] [r9.12]
41	§ 5.3.41	MSA bude zahrnovat ustanovení pro ukončení MSCA v politice MSA.	§ 10.1 Přesun odpovědnosti CZCA
42	§ 5.3.42	Politika MSA bude zahrnovat procedury změn.	§ 12 Úpravy a přizpůsobení politiky CZCA [r12.1]
43	§ 5.3.43	Audit MSA stanoví, zda požadavky této sekce jsou dodržovány.	§ 11.1 CZCA [r11.1] 2. odstavec
44	§ 5.3.44	MSA bude provádět audit operací zahrnutých ve schválené politice v intervalech ne delších než 12 měsíců.	§ 11.1 CZCA [r11.1] 1. odstavec
45	§ 5.3.45	MSA podá zprávu o výsledcích auditu, jak je zmíněno v 5.3.43 a poskytne zprávu o auditu v angličtině ERCA.	§ 11.1 CZCA [r11.3]
46	§ 5.3.46	Zpráva o auditu bude stanovovat jakékoli nápravné akce, včetně časového rozvrhu implementace, požadované ke splnění povinností MSA.	§ 11.1 CZCA [r11.3]

14 Glosář/Definice a zkratky

Politika certifikačních orgánů	Definovaný soubor předpisů, který vyjadřuje použitelnost klíčů, certifikátů a zařízení pro určitý okruh uživatelů (komunitu) anebo kategorii použitelnosti se společnými požadavky na zabezpečení.
Karta/karta systému Digitální tachograf	Karta s integrovaným obvodem, v této politice má tento termín stejné použití jako „**IC-karta**“ a „**paměťová karta**“.

Držitel karty	Osoba nebo organizace vlastnící a užívající kartu systému Digitální tachograf. Mezi ně patří řidiči, firemní zástupci, dílenští pracovníci a pracovníci kontrolního orgánu.
Certifikát	V obecném kontextu je certifikát zpravována struktura obsahující závazný podpis vydavatele, kterým se potvrzuje správnost informací obsažených v certifikátu a dále skutečnost, že vlastník certifikovaného veřejného klíče může doložit vlastnictví asociovaného privátního klíče.
Systém certifikačního orgánu (CAS)	Počítačový systém, v němž se vydávají certifikáty podepsáním údajů (uživatelských) certifikátu pomocí privátního podpisového klíče certifikačního orgánu.
Zařízení	V rámci systému Digitální tachograf existují tato zařízení: Karty systému Digitální tachograf, záznamová zařízení – záznamové zařízení montované do vozidel a senzory pohybu.
Záznamová zařízení	Jednotky montované do vozidel (elektronická záznamová zařízení), pracující dle podmínek daných
Senzor pohybu	Senzory montované do vozidla, zdroj informací o pohybu vozidla pro záznamové zařízení, pracující dle podmínek daných Nařízením Rady (ES) č. 1360/2002
Výrobce/Výrobce zařízení	Výrobci zařízení pro systém Digitální tachograf. V tomto dokumentu se toto označení nejčastěji používá pro výrobce záznamových zařízení (jednotek montovaných do vozidel) a výrobce senzorů pohybu, poněvadž tito výrobci mají v rámci systému jasně vymezené funkce.
Klíč senzoru pohybu	Symetrický klíč používaný pro senzory pohybu a jednotky montované do vozidel pro zaručení vzájemného rozpoznání.
Specifikace běžných postupů (PS)	Přehled zabezpečovacích postupů používaných v procesech v rámci systému Digitální tachograf.
Tajný klíč	Neveřejná část asymetrického páru klíčů používaná pro šifrovací techniky veřejného klíče.
Privátní klíč	Neveřejná část asymetrického páru klíčů používaná pro šifrovací techniky veřejného klíče. Typickým použitím privátního klíče jsou digitální podpisy nebo dešifrování zpráv.
Veřejný klíč	Veřejná část asymetrického páru klíčů používaná pro šifrovací techniky veřejného klíče. Veřejný klíč se nejčastěji používá pro ověřování digitálního podpisu nebo pro zašifrování zpráv určených vlastníkovi privátního klíče.

Klíče RSA	RSA je šifrovací algoritmus používaný pro asymetrické klíče (PKI) v systému Digitální tachograf.
Servisní agentura	Subjekt, který na sebe přebírá úkoly certifikačního orgánu členského státu a plní je jeho jménem, tedy subdodavatel.
Tachograf karty/ karty	Čtyři různé typy paměťových karet určených k použití v rámci systému Digitální tachograf: karta pro řidiče, firemní karta, dílenská karta a kontrolní karta.
Uživatel	Za uživatele označujeme uživatele zařízení a jsou to buď **držitelé karet** v případě karet nebo **výrobci** v případě záznamových zařízení/ senzorů pohybu. Všichni uživatelé musí být jedinečně identifikovatelnými subjekty.
V rámci tohoto dokumentu mají níže uvedené výrazy tento význam:	
Podepsaný	V případech, kdy tato politika vyžaduje podpis, je tento požadavek splněn zabezpečeným a ověřitelným digitálním podpisem.
Písemný	V případech, kdy tato politika vyžaduje písemné informace, je tento požadavek splněn formou datové zprávy, pokud informace v ní obsažené jsou natolik přístupné, aby je mohly zainteresované strany využít.

14.1 Seznam zkratek - anglický ekvivalent a český překlad

CA	Certification Authority	certifikační orgán
CAA/PA	Certification Authority Administrator/Personalization Administrator	správce certifikačního orgánu/Organizace pro personalizaci karet
CAS	Certification Authority System	systém certifikačního orgánu
CZCIA	Czech Card Issuing Authority	orgán pro vydávání karet systému Digitální tachograf České republiky
CZCP	Czech Card Personalization Organization	organizace pro personalizaci karet systému Digitální tachograf České republiky
CPS	Certification Practice Statement	specifikace běžných certifikačních postupů
ERCA	European Root CA	evropský kmenový certifikační orgán
ISSO	Information Systém Security Officer	inspektor ochrany informačního systému
ITSEC	Information Technology Security Evaluation Criteria	kritéria pro hodnocení zabezpečení IT
KG	Key Generation	generování klíče(ů)
MS	Member State	členský stát
CZA	Czech Authority	pověřený orgán České republiky pro systém Digitální tachograf
CZCA	Czech CA	certifikační orgán České republiky
PIN	Personal Identification Number	PIN, osobní identifikační číslo
PKI	Public Key Infrastructure	infrastruktura veřejného klíče
RSA	RSA	specifický algoritmus veřejného klíče
SA	System Administrator	správce systému
PS	Practice Statement	specifikace běžných postupů
VU	Vehicle Unit	záznamové zařízení
VUP	VU Personalizing Organization	organizace pro personalizaci záznamových zařízení

15 Schválení resortní politiky certifikačních orgánů systém Digitální tachograf

15.1 Potvrzení o schválení evropským certifikačním orgánem ERCA

EUROPEAN COMMISSION
DIRECTORATE GENERAL
Joint Research Centre

Institute for the Protection and Security of the Citizen
Traceability and Vulnerability Assessment Unit

CKDP
0100100000245117

MINISTERSTVO DOPRAVY
04 -11- 2005
40004/2005 - MD - CKDP

16 August 2005
G07-TRVA/JB/jb/(2005)D20574

Ministry of Transport of the Czech Republic
Nábřeží Ludvíka Svobody 1222/12
110 15 Prague 1
Czech Republic

To the attention of: Ing. Miroslav Duda

Subject: Start of services to the Czech Republic

Dear Mr. Duda,

We confirm the receipt of the following documents in response to our letter G07-TRVA/JB/jb/(2005)D/18509:

1. NCA Policy for the Digital Tachograph System in the Czech Republic v1.01 (hereinafter CZ-MSA);
2. FIPS 140-1 Validation Certificate no.160;
3. Security certificate BSI-DSZ-CC-0272-2004.

All of our requests for additional information have been addressed in a satisfactory manner, and we confirm our readiness to initiate key certification and distribution services to the entities operating under the CZ-MSA policy.

Yours sincerely,

J.W.Bishop

Attachments: None

Copy: J-M.Cadiou, A.Poucet, J-P.Nordvik (DG-JRC); L. Hubeers (DG-TREN)

J.W.Bishop G07-TRVA
Tel: +39-0332-789225
Fax: +39-0332-789289
e-mail: james.bishop@jrc.it

1/1

D20574 Start Of Services.Doc

15.2 Protokol o schvalování ERCA

EUROPEAN COMMISSION
DIRECTORATE GENERAL
Joint Research Centre

Institute for the Protection and Security of the Citizen
Traceability and Vulnerability Assessment Unit

22 July 2005
G07-TRVA/JB/jb/(2005)D/18509

Ministry of Transport of the Czech Republic
Nábřeží Ludvíka Svobody 1222/12
110 15 Prague 1
Czech Republic

To the attention of: Ing. Miroslav Duda

Subject: Approval of the National Certification Authority Policy for Digital Tachograph System in the Czech Republic, Version 2.0

Dear Mr. Duda,

We confirm the receipt of the above document (hereinafter: CZ-MSA) by DHL on 20th July 2005.

This document has been reviewed for conformity with Chapter 5 of the ERCA policy (hereinafter: ERCA-CP). Attachment 1 contains the review findings.

The review process identified no required changes to the CZ-MSA policy. This is the first time that a national policy has complied with the ERCA-CP on the first review, so please accept our compliments to you and your Department for the thorough preparation of this document.

Items 1, 4, and 5 in the Review Findings request additional information to be presented before the ERCA will provide services to the entities operating under the CZ-MSA policy.

Yours sincerely,

J.W.Bishop

Attachments:
1 – Review Findings

Copy: J-M.Cadiou, A.Poucet, J-P.Nordvik (DG-JRC); L. Huberts (DG-TREN)

J.W.Bishop G07-TRVA
Tel: +39-0332-786225
Fax: +39-0332-786280
e-mail: james.bishop@jrc.it

1/1

D18509 Approval 2005-07-22.Doc

Attachment 1: Review Findings

1. **Additional information request:** ERCA-CP §5.3.2: evidence of the certification of the device(s) actually used for national key generation.
2. **Remark:** ERCA-CP §5.3.7: CZ-MSA §1.1 does not identify manufacturers of vehicle units or of motion sensors. Requests for the motion sensor master keys Km and Km_{VU} will therefore be rejected by the ERCA, until CZ-MSA §1.1 is modified to identify vehicle unit and / or motion sensor manufacturers.

   Rationale: ERCA-CP §6.4.2 states that motion sensor keys are distributed only on a "need to know" basis.
3. **Typographical error:** ERCA-CP §5.3.10: the correspondence table entry in CZ-MSA §13 refers to [r8.9] instead of [r8.10].
4. **Additional information request:** ERCA-CP §5.3.12: evidence of the following certifications is requested:
   - certification of the device(s) actually used for card key generation;
   - security certification of the tachograph card adopted by the Czech Republic.
5. **Additional information request:** ERCA-CP §5.3.24: evidence of the certification of the device(s) actually used to store motion sensor keys.
6. **Typographical error:** ERCA-CP §5.3.34: the correspondence table entry in CZ-MSA §13 does not contain the reference to the ERCA-CP article.

16 Resortní politika certifikačních orgánů systému Digitální tachograf

Resortní politika certifikačních orgánů systému digitální tachograf České republiky verzi 2.0 zpracovalo Ministerstvo dopravy České republiky v roli CZA (CZA - Czech Authority), tj. v úloze nevyššího orgánu České republiky pro systém digitální tachograf.

Tato verze Resortní politika certifikačních orgánů systému digitální tachograf České republiky ve verzi 2.0 je v platnosti ode dne schválení pověřeným orgánem EU, a to od **16. srpna 2005**.

Česká republika, ministerstvo dopravy
nábřeží L. Svobody 12/1222
110 15 Praha 1

2. Národní certifikační politika pro Karty DT druhé generace

2. 1. Certifikační politika MSA-CZ pro Tachografový systém

Národní autorita České republiky pro systém Digitálního tachografu

CERTIFIKAČNÍ POLITIKA MSA-CZ

Tachografový systém

Verze: 1.0

Datum vydání: 4. 2. 2019

OBSAH

1 Úvod

1.1 Předmět Certifikační politiky

Tato CP je nově vytvořená certifikační politika České republiky pro MSA-CZ pro tachografový systém, který odpovídá požadavkům druhé generace tachografového systému nazývaného Smart Tachograph nebo také GEN2, které vychází z Nařízení Evropského parlamentu a Rady (EU) č. 165/2014 (Nařízení č. 165/2014).

Technické požadavky na komponenty tachografového systému jsou definovány v Prováděcím nařízení Komise (EU) č. 2016/799 (Prováděcí nařízení č. 2016/799) [2] a jeho novelizaci Prováděcím nařízením č. 2018/502 [3].

Struktura dokumentu vychází z doporučení nadřízené CP vydané ERCA [1].

Specifickou vlastností tachografového systému je, že mimo standardní PKI žádosti a certifikáty vydávané MSCA, musí řešit i správu symetrických klíčů, které jsou na úrovni MSCA distribuovány do komponent, které to vyžadují.

Tato CP také klade požadavky na další subjekty, které se podílí na zpracování žádostí o TC a jejich distribuci držitelům.

Funkcionalita MSCA-CZ je omezena pouze na vydávání certifikátů pro tachografové karty a správu symetrických klíčů určených do tachografových karet. Toto omezení vychází z toho, že:

- MSCA-CZ nepodporuje vydávání certifikátů MSCA_VU-EGF, protože v zemi není výrobce VU *(Vehicle Unit*) ani EGF *[External GNSS (Global Navigation Satellite System) Facilites].*
- MSCA-CZ nepodporuje výrobu snímačů pohybu.

Z uvedeného je patrné, že MSCA-CZ spravuje pouze tyto získané kryptografické komponenty

- Kořenový certifikát ERCA, případně původní a nový certifikát a jejich link certifikát.
- Certifikát vydaný ERCA pro MSCA_Card.
- Symetrický klíč K_M-WC.
- Symetrický klíč K_DSRC.

V rámci své činnosti MSCA-CZ vydává certifikáty pro všechny typy tachografových karet.

1.2 Jméno dokumentu a identifikace

Tento dokument je certifikační politikou subjektu MSA-CZ (Member State Authority) zodpovědné za provozování Smart Tachograf systému v České republice a nahrazuje tak původní **Resortní politiku certifikačních orgánů pro systém Digitální tachograf v České republice s** přechodem na verzi GEN2 (Smart Tachograph).

Dokument se jmenuje Certifikační politika MSA-CZ Tachografový systém.

Aktuální verze dokumentu je 1.0.

Tato politika vstupuje v platnost dne 4. února 2019.

CP nemá přidělen identifikátor na úrovni ASN1, protože samotný certifikát neobsahuje takový atribut (struktura CV certifikátů jej nevyužívá).

1.3 Zúčastněné strany

Zúčastněné strany Smart Tachografového systému jsou zachyceny na obrázku 1.

1.3.1 ERCA - Evropská kořenová CA

ERCA sama si vydá kořenový certifikát a v případě jeho obnovy i příslušný link certifikát.

ERCA pak s využitím aktuálně platného certifikátu vydává certifikáty národním MSCA. Součástí vydání MSCA certifikátu je i předání kořenového certifikátu případně i předchozího platného certifikátu s odpovídajícím link certifikátem.

ERCA také generuje a distribuuje symetrické klíče tachografového systému.

1.3.2 MSA-CZ - Národní Autorita České republiky

Národní autorita v kontextu této CP je instituce zastřešující a garantující funkci komponent Smart tachografového systému na území státu. MSA-CZ je vykonávána Ministerstvem dopravy České republiky (dále jen MD).

Základní požadavky kladené na MSA-CZ:

1. MSA-CZ je zodpovědná za vydání CP (tento dokument) v anglické verzi a její dodání na ERCA. ERCA vyhodnotí soulad dodané politiky s požadavky politik ERCA. MSA-CZ je povinna v případě nálezu upravit svou politiku.
2. MSC-CZ poté, co je CP schválena ERCA, může tuto politiku distribuovat klientům a závislým stranám.
3. Do doby než bude schválena CP, neposkytne ERCA certifikační služby MSCA_CZ.
4. MSA-CZ zodpovídá za periodické provádění auditu shody prostředí MSCA_CA s požadavky těchto politik a poskytuje výsledky těchto auditů ERCA. v případě nedodání těchto auditů ERCA neposkytne další certifikační služby.
5. MSA-CZ popíše všechny subjekty, jejich role a odpovědnost v procesu zpracování požadavku a vydání TC.

6. MSA-CZ vynutí periodické audity u subjektů, které v procesu vydání TC pracují s kryptografickými klíči (privátními i symetrickými). Součástí popisu je rozsah provedeného auditu.
7. MSA-CZ zachytí procesy správy kryptografických klíčů a certifikátů.
8. MSA-CZ vynutí, aby procesy generování a zápisu klíčů do karet garantovaly integritu a utajení.
9. MSA-CZ vynutí, aby každý uživatel TC byl identifikován v určitých stavech životního cyklu karty (žádost o kartu, vydání karty).
10. MSA-CZ je povinna informovat ERCA v případě kompromitace privátního klíče MSCA-CZ nebo některého symetrického klíče, který je ve správě MSCA-CZ.
11. MSA-CZ musí identifikovat procedury obnovy systému po katastrofě.
12. MSA-CZ vynutí, aby všichni jeho klienti měli aplikován systém ISMS. Jeho implementace musí odpovídat požadavkům ISO 27001.
13. MSA-CZ musí mít k dispozici opatření při ukončení činnosti MSCA-CZ.
14. MSA-CZ musí mít k dispozici změnové procedury.

Kontaktní adresa na MSA-CZ:

Ministerstvo dopravy ČR

Odbor agend řidičů

nábřeží Ludvíka Svobody 1222/12

110 15 Praha 1

Česká republika

1.3.3 MSCA-CZ - Národní CA České republiky

Národní CA pro potřeby tachografového systému.

Základní vlastnosti a požadavky na MSCA_CZ:

1. MSCA-CZ je jmenována MSA-CZ k implementaci národních politik a zabezpečení certifikačních služeb pro podporu personalizace TC.
2. MSCA-CZ je podřízena evropské ERCA.
3. MSCA-CZ je povinna dokumentovat tuto implementaci a vydat v podobě certifikační prováděcí směrnice (CPS) a předat ji MSA-CZ k ověření shody s požadavky CP. ERCA si může tuto CPS také vyžádat.
4. MSCA-CZ zajišťuje tyto hlavní činnosti:
    a. Generování vlastní žádosti o certifikát (CSR) a získání certifikátu vydaného ERCA.
    b. Generování žádosti o symetrické klíče poskytované ERCA a import těchto klíčů do MSCA.
    c. Správa všech držených kryptografických klíčů.

   d. Vydávání certifikátů ke klíčům určeným do tachografových karet.
   e. Podpora personalizačního procesu poskytnutím komponent spravovaných v MSCA-CZ a určených do TC.
5. MSCA-CZ musí garantovat, že procesy správy klíčů (generování, import, export) zajišťují těmto klíčům integritu a utajení.
6. MSCA-CZ je povinna informovat MSA-CZ o všech bezpečnostních incidentech, které mohou mít vliv na bezpečnost tachografového systému.
7. MSCA-CZ je provozována v prostředí CAP (Card Personaliser).
8. Obě komponenty (MSCA-CZ i CP) musí mít vybudován systém ISMS. Jeho implementace musí odpovídat požadavkům ISO 27001.

Kontaktní adresa na MSCA-CZ:

STÁTNÍ TISKÁRNA CENIN, státní podnik

Za Viaduktem 8

170 00 Praha 7

Česká republika

1.3.4 CAP (Card Personaliser)

CAP je subjekt pověřený MSA-CZ personalizací tachografových čipových karet.

Základní vlastnosti a požadavky na CP:

1. CAP je jmenován MSA-CZ pro potřeby personalizace TC.
2. CAP je zodpovědný za správnou personalizaci karet dle požadavků Prováděcího nařízení nařízení č. 2016/799 [2] a dalších relevantních požadavků včetně této politiky.
3. CAP je povinný informovat MSA-CZ o všech případných bezpečnostních incidentech, které mohou mít vliv na bezpečnost tachografového systému.
4. CAP je zodpovědný za výběr dodavatele TC a konkrétního čipu, který splňuje požadavky Prováděcího nařízení č. 2016/799 [2].
5. CAP je zodpovědný za výrobu vzorků pro funkční testy a jejich úspěšné provedení.
6. CAP je zodpovědný za zabezpečení karet TC proti jejich ztrátě a zneužití před jejich distribucí.

Kontaktní adresa na CAP je shodná s MSCA-CZ

1.3.5 CIA (Card Issuing Authority)

CIA je subjekt zodpovědný za vytvoření a provoz infrastruktury, která umožňuje zpracování žádostí o TC a jejich vydání držitelům karet.

Základní požadavky na CIA:

1. CIA garantuje provoz systému, který umožňuje sběr žádostí o TC a jejich distribuci žadatelům.
2. CIA je povinna řádně ověřit všechna data, která získává od držitelů karet v procesu přijetí žádosti o kartu, zejména pak ověřit jejich identitu.
3. CIA je povinna ověřit splnění všech předpokladů pro vydání daného typu karty pro identifikovaný subjekt, u karet řidiče zejména ověřit, zda řidič není držitelem jiné karty, případně karty vydané v jiné zemi.
4. CIA je povinna informovat držitele karty o všech požadavcích na něj kladených.
5. CIA je povinna zabezpečit data pro výrobu TC ve všech fázích životního cyklu (pořizování dat, správa, přenos do personalizace).
6. CIA je povinna zajistit bezpečnou distribuci vyrobených karet do místa výdeje jejich držitelům, včetně bezpečného předání PIN obálek pro karty dílny.
7. Přístup k datům spravovaných v systému CIA (ISDT) může být povolen jen autorizovaným osobám, na základě úspěšné autentizace.
8. Pokud CIA využívá služeb třetích stran, je povinna na tyto subjekty přenést požadavky na dodržení požadované bezpečnosti provozu.

Kontaktní adresa na CIA:

Ministerstvo dopravy ČR

Odbor agend řidičů

nábřeží Ludvíka Svobody 1222/12

110 15 Praha 1

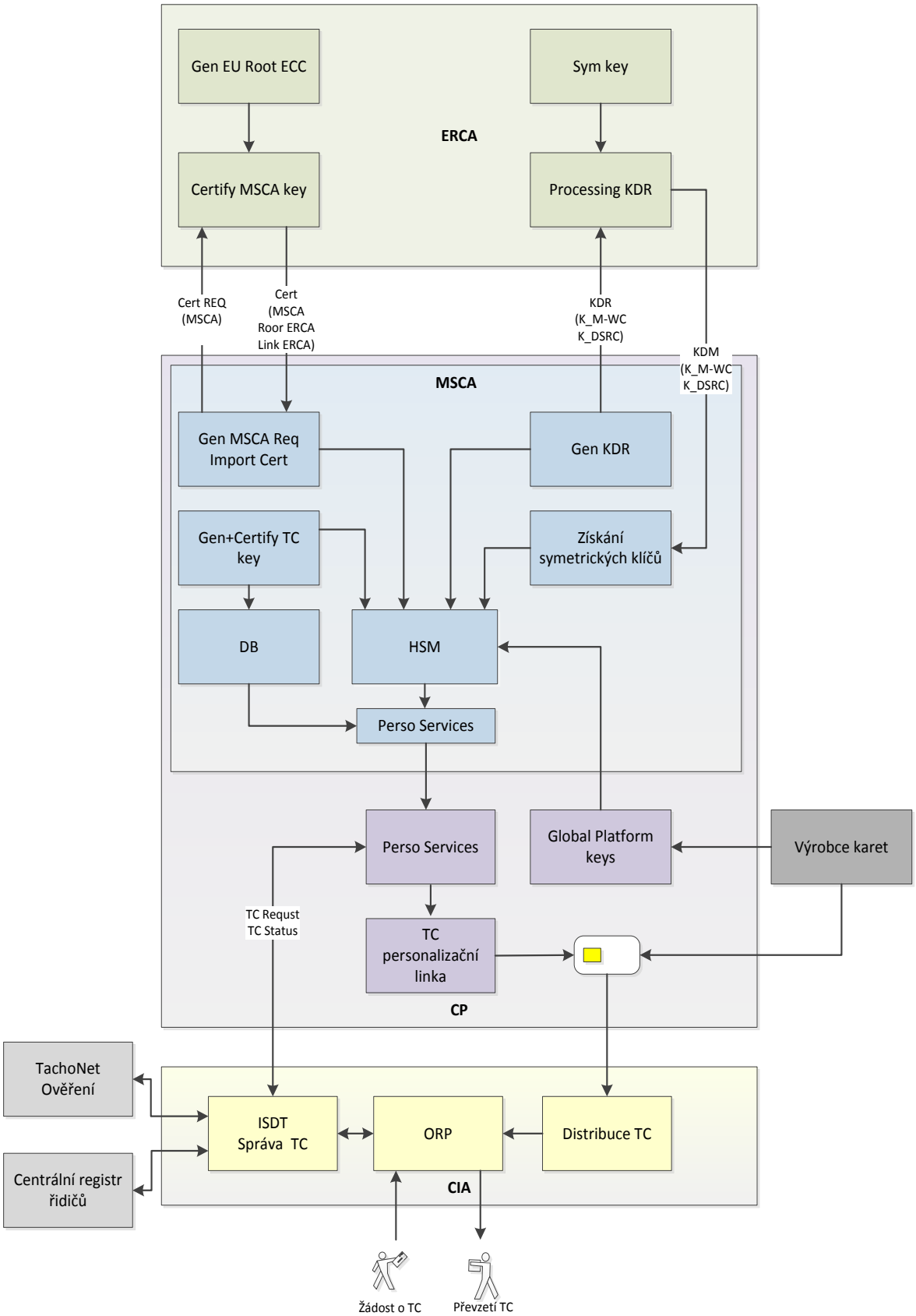
Česká republika

1.3.6 Držitel karty

Požadavky na držitele karty:

1. Držitel TC je povinen poskytnout CIA správné informace při podání žádosti o TC.
2. Držitel TC je povinen kartu využívat jen k danému účelu a zabránit její zneužití třetí osobou.
3. Držitel karty může být vlastníkem pouze jediné platné karty řidiče.
4. Držitel TC nesmí používat poškozenou nebo expirovanou kartu.
5. Držitel TC je povinen ihned nahlásit CIA, že došlo k poškození karty, zcizení nebo její ztrátě, případně zneužití jinou osobou.
6. Držitel TC je povinen poškozenou kartu nebo expirovanou kartu vrátit CIA.

Kontaktní údaje na držitele karty (bydliště, volitelně telefon a email) jsou udržovány v systému CIA – systém ISDT (viz obr. 1-) pro správu TC.


Gen EU Root ECC
Sym key
ERCA
Certify MSCA key
Processing KDR
Cert REQ (MSCA)
Cert (MSCA Roor ERCA Link ERCA)
KDR (K_M-WC K_DSRC)
KDM (K_M-WC K_DSRC)
MSCA
Gen MSCA Req Import Cert
Gen KDR
Gen+Certify TC key
Získání symetrických klíčů
DB
HSM
Perso Services
Perso Services
Global Platform keys
Výrobce karet
TC Requst TC Status
TC personalizační linka
CP
TachoNet Ověření
ISDT Správa TC
ORP
Distribuce TC
Centrální registr řidičů
CIA
Žádost o TC
Převzetí TC

Obrázek 1: Zúčastněné strany v systému Smart tachograph

1.3.7 Klienti CA

Z pohledu ERCA jsou klienty všechny národní MSCA.

Z pohledu MSCA-CZ je jediným jejím klientem subjekt zajišťující personalizaci tachografových karet (CAP).

CAP zajišťuje personalizaci pouze tachografových čipových karet:

- Karty řidiče
- Karty podniku
- Karty kontrolní
- Karty dílny

Z obecnějšího pohledu je možné chápat jako klienty i koncové držitele karet, které obsluhuje CIA v procesu pořízení žádosti a vydání karty.

1.3.8 Závislé strany CA

Závislými stranami jsou obecně národní kontrolní subjekty, které vyhodnocují dodržování politik stanovených pro kamionovou dopravu prostřednictvím tachografových karet. Na údajích z těchto karet jsou dále závislí:

- Řidiči - držitelé TC.
- Společnosti - držitelé karty podniku pro ověření dodržení režimu jízdy.
- Držitelé karet dílny pro nastavení parametrů senzorů ve vozidlech.
- Držitelé kontrolních karet pro kontrolu provozu (Policie ČR).

V užším pohledu jsou navzájem závislými stranami jednotky VU a tachografové karty (TC), které spolu komunikují a využívají vydané certifikáty ke vzájemné autentizaci.

1.4 Použití klíčů a certifikátů

Certifikáty ERCA představují nejvyšší bod důvěry v tomto PKI systému. Závislé strany proto umísťují tento certifikát do všech typů tachografových karet a VU, kde slouží k ověření certifikátů strany, se kterou komunikují.

MSCA-CZ smí využít své privátní klíče jen pro tyto potřeby:

1. Podepsání vlastní žádosti o certifikát (vytvoření CSR).
2. Podepsání certifikátů vydaných pro tachografové karty.

Certifikáty MSCA-CZ mohou být využity jen k ověření klientských certifikátů (Card_MA, Card_Sign) vydaných MSCA-CZ.

Card_MA certifikát a příslušný privátní klíč může být využit jen v kartě pro vzájemnou autentizaci s VU a ustavení komunikační relace (session) mezi kartou a VU.

Card_Sign certifikát může být využit pro ověření autenticity a integrity dat vyčtených z čipové karty, přičemž příslušný privátní klíč je použit jen pro podpis těchto vyčítaných dat.

Symetrické klíče:

MSCA-CZ zajistí bezpečnou distribuci klíče K_M-WC do čipu servisní karty v procesu personalizace karty.

MSCA-CZ zajistí bezpečnou distribuci klíče K_DSRC do čipu servisní a kontrolní karty v procesu personalizace karty.

1.5 Správa politik CP, CPS

Za správu této CP zodpovídá MSA-CZ. Kontaktní adresa:

Ministerstvo dopravy

Odbor agend řidičů

nábřeží Ludvíka Svobody 1222/12

110 15 Praha 1

Česká republika

1.6 Tabulka pojmů a zkratek

Zkratka	Definice	Popis
ASCII	American Standard Code for Information Interchange	Definuje kódování znaků abecedy pro přenos mezi systémy
ASN1	Abstract Syntax Notation One	Protokol pro popis datových struktur pro přenos mezi systémy
CA	Certification Authority	Certifikační autorita
CAR	CA Reference	Datová struktura identifikující v certifikátu vydávající certifikační autoritu a její klíč
CHA	Certificate Holder Authorization	Pověření pro držitele certifikátu
CHR	Certificate Holder Reference	Datová struktura identifikující držitele Certifikátu
CIA	Card Issuing Authority	Autorita (orgán) vydávající karty
CAP	Card Personaliser	Personalizátor tachografových karet
CP	Certificate Policy	Certifikační politika
CPS	Certification Practice Statement	Certifikační prováděcí směrnice
CSR	Certificate Signing Request	Žádost o certifikát
CV Cert.	Card Verifiable Certificate	Certifikát verifikovatelný čipovou kartou
DB	Databáze	Strukturované úložiště dat informačního systému
DSRC	Dedicated Short Range Communication	Technologie pro bezdrátové snímání jednotky ve vozidle pro potřeby kontrolních orgánů.
DT	Digitální tachograf	Zařízení registrující stav a rychlost vozidla
EA	European Authority	Evropská autorita
ECC	Elliptic Curve Cryptography	Kryptografický algoritmus založený na eliptických křivkách
ERCA	European Root Certification Authority	Kořenová certifikační autorita pro systém Digitálního tachografu v JRC, Ispra
HSM	Hardware Security Module	Kryptgrafický modul – HW zařízení pro bezpečné uložení citilivých

		krypgorafických dat
ISMS	Information Security Management System	Systém Řízení informační bezpečnosti
ISDT	Informační systém Digitálního tachografu	Systém sběru a evidence dat pro personalizaci karet DT
KDR	Key Distribution Request	Datová zpráva žádající o kryptografický klíč
KDM	Key Delivery Message	Datová zpráva předávající kryptografický klíč
K_M-WC	WC part of K_M	Symetriický klíč pro kartu dílny
K_DSRC	DSRC Master Key	Symetrický klíč pro zabezpečení přenosu
MA	Mutual Authentication	Vzájemná autentizace – kryptografické ověření pravosti obou komunikujících stran
MAC	Message Authentication Code	Kód zabezpečující integritu a autenticitu dat
MSA-CZ	Member State Authority - Czech Republic	Národní autorita mezinárodně garantující funkcionalitu Digitálního tachografu
MSCA-CZ	Member State Certification Authority - Czech Republic	Národní certifikační autorita garantující bezpečnost personalizačního systému a vydávaných karet Digitálního tachografu
ORP	Municipality	Obec s rozšířenou působností
PKI	Public Key Infrastructure	Infrastruktura veřejného klíče – technologie pro zajištění důvěrnosti, autenticity a neodmítelnosti odpovědnosti založená na asymetrické kryptografii
TC	Tachograph Card	Karta tachografu
VU	Vehicle Unit (celek ve vozidle)	Jednotka pro čtení karet DT ve vozidle
WC	Workshop Card	Karta dílny

Poznámka: Označení typu autority doplněné znaky “-CZ” již představuje konkrétní subjekt, který realizuje její činnost v ČR (např. MSCA-CZ).

2 Zodpovědnost za zveřejnění informací

2.1 Uložení informací

ERCA je zodpovědná za provoz veřejného repozitáře, který obsahuje dokumenty ERCA, certifikáty, stavové informace o certifikátech. Repozitář je provozován jako veřejný web https://dtc.jrc.ec.europa.eu/.

MSCA-CZ je zodpovědná za uložení všech certifikátů vydaných pro tachografové karty včetně identifikace těchto karet. Přístup k těmto informacím je neveřejný, na vyžádání kontrolních orgánů a MSA.

2.2 Zveřejnění informací

MSA-CZ vydá vlastní politiky - CP MSA-CZ (tento dokument). ERCA vyhodnotí shodu s politikami ERCA a vydá osvědčení o shodě. Teprve poté může MSA-CZ předat svou politiku klientům a závislým stranám.

MSA-CZ periodicky provádí audit řešení MSCA, vyhodnocení předává ERCA.

2.3 Čas a frekvence zveřejnění informací

Předání informací o certifikátu probíhá na základě požadavku 3. strany.

Předání CP MSA-CZ do ERCA je součástí procesu schválení CP.

2.4 Přístup do repozitáře

Informace o certifikátech spravovaných v MSCA-CZ jsou udržovány v systému MSCA-CZ a nejsou veřejně dostupné. Na požadavek kontrolních orgánů nebo MSA-CZ mohou být informace o certifikátech předány třetím stranám na datovém nosiči.

3 Identifikace a Autentizace

Kapitola popisuje formu identifikace a autentizace v procesu iniciálního i následného vydání certifikátu nebo symetrického klíče.

3.1 Pojmenování

3.1.1 Typy jmen

3.1.1.1 Předmět a vydavatel certifikátu

V CV certifikátech je vydavatel a předmět certifikátu identifikováni položkami CAR a CHR. Položka CHA obsahuje typ zařízení, pro které je certifikát vydán. Jejich obsah pro ERCA, SCA-CZ a pro certifikát karty(TC) definuje následující tabulka:

subjekt	identifikátor	Struktura (délka v bytech)	hodnota
ERCA	CAR	NationNumeric(1) NationAlpha (3) KeySerialNumber (1) AdditionalInfo (2) CaIdentifier (1)	0xFD “EC ” Serial (0x01 - 0xFF) 0xFFFF (viz Poznámka 1) 0x01
MSCA-CZ	CHR/CAR (dle vystavitele certifikátu)	NationNumeric(1) NationAlpha (3) KeySerialNumber (1) AdditionalInfo (2) CaIdentifier (1)	0x0C “CZ “ Serial (0x01 - 0xFF) 0xFFFF 0x01
TC	CHR	Serial (4) MonthYear (2) BCD Type (1) ManufactorCode (1)	Serial v daném měsíci MMYY viz Poznámka 2 0xA6
All	CHA	tachAppID (6) equipmentType (1)	‘FF 53 4D 52 44 54’ viz Poznámka 3

Tabulka 1: Skladba identifikátorů subjektů tachografového systému

Poznámka 1: Atribut *AdditionalInfo* v testovacích certifikátech obsahuje ASCII hodnotu řetězce “TK” (0x54, 0x4B).

Poznámka 2: Hodnota položky *Type* z atributu CHR TC:

- 01 - pro kartu řidiče
- 02 - pro kartu dílny
- 03 - pro kartu kontrolní
- 04 - pro kartu podniku

Poznámka 3: Pozor na změny obsahu struktury CHA (Certificate Holder Authorization).

Komponenta *tachAppIDV* GEN1 obsahovala STRING (posloupnost znaků) “TACHO”, v GEN2 obsahuje STRING “SMRDT” (0x53, 0x4D, 0x52, 0x44, 0x54).

Komponenta *Equipment type* může nabývat hodnot uvedených u položky Type (viz Poznámka 2), dále pak (pro GEN2) může nabývat tyto specifické hodnoty dle určení certifikátu:

- 17 - pro kartu řidiče - podpisový certifikát
- 18 - pro kartu dílny - podpisový certifikát

Poznámka 4: Žádost o certifikát, kterou odesílá MSCA-CZ na ERCA musí obsahovat v atributu CHA položku *Equipment type* s hodnotou 14 - definuje subjekt MSCA (viz Příloha 1). Uvedené hodnoty jsou v dekadickém vyjádření, v certifikátu jsou uloženy jejich binární hodnoty.

Poznámka 5: Hodnoty *EquipmentType* jsou uvedeny v dekadickém vyjádření, do čipu se zapisuje binární hodnota.

3.1.1.2 Key Distribution Requests and Key Distribution Messages

Identifikace subjektu žádajícího o symetrický klíče se promítne do KDR a KDM ve formě identifikátoru efemérního klíče žádajícího subjektu. Jeho struktura je identická s údaji pro MSCA-CZ uvedenými v kapitole 3.1.1.1 s těmito rozdíly v hodnotě atributů:

- *keySerialNumber* musí být pro daný subjekt jedinečný a pro každou žádost jiný.

- *aditionalInfo* obsahuje hodnotu “KR” (0x4B,0x52) - Key Request, pro testovací žádost však zůstává hodnota “TK” (0x54, 0x4B) - Test Key.

Strukturu těchto zpráv plně definuje CP ERCA [1] (kap. 4.1)

3.2 Iniciální ověření identity

3.2.1 Ověření vlastnictví privátního klíče

MSCA-CZ je provozována v prostředí CAP. CAP pak v on-line spojení s MSCA-CZ žádá jediným požadavkem o vygenerování klíčového páru a vydání certifikátu daného typu a s požadovanou dobou platnosti. Klíčový pár je generován v lokálním HSM a MSCA-CZ proto nemusí ověřovat vlastnictví privátního klíče.

3.2.2 Ověření identity organizace

Jediným oprávněným klientem MSCA-CZ je subjekt jmenovaný MSA-CZ pro personalizaci tachografových karet (CP). Žádným jiným subjektům MSCA-CZ své služby neposkytuje a navržené architektonické uspořádání to ani neumožňuje.

V širším pojetí je možné chápat ověření identity organizace, která žádá o vydání tachografové karty pro potřeby svých zaměstnanců. Tato povinnost zůstává na subjektu CIA, který ověřuje identitu subjektu a jeho oprávněnost žádat o kartu daného typu.

3.2.3 Ověření identity osoby

Z důvodů uvedených v kap. 3.2.2 není na úrovni MSCA-CZ nijak možné ověřovat identitu osoby podávající žádost o certifikát. Tato povinnost zůstává na subjektu CIA, který realizuje ověření identity a oprávněnosti podat žádost o kartu touto identitou.

3.2.4 Ověření Autority

MSCA-CZ je provozována v prostředí CP, identitu autority není potřeba ověřovat.

3.2.5 Požadavky na interoperabilitu

CAP jako personalizátor TC je zodpovědný za výběr vhodného dodavatele čipových modulů, které vyhovují požadavkům EU [2]. Ověření této interoperability zajistí CAP funkčními testy vzorků karet před jejich typovým schválením (využití nástroje Collis). Následně CAP zajistí testy interoperability, které probíhají v JRC Ispra na základě kontraktu objednaného CP.

Testy interoperability ověří datovou kompatibilitu personalizovaných dat do čipu při provozu s různými výrobci VU.

MSCA-CZ nesmí spoléhat na služby žádné externí CA pro podepsání certifikátů a služby distribuce klíčů pro potřeby tachografového systému.

3.3 Ověření identity při obnově certifikátu

Požadavky na ověření identity při obnově certifikátu (vždy spojeno s vydáním nové karty) jsou identické jako v případě iniciálního ověření identity (viz kap. 3.2)

3.4 Ověření identity při revokaci certifikátu

Na úrovni MSCA-CZ| není poskytována funkčnost jak zneplatnit vydaný certifikát pro TC.

4 Požadavky na životní cyklus certifikátů a MASTER KEY

4.1 Žádost o certifikát MSCA-CZ a jeho vydání

4.1.1 Žádost o certifikát (CSR)

Tato kapitola shrnuje požadavky, které musí být splněny pro vydání certifikátu pro MSCA-CZ a také požadavky na vydání certifikátu pro TC a řízení jeho životního cyklu v prostředí MSCA-CZ.

Předpokladem pro úspěšné vydání certifikátu subjektu MSCA je vydání Prohlášení o shodě vydané Evropskou autoritou (podléhá European Commision) pro MSA, která zastřešuje příslušné MSCA.

Dalším nezbytným předpokladem je, aby MSCA předala svou CPS MSA a ta schválila shodu s vlastními politikami (CP). Oznámení o této shodě odesílá MSA na ERCA.

MSA je zodpovědná za periodické provádění auditu prostředí MSCA a vyhodnocování shody s poadavky této CP. MSA předává výsledky auditu na ERCA.

Žádost o certifikát generovaná MSCA-CZ musí odpovídat svou strukturou požadavkům uvedeným v dokumentu ERCA CP [1] kap. 4.1 tabulka 2.

Generování žádosti o certifikát MSCA-CZ musí probíhat ve fyzicky bezpečném prostředí pod duální kontrolou osob v důvěryhodných rolích.

Zařízení v němž jsou generovány a spravovány klíče MSCA-CZ musí splňovat požadavky této CP uvedené v kap. 6.2

Při generování žádosti se použije protokolová suite, dle tabulky níže, rozhodujícím faktorem volby je odpovídající síla kořenového certifikátu ERCA.

Suite	ECC key len[bitů]	AES key len[bitů]	hash	MAC len [byte]
CS#1	256	128	SHA-256	8
CS#2	384	192	SHA-384	12
CS#3	521	256	SHA-512	16

Tabulka 2: Protokolové suity pro tachografový systém

MSCA-CZ ověří na webových stránkách ERCA aktuální verzi klíče ERCA, tak aby bylo možné vydat žádost s odkazem na aktuální klíč - pro vytvoření správné hodnoty CAR v žádosti (viz kap. 2.1) a požadované kryptografické síly - použití konkrétní suite (viz Tabulka 2).

MSCA-CZ v žádosti o certifikát v položce CHA (Certificate Holder Authorization) uvede řetězec, který vznikne spojením Tachograph Application ID (‘FF 53 4D 52 44 54’) a typem zařízení (Equipment type), pro které je certifikát určen [pro MSCA je to jednobajtová hodnota 0x0E (‘FF 53 4D 52 44 54 0E’)].

MSCA-CZ pro vymezení časové platnosti certifikátu bude vycházet z doby platnosti 7 let + 1 měsíc, pro certifikát používaný pro TC.

Vnější podpis žádosti může chybět pouze v případě, že je jedná o iniciální žádost o certifikát. v následných žádostech musí být vnější podpis použit.

MSCA-CZ musí při generování žádosti spočítat hash celé žádosti (algoritmus odpovídá síle použitého klíče MSCA). Tato hash pak slouží ke vzdálené autorizaci žádosti při zpracování na ERCA. Tato hash musí být součástí protokolu o generování CSR.

Žádost o certifikát by měla být uložena na medium CD-R v single session mode (formát ISO 9660:1988).

MSCA-CZ by měla uložit na medium žádost ve třech formátech:

- ASCII (.txt file)
- Base64 (.pem file)
- Binary (.bin file)

MSCA-CZ vytiskne doprovodný papírový protokol o generování žádosti, který obsahuje položky specifikované v CPS ERCA.

Papírový protokol je součástí kurýrem předané žádosti na ERCA, kopii protokolu je předána i MSA-CZ, která autorizuje zpracování žádosti.

4.1.2 Zpracování žádosti o certifikát

Zpracování žádosti o certifikát je plně definováno v [1] v kap. 4.1.2

ERCA po ověření schopnosti zpracovat přijatou žádost autorizuje její původ. Autorizace spočívá v tom, že ERCA ověří telefonicky u kontaktní osoby MSA-CZ znalost hodnoty hash celé žádosti, která je na protokolu uvedena.

ERCA zapisuje certifikát na médium totožných vlastností jak bylo uvedeno u žádosti (CD-R, formát ISO 9660:1988).

MSCA-CZ by měla být schopna vydaný certifikát zpracovat ve všech poskytnutých formátech:

- ASCII (.txt file)
- Base64 (.pem file)
- Binary (.bin file)

Součástí vydaného certifikátu je i papírový protokol o vydání certifikátu.

4.1.3 Akceptace certifikátu

Kurýr MSCA-CZ podepisuje převzetí certifikátu v prostorách ERCA.

Po přijetí certifikátu v MSCA-CZ je nutné ověřit jeho použitelnost:

- Čitelnost média
- Správný formát certifikátu (viz Tabulka 3)
- Ověřit shodu údajů uvedených v CSR
- Ověření podpisu certifikátu s využitím veřejného klíče ERCA (certifikát ERCA je také zapsán na datový nosič s vydaným certifikátem)

Pokud některá z těchto kontrol bude neúspěšná, MSCA-CZ musí zahájit s ERCA proces revokace certifikátu.

4.1.4 Obnovení a prodloužení platnosti certifikátu

Obnovení (rekey) certifikátu znamená výměnu klíče a vydání nového certifikátu. Obnovení certifikátu může nastat v těchto případech:

- Pokud se doba použití klíče MSCA-CZ blíží ke konci (periodická operace)
- Jako důsledek procesu revokace certifikátu

Procesy obnovy certifikátu jsou totožné jako v případě iniciální žádosti. Obnovení certifikátu MSCA-CZ musí proběhnout minimálně 2 měsíce před vypršením doby použití privátního klíče.

Prodloužení platnosti certifikátu bez změny klíče (renewal) není dovoleno.

Modifikace obsahu certifikátu není dovolena.

4.1.5 Revokace certifikátů

MSCA-CZ certifikát může být revokován v těchto případech:

- Odmítnutí přijetí certifikátu, jako důsledku neúspěšného importu (viz 4.1.3).
- Kompromitace privátního klíče MSCA-CZ.

- Nedostupnost/ztráta privátního klíče MSCA-CZ.
- Ukončení činnosti MSCA-CZ.
- V případě, kdy MSA-CZ nebo MSCA-CZ nesplnily povinnosti plynoucí z nařízení [2] a CP ERCA [1].

Došlo-li ke kompromitaci klíče nebo podezření na kompromitaci, musí MSCA-CZ tento incident notifikovat na MSA-CZ a ERCA nejpozději do 8 hodin po zjištění této skutečnosti.

Způsob vyšetření incidentu je definován v bezpečnostní dokumentaci CAP, v jehož bezpečnostním perimetru je MSCA-CZ provozována.

ERCA bude vyhodnocovat žádosti o revokaci jen od těchto autoritativních subjektů:

- European Authority
- MSA
- MSCA

Perioda zpracování žádosti o revokaci je 5 pracovních dnů, poté musí být žádost vyhodnocena do 3 dnů.

Status certifikátů MSCA publikovaný na ERCA se aktualizuje první pracovní den každého týdne.

4.1.6 Ukončení činnosti MSA

Pokud se MSA-CZ rozhodne ukončit svou činnost, notifikuje ERCA. O dopadu ukončení činnosti na MSCA-CZ rozhodne MSA-CZ (revokace certifikátu nebo ukončení platnosti po expiraci).

4.2 Distribuce Master Key

4.2.1 Generování žádosti o klíč (KDR)

Podmínky pro získání Master key (hlavního klíče) jsou stejné jako pro získání certifikátu

- EU (Evropská autorita) vydá prohlášení o shodě pro příslušnou MSA
- MSA schválí CPS MSCA.

Způsob vytvoření žádosti o klíč a jeho formát specifikuje CP ERCA [1] v kap. 4.2.1

Generování žádosti o symetrický klíč musí probíhat ve fyzicky bezpečném prostředí pod duální kontrolou osob v důvěryhodných rolích.

MSCA-CZ v žádosti o klíč v položce CHA (Certificate Holder Authorization) uvede řetězec, který vznikne spojením Tachograph Application ID (‘FF 53 4D 52 44 54’) a typem klíče a verzí klíče. MSCA-CZ může žádat o tyto typy klíče:

- K_M-WC - typ klíče 27
- K_DSRC - typ klíče 09

MSCA-CZ pro každý klíč použije samostatnou žádost, pro každou žádost použije jiný efemérní klíč.

MSCA-CZ žádá o daný klíč pouze jednou, opakování žádosti o stejný typ vede k vyšetřování důvodu.

MSCA-CZ musí při generování žádosti spočítat hash celé žádosti (algoritmus odpovídá síle použitého klíče MSCA). Tato hash pak slouží ke vzdálené autorizaci žádosti při zpracování na ERCA. Tato hash musí být součástí protokolu o generování žádosti o klíč.

Žádost o distribuci klíče by měla být uložena na medium CD-R v single session mode (formát ISO 9660:1988).

MSCA-CZ by měla uložit na medium žádost ve třech formátech:

- ASCII (.txt file)
- Base64 (.pem file)
- Binary (.bin file)

MSCA-CZ vytiskne doprovodný papírový protokol o generování žádosti, který obsahuje položky specifikované v CPS ERCA.

Papírový protokol je součástí kurýrem předané žádosti na ERCA, kopie protokolu je předána i MSA-CZ, která autorizuje zpracování žádosti.

4.2.2 Zpracování žádosti o klíč (KDM)

Zpracování žádosti o klíč je plně popsáno v [1] v kap. 4.2.2

ERCA po ověření schopnosti zpracovat přijatou žádost autorizuje její původ. Autorizace spočívá v tom, že ERCA ověří telefonicky u kontaktní osoby MSA-CZ znalost hodnoty hash celé žádosti, která je na protokolu uvedena.

ERCA zapisuje certifikát na médium CD-R, formát ISO 9660:1988.

MSCA-CZ by měla být schopna vydaný klíč zpracovat ve všech poskytnutých formátech:

- ASCII (.txt file)
- Base64 (.pem file
- Binary (.bin file)

Součástí vydaného certifikátu je i papírový protokol o vydání certifikátu.

4.2.3 Akceptace klíče

Kurýr MSCA-CZ podepisuje převzetí KDM v prostorách ERCA.

Po přijetí KDM v MSCA-CZ je nutné ověřit jeho použitelnost:

- Čitelnost média.
- Správný formát certifikátu (viz [1] kap.7, tabulka 5).
- Ověřit shodu Message Recepient Authorization v KDM s hodnotou uvedenou v KDR.
- Ověřit, zda public point leží na křivce specifikované v KDR.

Pokud některá z těchto kontrol bude neúspěšná, musí MSCA-CZ oznámit tuto skutečnost na ERCA.

V případě úspěšného přijetí žádosti MSCA-CZ derivuje z KDM klíče K_ENC a K_MAC a tyto použije pro dešifrování a ověření integrity klíče. Operace dešifrování musí proběhnout v HSM, které splňuje požadavky uvedené v kap. 6.2.

Pokud dešifrování neproběhne úspěšně, musí MSCA-CZ tuto skutečnost oznámit ERCA.

Po úspěšném přijetí klíče musí MSCA-CZ odstranit z HSM efemérní privátní klíč a odvozené klíče K_ENC a K_MAC.

MSCA-CZ musí používat přijatý Master Key ve shodě s požadavky kap. 6.2

Pokud došlo k poškození nosiče s KDM, může MSCA-CZ po nahlášení tohoto incidentu požádat o zaslání nového nosiče s odkazem na původní žádost KDR. Detaily tohoto postupu jsou popsány v CPS ERCA.

4.2.4 Vydání nového symetrického klíče

V případě, že ERCA vydá novou verzi symetrického klíče, upozorní na to na svých webových stránkách. Součástí zveřejnění je i délka nového klíče.

MSCA-CZ žádá o tento klíč identických způsobem, v žádosti se odkazuje na novou verzi klíče, v žádosti použije kryptografii odpovídající délce nového klíče, tak jak je uvedeno v tabulce 2.

4.2.5 Oznámení o kompromitaci klíče

V případě, že MSCA-CZ zjistilo kompromitaci klíče nebo existuje podezření na kompromitaci, musí zástupce MSCA-CZ tuto skutečnost oznámit MSA-CZ a ERCA do 8 hodin po zjištění této skutečnosti. Součástí tohoto oznámení je poskytnutí okolností, za kterých k tomu došlo.

MSA-CZ musí zahájit vyšetření incidentu a výsledek šetření poskytnout ERCA.

Informaci o stavu klíče je možné zjistit na webových stánkách ERCA (https://dtc.jrc.ec.europa.eu/)

4.2.6 Ukončení vztahu

V případě, že MSCA-CZ ukončí svou roli klienta u ERCA, musí bezpečně zničit všechny kopie symetrických Master Key, které má v držení.

4.3 Základní principy a vlastnosti řešení pro TC.

4.3.1 Základní principy zpracování žádosti a vydání TC

Základní principy zpracování žádosti vychází ze schéma na obr.1.

1. Žádost o tachografovou kartupodává žadatel na specifické přepážce úřadovny ORP (municipality).
2. Úředník ORP ověří identitu žadatele proti primárním identifikačním dokladům (občanský průkaz nebo pas) a přebere žádost o vydání tachografové karty (pro každý typ karty specifický formulář, pro kartu řidiče se formulář vytiskne na základě sdělených údajů).
3. Úředník se autentizuje s využitím autentizačního certifikátu do systému ISDT a žádost zavede do tohoto systému. Součástí pořízení dat pro kartu je zajištění fotografie a podpisu držitele (jen pro karty řidiče). Fotografie je buď stažena z registru řidičů nebo je pořízena lokální kamerou (součást řešení ISDT). Podpis je sejmut na

grafickém Signpadu. Data jsou uložena do systému s respektováním principu neodmítnutelnosti zodpovědnosti za vložená data.

4. Systém ISDT ověřuje zadaná data vůči registrům:
    a. Ověření shody zadané identity žadatele vůči registru řidičů;
    b. Ověření, zda pro zadanou identitu žadatele již nebyla vydána v ČR požadovaná karta;
    c. Ověření, zda nebyla vydána karta v jiném státě EU (s podporou Tachonet)
5. Úředník na základě výsledků ověření schválí žádost ke zpracování.
6. Klientská stanice CIA zajistí stažení dávek schválených žádostí ke zpracování v CAP
7. Pracovník CIA předá nosič (flash disk) se staženými žádostmi pracovníkovi CAP. Předání je stvrzeno podpisem předávacího protokolu k dané dávce karet.
8. CAP vygeneruje data pro výrobu TC, vyžádá u MSCA-CZ vygenerování klíčových párů a příslušných certifikátů pro daný typ TC.
9. Na lince CAP se zajistí elektronická i grafická personalizace těla karty (laserové gravírování).
10. MSCA-CZ s podporou kryptografických služeb poskytovaných HSM umožní zápis požadovaných klíčů a dat do čipu karty, včetně podpory pro výpočet klíčů Global platform pro daný čip (chrání čip od výrobce k personalizátoru).
11. Po výrobě dané dávky karet se vyrobené karty včetně elektronické průvodky předají pracovníkům CIA (s podpisem Předávacího protokolu), kteří následně odešlou stavovou informaci o vyrobených kartách do systému ISDT. Předaná dávka vyrobených karet musí odpovídat předané dávce žádostí.
12. Pracovníci CIA zajistí setřídění karet dle ORP, zabalí je a zajistí fyzickou distribuci na tato místa.
13. Po doručení zásilky karet na dané ORP provede úředník potvrzení přijetí zásilky (v systému ISDT) a umožní tak jejich vydání držitelům (žadatelům).
14. Před vydáním karty držiteli je tento autentizován s využitím primárních identifikačních dokladů a podepíše protokol o převzetí, který obsahuje i poučení o způsobu nakládání s TC.

4.3.2 Vlastnosti řešení plynoucí z architektury

MSCA-CZ funguje přímo v prostředí CP, jak je patrno z obr.1. Tato skutečnost usnadňuje bezpečnou interakci obou zúčastněných stran a vedla k řešení těchto vlastností:

- Prostředí CAP je izolováno od on-line připojení do internetu, veškeré přenosy dat z/do vnějšího prostředí probíhají off-line.
- Klíčové páry určené pro certifikáty pro TC generuje přímo MSCA-CZ v lokálním HSM.
- Privátní část klíče TC je zašifrována symetrickým klíčem a uložena v databázi MSCA-CZ do doby než bude uložen do čipu TC (zabezpečuje utajení i integritu privátního klíče).
- Veřejná část klíče se použije pro generování certifikátu vydaného MSCA-CZ.
- Operaci generování certifikátů iniciuje CAP (PersoServices) na základě zpracování žádostí o karty daného typu.
- Interakce MSCA-CZ a CAP je na lokální síti, serverová strana (MSCA) vyžaduje aktivaci HSM.
- Požadavek na operaci z klientské strany (CAP) je možný jen pro autentizovaného uživatele.
- HSM poskytuje kryptografickou podporu pro personalizaci karet a zahrnuje:
    - Správu Global platform klíčů pro zabezpečení čipů od dodavatele karet.
    - Správu vlastního privátního klíče MSCA-CZ.
    - Správu symetrických klíčů od ERCA.
    - Správu symetrických klíčů pro zabezpečení privátních klíčů TC.

- Generování session key pro jednotlivé čipy na úrovni Global platform klíčů (ENC, MAC).
- Poskytnutí Symetrických klíčů ERCA pro potřeby zápisu do karty.

5 Vybavení, správa a provozní kontrola

5.1 Fyzické zabezpečení

Provoz MSCA-CZ a CAP musí být zajištěn v bezpečném prostředí v definovaném a chráněném perimetru s přístupem jen autorizovaným osobám.

Paměťová média, přístupové karty, musí být uloženy tak, aby bylo znemožněno jejich zneužití.

HSM musí být chráněno tak, aby nebyl možný neautorizovaný přístup.

MSCA-CZ musí mít definovány postupy pro obnovu po katastrofě.

MSCA-CZ musí mít definovány postupy pro likvidaci odpadů, aby se zabránilo neoprávněnému použití, přístupu nebo zpřístupnění důvěrných informací.

5.2 Procedurální zabezpečení

Procedurální opatření mají za cíl zvýšit bezpečnost provozování systému MSCA-CZ a CP.

K základním opatření patří:

- Rozdělení rolí pro kritické operace v systému.
- Autentizace osob při přihlášení k výkonu svých rolí.
- Utajovaná data musí být uložena s garancí důvěrnosti a integrity.
- Jejich přenos po nezabezpečené síti musí garantovat důvěrnost a integritu.
- Oba systémy musí zajistit účinnou správu uživatelů a řízení přístupu.
- Oba systémy musí zajistit, že přístup k informacím a funkčnostem aplikací je umožněn jen autorizovaným osobám a poskytuje nástroje pro rozdělení rolí.
- Osoby obsluhující oba systémy musí být identifikovány a autentizovány.
- Aktivity uživatelů obou systémů musí být logovány.
- Systém CAP musí mít ustaven systém řízení informační bezpečnosti (ISMS) založený na hodnocení rizik (zahrnuje i MSCA-CZ) obsažených funkčností.
- Implementace ISMS by měla odpovídat požadavkům ISO 27001.

5.3 Personální zabezpečení

Osoby pověřené správou MSCA-CZ a CAP musí poskytovat záruky v těchto vlastnostech:

- Dostatečná důvěryhodnost.
- Kvalifikační předpoklady pro výkon své funkce.

Osoby jmenované do rolí musí prodělávat pravidelné školení ve shodě s plánem v CPS.

Role, do kterých jsou osoby jmenovány, musí být identifikovány a definovány v CPS MSCA-CZ.

Žádná osoba nesmí být autorizována současně do více rolí (tam, kde rozdělení rolí představuje bezpečnostní požadavek).

5.4 Procedury auditu

Všechny bezpečnostně významné události MSCA-CZ a CAP musí být automaticky logovány a opatřeny časovým údajem. Zahrnují minimálně tyto události:

- Úspěšný i neúspěšný pokus o: vytvořit, modifikovat, zrušit nebo obnovit stavovou informaci o účtu uživatele systému nebo nastavit oprávnění k účtu.
- Úspěšný i neúspěšný pokus změnit autentizační metodu uživatele.
- Úspěšný i neúspěšný pokus přihlásit nebo odhlásit od účtu uživatele.
- Úspěšný i neúspěšný pokus změnit konfiguraci SW (software).
- Start a stop SW.
- Bootování a shut-down systému.
- Úspěšný i neúspěšný pokus o vydání certifikátu a symetrického klíče.
- Úspěšná i neúspěšná interakce s DB při manipulaci s daty pro certifikáty.
- Úspěšný i neúspěšný pokus pro připojení k HSM.
- Úspěšný i neúspěšný pokus pro autentizaci uživatele k HSM.
- Úspěšný i neúspěšný pokus pro generování nebo odstranění páru klíčů/symetrického klíče v HSM.
- Úspěšný i neúspěšný pokus pro export/import klíče z HSM.
- Úspěšný i neúspěšný pokus pro použití klíče v HSM.

Logový záznam musí obsahovat identitu uživatele.

Integrita systémových logů musí být chráněna a zabezpečena proti neautorizovanému prohlížení, modifikacím nebo odstranění.

Systémový log musí být backupován a uložen ve shodě s CPS.

5.5 Archivace záznamů

Přehled událostí, které mají být archivovány musí být popsán v interních procedurách MSCA-CA, CP.

Použitá metoda archivace musí garantovat integritu, autenticitu a utajení záznamů.

Způsob uložení by měl vylučovat ztrátu archivovaných údajů, doba archivace není stanovena (archivované údaje se nelikvidují).

Údaje uvedené v kap. 5.4 musí být periodicky vyhodnocovány. Nejdelší periodou vyhodnocení může být 1 rok.

5.6 Kompromitace a obnova po katastrofě

MSCA-CZ musí definovat bezpečnostní incidenty a procedury pro jejich ošetření v manuálu *Ošetření bezpečnostních incidentů (Security Incident handling manual)*, který je vydán pro administrátory a auditory systému.

MSCA-CZ musí mít vypracován *Plán kontinuity provozu (Business continuity plan)* pro udržení služeb systému v případě incidentů nebo nehod, které znemožňují normální využívání systému. MSCA-CZ by měla v tomto plánu i zohledňovat obměnu systému plynoucí z morálního/technologického zastarání řešení.

MSCA-CZ musí mít vypracován *Plán zálohy a obnovy (Back-up and Recovery plan)* pro obnovu relevantních dat v systému.

Tyto události jsou chápány jako katastrofy:

- Kompromitace nebo zcizení privátního klíče a/nebo symetrického Master key.
- Ztráta (zničení) privátního a/nebo symetrického Master key.
- Selhání/porucha HW (hardware) MSCA-CZ.

5.7 Ukončení provozu MSCA-CZ

V případě ukončení činnosti MSCA-CZ, MSA-CZ musí tuto skutečnost oznámit EA a ERCA a jmenovat jiný subjekt pro provozování MSCA-CZ.

Je povinností MSA-CZ zajistit, aby byl funkční vždy alespoň jeden subjekt v roli MSCA-CZ.

6 Technická bezpečnost

6.1 Klíčový pár a instalace symetrických klíčů

MSCA-CZ musí generovat privátní klíč ve shodě s požadavky CP ERCA [1], Appendix 11.

MSCA-CZ by měla mít testovací systém pro podporu testů interoperability. Pokud existuje, musí se jednat o oddělený systém s vlastní sadou testovacích klíčů. Testovací systém musí být schopen požádat o vydání testovacího certifikátu a požádat o testovací symetrické klíče a musí být schopna vytvořit podporu pro CAP.

6.2 Ochrana privátního a symetrického klíče

MSCA-CZ musí zajistit důvěrnost, integritu a dostupnost privátnímu i symetrickým klíčům, které spravuje.

Privátní klíč musí být generován a symetrické klíče spravovány v zařízení, které splňuje některé z níže uvedených požadavků:

- Je certifikováno na EAL4 nebo vyšší ve shodě s ISO/IEC 15408 s použitím vhodného Protection Profile.
- Splňuje požadavky identifikované ISO/IEC 19790 level 3.
- Splňuje požadavky identifikované FIPS PUB 140-2 level 3.
- Nabízí ekvivalentní úroveň bezpečnosti odpovídající národním nebo mezinárodním hodnotícím kritériím pro IT bezpečnost.

MSCA-CZ by měla použít pro uložení klíčů HSM. Operace s privátními klíči i symetrickými klíči musí vždy probíhat uvnitř HSM.

Operace s klíči mohou být prováděny jen ve fyzicky bezpečném prostředí, osobami v důvěryhodných rolích pod duální kontrolou a všechny operace musí být logovány.

Backupování, uložení a obnova klíčů může být provedena jen osobami v důvěryhodných rolích, pod duální kontrolou, ve fyzicky bezpečném prostředí.

Všechny kopie privátních a symetrických klíčů musí být předmětem stejné úrovně bezpečnostních opatření jako tyto klíče ve fázi užití.

Import a export privátního klíče je možné provádět jen pro potřeby zálohy a obnovení klíče.

Import a export symetrických klíčů je možné provádět jen pro potřeby zálohy a obnovení klíče, mimo to jen pro podporu zápisu klíče do TC v personalizačním procesu. Tento proces musí probíhat ve fyzicky bezpečném prostředí a řízen osobami v důvěryhodných rolích.

Pro jiné účely nesmí být klíče distribuovány.

Na konci periody použití privátního klíče MSCA-CZ musí tato zničit všechny existující kopie klíče tak, aby je nebylo možné obnovit. Totéž platí pro symetrické klíče na konci jejich životního cyklu (neplatí pro klíče uložené v TC, ty jsou používány až do vypršení platnosti karty).

Všechny privární i symetrické klíče musí být vyloučeny z použití, pokud existuje podezření na kompromitaci klíčů. v takovém případě MSCA-CZ musí zahájit prošetření, zda mohlo dojít ke kompromitaci.Je-li kompromitace potvrzena nebo nemůže být vyloučena, klíče musí být nevratně odstraněny, včetně jejich kopií. Pokud může být kompromitace vyloučena, klíče mohou být dále používány. Na odstranění klíčů v HSM musí být použity interní funkce HSM.

6.3 Další aspekty správy klíčových párů

Certifikáty MSCA-CZ a tedy i jejich veřejné klíče musí být uchovávány neomezenou dobu.

Doba použití privátního klíče MSCA-CZ nesmí překročit 2 roky, počátek této periody je shodný s počátkem platnosti certifikátu (effecive date).

6.4 Aktivační data

MSCA-CZ je povinna ve své CPS uvést počet osob v důvěryhodných funkcích, který je potřeba pro aktivaci systému pro generování, užití a odstranění privátního klíče nebo import a užití symetrického klíče.

Generování, import, užití nebo odstranění privátních klíčů MSCA-CZ nebo symetrických klíčů uložených v HSM je možné jen po autentizaci osob v důvěryhodných rolích pomocí schválených prostředků. Doba trvání autentizované session nemůže být neomezená.

Také použití MSCA-CZ musí vyžadovat autentizaci obsluhy.

6.5 Řízení počítačové bezpečnosti

MSCA-CZ musí specifikovat schválené procedury a opatření technické bezpečnosti pro správu počítačového systému. Procedury a opatření musí garantovat vždy dosažení požavané bezpečnosti.

6.6 Řízení bezpečnosti životního cyklu

MSCA-CZ provede analýzu bezpečnostních požadavků ve fázi návrhu řešení, aby jejich implementací zajistila požadovanou bezpečnost.

Musí být zajištěno oddělení předprodukčního a produkčního systému. Změnové procedury a procedury řízení bezpečnosti musí garantovat požadovanou úroveň bezpečnosti produkčního systému.

Změnové procedury musí být dokumentovány a použity pro release verzi, případně modifikaci provozovaného SW.

6.7 Síťová bezpečnost

MSCA-CZ musí být provozována na segmentu sítě bezpečně odděleného od internetu.

6.8 Časová razítka

Datum a časový údaj musí být součástí auditního záznamu. MSCA-CZ musí definovat způsob časové synchronizace.

7 Profily certifikátů, CRL

7.1 Profil certifikátu

Všechny certifikáty musí mít profil definovaný v CP ERCA [1] v Příloze 11 (viz tabulka 3. převzatá z CP ERCA [1]).

V případě MSCA-CZ budou použity tyto specifické atributy pro certifikáty vydané pro TC:

Vlastnosti iniciálního klíče:

- Protocol suite #1.
- Domain parametr NIST P-256 (secp256r1).
- Hodnota OID = 1.2.840.10045.3.1.7.

Hodnota CAR iniciálního klíče dle tabulky z kap. 3.1:

- Key serial number = 01 (současný klíč MSCA-CZ GEN1 má hodnotu 04).

Platnosti certifikátu TC

- Certificate effective date - od nulté sekundy dne počátku platnosti karty.
- Certificate expiration date - do nulté sekundy dne následujícího po dni konce platnosti karty.

Data Object	Field ID	Tag	Length (bytes)	ASN.1 data type
ECC (CV) Certificate	C	'7F 21'	var	
Certificate Body	B	'7F 4E'	var	
Certificate Profile Identifier	CPI	'5F 29'	'01'	INTEGER (0…255)
Certification Authority Reference	CAR	'42'	'08'	KeyIdentifier
Certificate Holder Authorisation	CHA	'5F 4C'	'07'	Certificate Holder Authorisation
Public Key	PK	'7F 49'	var	
Standardised Domain Parameters OID	DP	'06'	var	OBJECT IDENTIFIER
Public Point	PP	'86'	var	OCTET STRING
Certificate Holder Reference	CHR	'5F 20'	'08'	KeyIdentifier
Certificate Effective Date	CEfD	'5F 25'	'04'	TimeReal
Certificate Expiration Date	CExD	'5F 24'	'04'	TimeReal
ECC Certificate Signature	S	'5F 37'	var	OCTET STRING

Tabulka 3: Struktura CV certifikátu

7.2 CRL profil

MSCA-CZ neposkytuje žádnou možnost pro zneplatnění klientského certifikátu uloženého na TC.

CIA je zodpovědná za status TC, pokud došlo k jejímu zadržení/zneplatnění. Certifikát jako takový není možné zneplatnit.

CIA by měla zajistit od držitelů karet převzetí všech nefunkčních karet nebo původních karet, které již byly nahrazeny novou kartou. CIA současně vede informace o ztracených nebo zcizených kartách.

CIA je povinna poskytnout tuto stavovou informaci subjektům, které je ze zákonných důvodů vyžadují.

8 Audit shody a další hodnocení

8.1 Perioda a okolnosti hodnocení

Subjekty u nichž dochází ke styku s privátními a symetrickými klíči, musí podstoupit plný formální audit. Tento požadavek se týká MSCA-CZ a CP.

Národní audit musí stanovit, zda subjekt, který je předmětem auditu zachovává požadavky, které na něj klade tato politika.

První audit musí proběhnout do jednoho roku od počátku poskytování služeb. Pokud by byly nalezeny neshody, musí další audit proběhnout do 12 měsíců, v případě shody postačí další audit s periodou 24 měsíců.

Před započetím řádné funkce auditovaných subjektů provede MSA-CZ předprovozní ohodnocení subjektu s cílem vyhodnotit, zda je schopen zajistit provoz odpovídající požadavkům této CP.

8.2 Identita a kvalifikace hodnotitele

Audit musí být proveden nezávislým auditorem.

Osoba navržená pro provedení auditu musí být schválena MSA-CZ.

Jméno auditora musí být registrováno.

Auditor by měl splňovat tyto požadavky:

- Etické chování (spolehlivost, důvěryhodnost, konzistentní přístup).
- Spolehlivá prezentace výsledků auditu.
- Profesionální přístup.

Auditor musí mít dostatečné znalosti a nejlépe být akreditován pro tyto činnosti:

- Provádění bezpečnostních auditů IT.
- PKI systémy a kryptografické technologie.
- Provoz SW s podporou PKI.
- Znalost relavantních politik EK, ERCA.

8.3 Vztah hodnotitele k hodnocenému subjektu

Auditor musí být nezávislým ve vztahu k hodnocenému subjektu.

8.4 Oblasti pokryté hodnocením

Audit na národní úrovni musí pokrýt shodu s touto politikou a CPS MSCA-CZ.

Oblasti pokryté auditem se musí dotýkat implementace technických, procedurálních a personálních postupů popsaných ve výše uvedených dokumentech.

Auditor by se měl zaměřit zejména na tyto oblasti:

- Identifikace a autentizace.
- Provozní funkce.
- Fyzická, procedurální a personální bezpečnost.
- Technické kontrola bezpečnosti.

Součástí auditu subjektu je i vyhodnocení auditních logů pro posouzení bezpečnosti.

Nalezené nedostatky musí být odstraněny. Ohodnocení a nalezené nedostatky musí být zaznamenány.

8.5 Opatření přijatá jako výsledek nedostatků

V případě nalezení nedostatků musí být ihned zahájeny akce na jejich odstranění.

Po provedených nápravných opatření se musí provést následný audit do 12 měsíců.

8.6 Zveřejnění výsledků

Na národní úrovni musí auditor reportovat plný výsledek auditu posuzovanému subjektu a MSA-CZ.

MSA-CZ musí zaslat relevantní report (výtah) z auditní zprávy na ERCA. Tento report musí obsahovat počet nalezených závad a jejich podstatu.

ERCA poté publikuje datum přijetí reportu na svých webových stránkách. ERCA si může vyžádat plnou auditní zprávu od MSA-CZ.

9 Další obchodní a právní záležitosti

9.1 Poplatky

MSCA-CZ neúčtuje za své služby žádné poplatky, provoz MSCA-CZ se promítne do koncové ceny tachografové karty jejímu držiteli.

9.2 Finanční odpovědnost

MSA-CZ nepřiznává žádné finanční kompenzace škod nebo ztrát vzniklých porušením svých povinností.

9.3 Důvěrnost obchodních informací

K důvěrným informacím zpracovávaným na MSCA-CZ patří:

- Privátní klíče MSCA-CZ
- Importované symetrické klíče z ERCA
- Auditní záznamy
- Auditní zprávy

9.4 Zpracování osobních údajů

MSCA-CZ nezpracovává žádné osobní údaje.

CIA je zodpovědná za sběr a správu osobních údajů, které souvisí s vystavením žádosti o kartu.

CAP zpracovává osobní údaje z žádosti o tachografovou kartu, které použije v procesu personalizace při zápisu dat na tělo karty a do čipu.

Všechny subjekty, které přichází do styku s osobními údaji, s nimi musí nakládat ve shodě s požadavky General Data Protection Regulation – GDPR [4].

9.5 Práva k duševnímu vlastnictví

Ochrana duševního vlastnictví se řídí pravidly zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon).

Za jejich dodržování odpovídá bezpečnostní pracovník každého ze subjektů provozujících některou z komponent tachografového systému.

9.6 Požadavky a záruky

MSCA-CZ, CP, CIA musí poskytovat své služby ve shodě s požadavky této CP.

9.6.1 Požadavky na MSCA-CZ

Povinností MSCA-CZ je:

- Poskytovat své certifikační služby v souladu s touto CP.
- Vypracovat CPS, která odráží konkrétní implementaci řešení a je ve shodě s touto CP.
- Podstoupit nezávislý audit své činnosti, který je nutný pro zajištění kontinuity činností (požadavek ERCA) a na jejím základě zkvalitňovat svou činnost.
- Poskytnout informaci o stavu certifikátu pro TC subjektům, které to vyžadují ze zákonných důvodů.

9.6.2 Požadavky na CAP

Povinností CAP je:

- Garantovat použití tachografové karty, která splňuje požadavky [2] a má doložené požadované bezpečnostní certifikace.
- Zajistit funkční testy karty a testy interoperability.
- Zajistit bezpečné převzetí dat určených pro personalizací s garancí jejich autenticity integrity a utajení.
- V procesu personalizace karty vyrobit požadovaný typ karty, případně dodání PIN ke kartě.
- Bezpečně předat vyrobené karty pro jejich distribuci subjektu CIA.

9.6.3 Požadavky na CIA

Povinností CIA je:

- Zajistit důvěryhodným způsobem sběr žádostí o vydání tachografové karty.
- Ověřit náležitě identitu žádajícího subjektu a ověřit oprávněnost žádosti o kartu.
- Garantovat bezpečný přenos žádostí o tachografové karty do procesu personalizace.
- Zajistit distribuci tachografových karet z procesu personalizace na výdejní místa.
- Ověřit náležitě identitu subjektu při převzetí vyrobené karty.
- Bezpečně spravovat data držená v systému ISDT, včetně aktuálního stavu karet.
- Poskytnout tato data jen subjektům, kteří mají zákonný důvod je získat.

9.6.4 Odmítnutí odpovědnosti a záruky

MSCA-CZ nenese odpovědnost za škody vzniklé:

- Využitím certifikátu, který je v rozporu s touto CP.
- Vydáním certifikátu pro karty, jejíž držitelé nebyli náležitě ověřeni.
- V důsledku války, živelné katastrofy.

CIA nenese odpovědnost za škody vzniklé:

- Pořízením žádostí a vydáním karty držiteli, který zneužil identifikační doklad jiné osoby.
- V důsledku války, živelné katastrofy.

9.6.5 Omezení odpovědnosti

MSCA-CZ a CAP nenesou odpovědnost ve vztahu ke koncovým uživatelům, pouze ve vztahu k orgánu členského státu (MSA-CZ) a organizaci vydávající karty (CIA).

Veškerou odpovědnost vůči koncovým uživatelům nese orgán členského státu (MSA-CZ) a nebo organizace pro vydávání karet (CIA).

9.7 Pozměňovací návrhy

Tato CP je vypracována MSA-CZ tak, aby naplňovala požadavky CP ERCA [1] a přenášela je na subjekty v kompetenci MSA-CZ. Pokud by došlo ke změně CP ERCA [1], mohou se tyto změny odrazit i ve znění této CP.

MSCA-CZ může předkládat návrhy na úpravy této politiky. v případě schválení takové změny bude vydána nová CP s příslušnou změnou verze.

9.8 Postupy řešení sporů

Spory a neshody mezi subjekty provozující jednotlivé komponenty tachografového systému řeší MSA-CZ. Pro tuto potřebu bude ustavena komise ze zástupců stran, které jsou ve sporu s kompetentními pracovníky MSA-CZ nebo jimi jmenovanými osobami.

9.9 Rozhodné právo

Ustanovení CP MSA-CZ a jejich výklad se řídí právním řádem České republiky.

9.10 Různá ustanovení

CIA se svým systémem ISDT, který zajišťuje sběr žádostí o vydání tachografové karty a jejich distribuci držitelům, spadá svým charakterem do oblasti významných informačních systémů ve smyslu zákona č.181/2014 Sb. (Zákon o kybernetické bezpečnosti). Způsob provozování tomu musí odpovídat.

10 Příloha 1

Identifikační atributy certifikátů pro tachografový systém - přehled

Atribut certifikátu	root	link	MSCA	TC
CAR	ERCA	ERCA	ERCA	MSCA
- nationNumeric	‘FD’	‘FD’	‘FD’	‘0C’
- nationAlpha	“EC ”	“EC ”	“EC ”	“CZ ”
- keySerialNumber	‘01’	‘01’	‘01’	‘01’
- additionalInfo	‘FF FF’	‘FF FF’	‘FF FF’	‘FF FF’
- CaIdentifier	‘01’	‘01’	‘01’	‘01’
CHA				
- tachAppID	‘FF 53 4D 52 44 54’	‘FF 53 4D 52 44 54’	‘FF 53 4D 52 44 54’	’FF 53 4D 52 44 54’
- equipmentType	13	13	14	01- řidič 02- dílna 03- kontrolní 04- podnik 17- řidič Sign 18- dílna Sign
PubKey				secp256r1
CHR	= CAR ERCA Totožná hodnota KeySerialNumber	=CAR ERCA Liší se v KeySerialNumber	=CAR MSCA	
- Serial Number	-	-	-	Integer 4 byte
- Date	-	-	-	MMYY (BCD)
- Type	-	-	-	01- řidič

				02- dílna 03- kontrolní 04- podnik
- Manufacture code	-	-	-	´A6´
CEfD				Time 00:00:00 First day validity
CExD				Time 00:00:00 Next Day after Last day validity

Tabulka 4: Hodnoty základních atributů certifikátů v tachografovém systému

Poznámka 1:

Doba platnosti TC je pro jednotlivé typy karet stanovena takto:

- Karta řidiče 5 let
- Karta podniku 5 let
- Karta kontrolní 2 roky
- Karta dílny 1 rok

11 Seznam odkazů na dokumenty

[1] European Root Certificate Policy and Symmetric Key Infrastructure Policy v.1.0 June 2018

[2] Commission Implementing Regulation (EU) 2016/799 (Prováděcí nařízení č. 2016/799)

[3] Commission Implementing Regulation (EU) 2018/502 (Prováděcí nařízení č. 2018/502)

[4] Nařízení Evropského parlamentu a Rady (EU) 2016/679

2. 2. Potvrzení o schválení evropským certifikačním orgánem ERCA

Ref. Ares(2019)636352 - 04/02/2019

EUROPEAN COMMISSION
JOINT RESEARCH CENTRE

Directorate E – Space, Security & Migration
Cyber & Digital Citizens' Security Unit

Ispra, 04 February 2019

Ministry of Transport of the Czech Republic
Driver Agendas Department
nábřeží Ludvíka Svobody 1222/12
110 15 Praha 1
Czech Republic

To the attention of:
Mr. Stanislav Bezděka

Subject: Approval of the Czech Republic policy for the smart tachograph V1.0

Dear Mr. Stanislav Bezděka,

We confirm the receipt of the following document, registered as document Ares(2019)630944 - 04/02/2019:

NATIONAL AUTHORITY OF THE CZECH REPUBLIC
FOR THE DIGITAL TACHOGRAPH SYSTEM
MSA-CZ CERTIFICATE POLICY – Tachograph System
Version 1.0

hereafter referred as CZ-A Policy.

The document has received a review for conformity with the requirements of the "*Smart Tachograph European Root Certificate Policy and Symmetric Key Infrastructure Policy Version 1.0*".
We thank you for having considered the remark of the policy review team, and confirm that the CZ-A policy is hereby approved.

As consequence, ERCA is ready to provide services for the Smart Tachograph to the entities operating under the CZ-A Policy.

Yours sincerely,

Michel Chiaramello

Cc: JRC.E.3 Jean-Pierre Nordvik, Head of Unit
A. Herrera Alcantara, Project Leader

Joint Research Centre, Via E.Fermi, 2749, I-21027 Ispra (Varese) - Italy - Office: TP 361,
Telephone: direct line +39 0332 785781, email: jrc-erca@.ec.europa.eu, https://dtc.jrc.ec.europa.eu