PŘÍLOHA G

Resortní politika certifikačních orgánů pro systém Digitální tachograf v České republice

(“Národní certifikační politika”)

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.

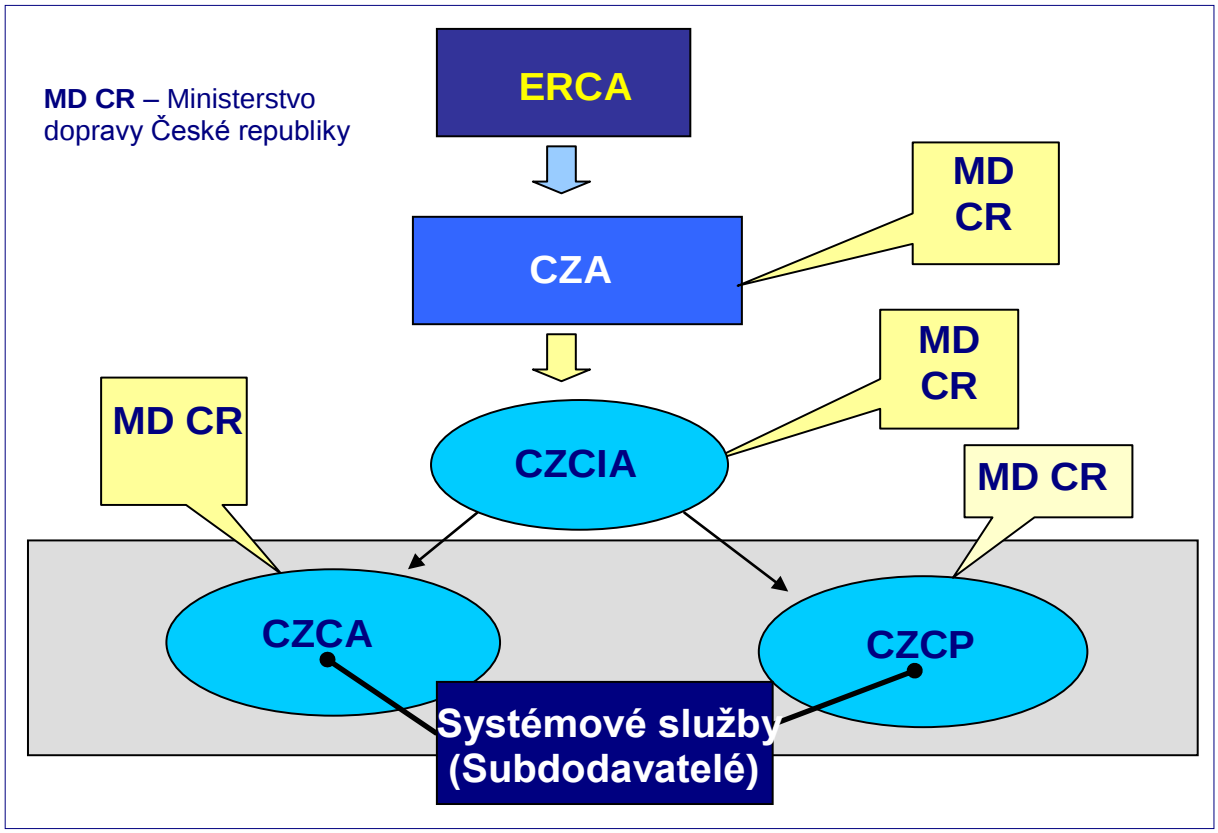


Diagram 1: Struktura odpovědných organizací

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]

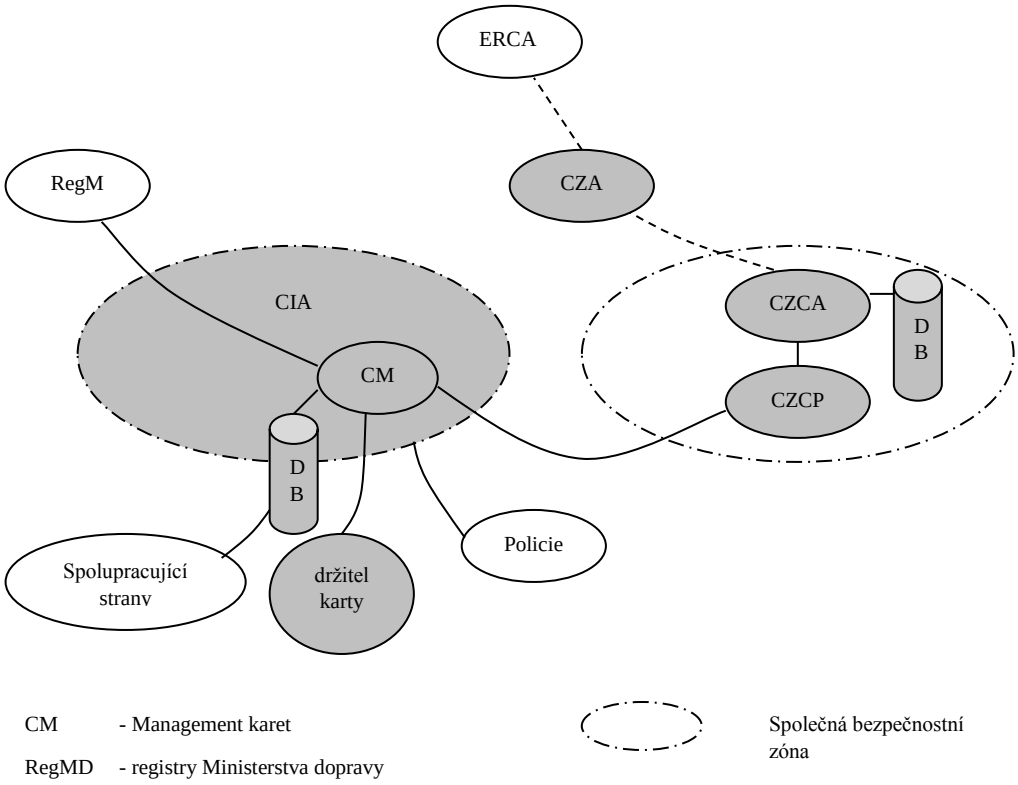
Rámec resortní politiky certifikačních orgánů České republiky je vyznačen šedou barvou v diagramu na obr. 1, který zachycuje strukturu tachografového systému v ČR a vazby v něm zúčastněných subjektů.

[r2.4]

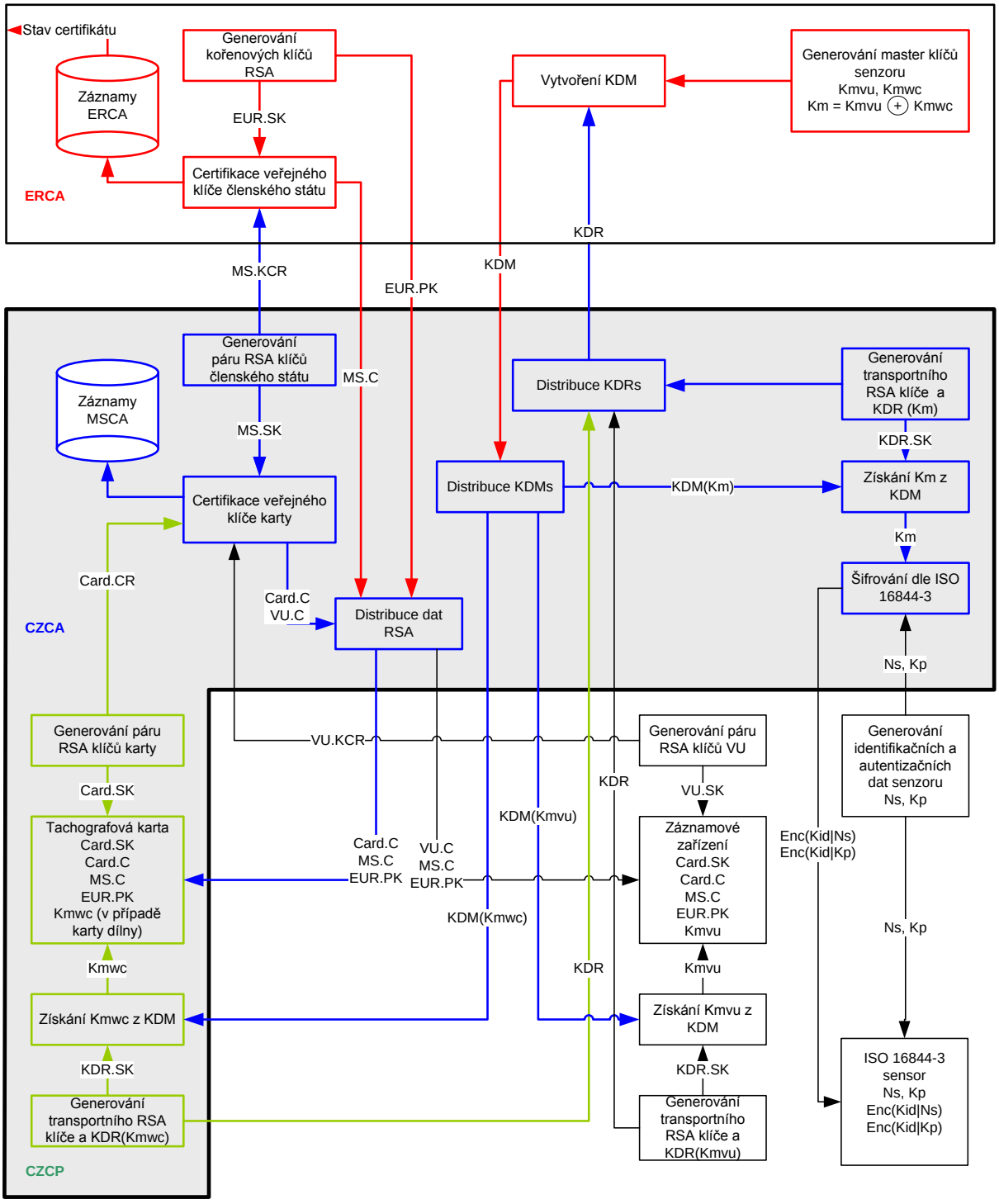
Procesní model systému vychází ze schématu uvedeného na obr. 2.

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

položka	odkaz v politice ERCA	Požadavky	odkaz v CZCA politice
			bezpečnostního konceptu [r9.7]
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.	§ 7.1 Všeobecné požadavky, záznam [r7.1]

položka	odkaz v politice ERCA	Požadavky	odkaz v CZCA politice
		Pro tyto účely MSA: - 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.	§ 7.2 Generace klíčů [r7.5]
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	§ 6 Klíčový management v rámci CZCA (odstavec 2)

položka	odkaz v politice ERCA	Požadavky	odkaz v CZCA politice
		kontrolou politiky MSA.	§ 6.2 Pár klíčů CZCA (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)	§ 6.3 Symetrické klíče pro workshop karty

položka	odkaz v politice ERCA	Požadavky	odkaz v CZCA politice
		personalizátorovi komponentů (v tomto případě výrobci dopravních prostředků), s využitím odpovídajících prostředků zabezpečení, výhradně pro účely vložení do dopravních prostředků.	a senzory vzdálenosti a pohybu (Km, Kmwc, 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;	§ 6.2 Pár klíčů CZCA (MS.SK, MS.PK) [r6.4]

položka	odkaz v politice ERCA	Požadavky	odkaz v CZCA politice
		c) vydávání seznamů rušených certifikátů, pokud je tato metoda používána pro poskytování certifikátu.	
28	§ 5.3.28	MSA podepíše certifikáty pro vybavení ve stejném zařízení, jaké bylo použito pro uložení privátních klíčů členského státu (viz 5.3.2).	§ 6 Klíčový management v rámci 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	§ 6.2 Pár klíčů CZCA (MS.SK, MS.PK)

položka	odkaz v politice ERCA	Požadavky	odkaz v CZCA politice
		odezvy ERCA	[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, kterých se to týká.	§ 9.1 IT Systém bezpečnostního managementu (ISMS) [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
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. Huberts (DG-TREN)

J.W.Bishop G07-TRVA
Tel: +39-0332-785225
Fax: +39-0332-789990
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

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