VOJENSKÝ ÚTVAR 8116
TRENČÍN
Č.: ZaSKIS-56/270

Trenčín, 25. jún 2018
Výtlačok číslo:
Počet listov: 35

Schvaľujem: Juraj ŠTEFANKA

Certifikačný poriadok CAMOSR

Spracovateľ: Odbor informačnej bezpečnosti / SkPKI a CA
Verzia: 7.0.
Dátum platnosti: 1.7.2018

Odbor informačnej bezpečnosti
Olbrachtova 5, 911 01 TRENČÍN
tel.: +421 960 406300
fax.: +421 960 406503
e-mail: pki@mil.sk
web: http://pki.mil.sk

Ochranné známky

Mená produktov uvádzané v tomto dokumente môžu byť registrované ochranné známky príslušných firiem.

História zmien

Verzia	Dátum	Opis revízie
0.1.	23.09.2005	prvý návrh – na pripomienkovanie
1.0.	17.10.2005	na schválenie
1.1.	14.11.2005	schválený
2.0.	26.07.2006	zrevidovaný
2.1.	17.10.2006	po jazykovej korektúre
2.2	14.09.2007	zrevidovaný
2.3	20.11.2007	zrevidovaný
2.4	15.03.2009	aktualizovaný, doplnený o LRA
3.0.	11.09.2009	Aktualizovaný, zmena VÚ, zmena možných hodnôt atribútu serial Number
3.1.	03.11.2009	Aktualizovaný, aktualizované vyhlášky NBÚ SR
4.0.	27.11.2009	Aktualizovaný, zmena systému CA
4.1.	03.05.2010	Doplnenie LRA ZV
5.0.	01.03.2011	Aktualizovaný, zmena systému CA, zmena OID
5.1.	19.08.2011	Zrevidovaný
5.2	06.07.2012	Zrevidovaný
5.3.	04.03.2013	Zrevidovaný
5.4.	25.03.2014	Zrevidovaný
5.5	22.06.2015	Zrevidovaný
6.0.	02.05.2017	Nahradenie zákona 215/2003 zákonom 272/2016, spojenie CP pre CA s CP pre TSA, zmena OID
7.0.	09.05.2018	Zrevidovaný, Nahradenie zákona 122/2013 zákonom 18/2018

Obsah

ZOZNAM OBRÁZKOV A TABULIEK

Obrázky

Tento dokument neobsahuje obrázky

Tabuľky

SKRATKY A POJMY

Skratky

CA	–	Certifikačná autorita (Certification Authority)
MOSR	–	Ministerstvo obrany Slovenskej republiky
CP	–	Certifikačný poriadok (Certificate Policy)
CPS	–	Pravidlá na výkon certifikačných činností (Certificate Practice Statement)
CRL	–	Zoznam zrušených certifikátov (Certificate Revocation List)
HSM	–	Bezpečné zariadenie na vyhotovenie elektronického podpisu; kryptografický modul, hardvérový bezpečnostný modul (Hardware Security Modul)
PMA	–	Autorita pre správu CP (Policy Management Authority)
NBÚ	–	Národný bezpečnostný úrad
KC	–	Kvalifikovaný certifikát pre elektronický podpis
KCPe	-	Kvalifikovaný certifikát pre elektronickú pečať
RA	–	Registračná autorita (Registration Authority)
LRA	–	Lokálna RA – je RA konajúca v mene CAMOSR, pôsobiaca v teritóriu RÚ ZaSKIS, v ktorého pôsobnosti je zriadená.
PKI	–	Infraštruktúra verejných kľúčov (Public Key Infrastructure)
PKCS	–	Kryptografický štandard verejného kľúča (Public Key Cryptography Standards).
CAMOSR	–	Certifikačná autorita, poskytovateľ dôveryhodných služieb Ministerstva obrany Slovenskej republiky
CAMOSR2	–	Prvý následník certifikačnej autority, poskytovateľa dôveryhodných služieb Ministerstva obrany Slovenskej republiky
CAMOSR3	–	Druhý následník certifikačnej autority, poskytovateľa dôveryhodných služieb Ministerstva obrany Slovenskej republiky
TSA	–	Time Stamp Authority (autorita časovej pečiatky)
QSCD	–	Kvalifikované zariadenie na vyhotovenie elektronického podpisu

Pojmy

Dôveryhodná služba - elektronická služba, ktorá sa spravidla poskytuje za odplatu a spočíva:

a) vo vyhotovovaní, overovaní a validácii elektronických podpisov, elektronických pečatí alebo elektronických časových pečiatok, elektronických doručovacích služieb pre registrované zásielky a certifikátov, ktoré s týmito službami súvisia, alebo

b) vo vyhotovovaní, overovaní a validácii certifikátov pre autentifikáciu webových síde, alebo

c) v uchovávaní elektronických podpisov, pečatí alebo certifikátov, ktoré s týmito službami súvisia.

Kvalifikovaný poskytovateľ dôveryhodných služieb - poskytovateľ dôveryhodných služieb, ktorý poskytuje kvalifikované dôveryhodné služby podľa zákona č. 272/2016 Z. z. o dôveryhodných službách, a ktorá má na poskytovanie týchto služieb kvalifikáciu Národného bezpečnostného úradu (ďalej len NBÚ).

Certifikát pre elektronický podpis – je elektronické osvedčenie, ktoré spája údaje na validáciu elektronického podpisu s fyzickou osobou a potvrdzuje aspoň jej meno alebo pseudonym.

Certifikát pre elektronickú pečať - je elektronické osvedčenie, ktoré spája údaje na validáciu elektronického podpisu s právnickou osobou a potvrdzuje jej názov.

Poskytovateľ dôveryhodných služieb – poskytovateľ dôveryhodných služieb, ktorý vykonáva dôveryhodné služby spojené s vydávaním, archivovaním, rušením platnosti certifikátov, overovaním ich platnosti a pod.

Držiteľ – entita identifikovaná v certifikáte ako držiteľ súkromného kľúča prislúchajúceho k verejnému kľúču obsiahnutému v certifikáte.

Elektronická pečať - sú údaje v elektronickej forme, ktoré sú pripojené alebo logicky pridružené k iným dajom v elektronickej forme s cieľom zabezpečiť pôvod a integritu týchto pridružených údajov.

Elektronický podpis – informácia pripojená alebo inak logicky spojená s elektronickým dokumentom, ktorá obsahuje údaj umožňujúci identifikáciu podpisovateľa.

Hashovacia funkcia (hash, message digest, fingerprint) – rýchlo spočítateľná funkcia, ktorá dostane na vstupe dokument ľubovoľnej dĺžky a zostrojí z neho pomerne krátku (napr. 160 bitov) charakteristiku, nazývanú hashovacia hodnota (tiež hašovacia hodnota, hash).

Kvalifikovaný certifikát pre elektronickú pečať - je certifikát pre elektronickú pečať:
a) ktorý vydal kvalifikovaný poskytovateľ dôveryhodných služieb pre elektronický podpis,
b) ktorý spĺňa požiadavky Prílohy číslo III Nariadenia (EÚ) 910/2014

Kvalifikovaný certifikát pre elektronický podpis - je certifikát elektronický podpis:
a) ktorý vydal kvalifikovaný poskytovateľ dôveryhodných služieb pre elektronický podpis,
b) ktorý spĺňa požiadavky Prílohy číslo 1 Nariadenia (EÚ) 910/2014.

Kvalifikovaný elektronický podpis – je zdokonalený elektronický podpis vyhotovený s použitím zariadenia na vyhotovenie kvalifikovaného elektronického podpisu a založený na kvalifikovanom certifikáte pre elektronické podpisy.

Mandátny certifikát - je kvalifikovaný certifikát vydaný fyzickej osobe, oprávnenej zo zákona alebo na základe zákona konať za inú osobu alebo orgán verejnej moci alebo v ich mene, alebo osobe, ktorá vykonáva činnosť podľa osobitného predpisu alebo vykonáva funkciu podľa osobitného predpisu a obsahuje údaje uvedené v §8 písm. a) až d) zákona č. 272/2016 Z. z.

Podpisová politika – je súbor pravidiel, ktoré vyjadrujú použiteľnosť certifikátu a/alebo triedy aplikácií so spoločnými bezpečnostnými požiadavkami.

Používateľ certifikátu – entita, ktorá koná na báze dôvery v daný certifikát a/alebo na základe elektronického podpisu overeného daným certifikátom. Synonymom pojmu používateľ certifikátu je pojem strana spoliehajúca sa na certifikát.

Pravidlá na výkon certifikačných činností – postupy, ktoré certifikačná autorita uplatňuje pri vydávaní certifikátov.

Kvalifikované zariadenie na vyhotovenie elektronického podpisu (QSCD) - zariadenie na vzhotovenie elektronického podpisu, ktoré spĺňa požiadavky stanovené v prílhe II Nariadenia eIDAS.

Subjekt – entita identifikovaná v certifikáte ako držiteľ súkromného kľúča prislúchajúceho k verejnému kľúču obsiahnutému v certifikáte.

Vlastná CA – časť infraštruktúry poskytovateľa dôveryhodných služieb (obsahujúca napr. HSM modul), ktorá spolu s poskytovateľom vydáva certifikáty.

Zdokonalený elektronický podpis – je elektronický podpis, ktorý spĺňa požiadavky stanovené v článku 26 Nariadenia (EÚ) 910/2014.

Žiadateľ o certifikát – entita, ktorá certifikačnej autorite predkladá žiadosť v mene jedného alebo viacerých subjektov.

X.509 - medzinárodný štandard, ktorý okrem iného definuje aj formát certifikátu verejného kľúča.

1 ÚVOD

Tento dokument obsahuje certifikačný poriadok (ďalej len CP), poskytovateľa dôveryhodných služieb Ministerstva obrany Slovenskej republiky (ďalej len CAMOSR) pri implementovaní infraštruktúry verejných kľúčov (ďalej len PKI) pozostávajúcej z produktov a služieb, ktoré poskytujú a spravujú kvalifikované certifikáty (ďalej len certifikáty) podľa štandardu X.509 pre kryptografiu verejných kľúčov v súlade so zákonom č. 272/2016 Z.z o dôveryhodných službách. Certifikáty identifikujú subjekt nachádzajúci sa v certifikáte a zväzujú tento subjekt s príslušným párom kľúčov.

1.1 Prehľad

Tento CP sa týka poskytovania dôveryhodných služieb vydávania, overovania a validácie:

- **kvalifikovaných certifikátov pre elektronický podpis, kde súkromný kľúč je uložený na QSCD**
- **kvalifikovaných certifikátov pre elektronickú pečať, kde súkromný kľúč je uložený na QSCD**
- **kvalifikovaných certifikátov pre službu OCSP, kde súkromný kľúč je uložený na QSCD**
- **kvalifikovaných certifikátov pre službu kvalifikovanej časovej pečiatky, kde súkromný kľúč je uložený na QSCD**
- **kvalifikovaných časových pečiatok**

v zmysle ustanovení Nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES (ďalej len „Nariadenie eIDAS“).

Kvalifikovaný certifikát vo všeobecnosti zväzuje verejný kľúč vlastnený fyzickou osobou, právnickou osobou, zariadením alebo webovým sídlom so súborom informácií, ktoré identifikujú entitu spojenú s používaním zodpovedajúceho súkromného kľúča.

CP je využívaný pri implementácii PKI, ktorá pozostáva z produktov a služieb, ktoré poskytujú a spravujú certifikáty podľa štandardu X.509.

CAMOSR v rámci tohto certifikačného poriadku sa rozumie, kvalifikovaný poskytovateľ dôveryhodných služieb vyhotovovania, overovania a validácie kvalifikovaných certifikátov pre elektronický podpis, elektronickú pečať, službu OCSP a službu kvalifikovanej časovej pečiatky Ministerstva obrany Slovenskej republiky, kde služby sú poskytované nasledovnými autoritami:

Názov	Sériové číslo certifikátu	Vydavateľ	DigitalID v SK dôveryhodnom zozname
CAMOSR2	00FE	KCA NBU SR 3	UeLpwDTkQOZWmso+SdQmT/zeimI=
TSAmil	100007dc	CAMOSR2	
TSAext	10000862	CAMOSR2	

1.2 Identifikácia

Názov:	**Certifikačný poriadok CAMOSR**
Skratka názvu:	**CP CAMOSR**
Verzia:	**Máj 2017**
Tomuto dokumentu je priradený identifikátor objektu (OID):	**1.3.158.30845572.1.7.3.01**

Pojmom KC resp. KC CAMOSR sa v tomto dokumente označuje kvalifikovaný certifikát vydaný kvalifikovanou certifikačnou autoritou, ktorá poskytuje kvalifikované dôveryhodné služby CAMOSR.

Popis použitého identifikátora objektu (OID):

1. - ISO assigned OIDs

1.3. - ISO Identified Organization

1.3.158. - Identifikačné číslo subjektu (IČO)

1.3.158.30845572. - Ministerstvo obrany Slovenskej republiky

1. 3.158.30845572.1. - JIDO

1. 3.158.30845572.1.7. - Dokument

1. 3.158.30845572.1.7.3. - PKI

1. 3.158.30845572.1.7.3.01 - CP CAMOSR

1.3 Komunita a použiteľnosť

1.3.a Autority

Autorita pre správu poriadkov

Autorita pre správu poriadkov (Policy Management Authority) (ďalej len PMA) je zložka CAMOSR ustanovená za účelom:

- dohľadu na vytváranie a aktualizáciu certifikačných poriadkov, vrátane vyhodnocovania zmien a plánov na implementovanie ľubovoľných prijatých zmien,
- revízie výsledkov auditov, aby sa určilo, či CAMOSR adekvátne dodržiava ustanovenia schváleného dokumentu CP,
- vydávania odporúčaní pre CAMOSR ohľadne nápravných akcií a iných vhodných opatrení,
- riadenia a usmerňovania činnosti vlastných certifikačných a registračných autorít, lokálnych poskytovateľov dôveryhodných služieb,
- vykonávania revízie CP poskytovateľa dôveryhodných služieb prostredníctvom analýzy CP, aby sa zaručilo, že prax CAMOSR vyhovuje príslušnému certifikačnému poriadku.

PMA predstavuje zastrešujúcu zložku, ktorá rozhoduje s konečnou platnosťou vo všetkých záležitostiach a aspektoch týkajúcich sa CAMOSR a jej činnosti.

Vlastná certifikačná autorita

Je entita autorizovaná PMA na vytváranie, podpisovanie a vydávanie kvalifikovaného certifikátu s verejným kľúčom.

Je uvádzaná vo vydaných KC ako vydavateľ a jej súkromné kľúče sú používané na podpisovanie týchto KC.

Má úplnú zodpovednosť za poskytovanie KC služieb špecifikovaných v bode 1.1.

Zaručuje, že všetky aspekty jej služieb, operácií a infraštruktúry zviazanej s certifikátmi vydanými podľa tejto politiky sa vykonávajú v súlade s požiadavkami a ustanoveniami tohto poriadku a jeho pravidiel na výkon kvalifikovaných certifikačných činností.

CAMOSR je súčasťou hierarchickej PKI, sama však nemá podriadené certifikačné autority, ale je podriadená koreňovej KCA NBÚ. Charakter tejto podriadenosti a spôsob jej implementácie určuje NBÚ.

Registračná autorita (RA)

Je entita, ktorá na základe rozhodnutia PMA prijíma žiadosti o vydanie certifikátu, kontroluje súlad údajov v žiadosti o vydanie certifikátu s údajmi v predloženom preukaze totožnosti žiadateľa o vydanie certifikátu, odosiela žiadosti o vydanie certifikátu certifikačnej autorite, odovzdáva certifikáty žiadateľom o vydanie certifikátu.

Lokálna registračná autorita (LRA) – je RA konajúca v mene CAMOSR, pôsobiaca v teritóriu RÚ KIS, v ktorého pôsobnosti je zriadená.

LRA musí vykonávať svoje aktivity v súlade so schváleným certifikačným poriadkom CAMOSR.

Pod pojmom registračná autorita (RA) sa pre účely tohto dokumentu rozumie ľubovoľná lokálna registračná autorita (LRA).

Autorita vydávajúca časové pečiatky

Je entita autorizovaná PMA na vytváranie časových pečiatok pomocou súkromného kľúča používaného výhradne na túto činnosť. V tele časovej pečiatky je identifikácia TSAmil, TSAext (ďalej len TSAMOSR) ako vydavateľa časovej pečiatky.

Na poskytovanie časovej pečiatky je používané zariadenie certifikované podľa štandardu FIPS 140-2 level 3.

1.3.b Koncové entity

Subjekty, žiadatelia a držitelia certifikátu CAMOSR

Subjekt je entita, ktorej meno sa objaví ako subjekt certifikátu (neplatí pre KC obsahujúce v CN PSEUDONYM) a ktorá sa zaviaže, že bude používať svoj kľúč a certifikát v súlade s týmto certifikačným poriadkom.

Subjekt sa prevzatím svojho certifikátu stáva držiteľom daného certifikátu. Držiteľom môže aj zariadenie alebo systém prevádzkovaný fyzickou alebo právnickou osobou alebo prevádzkovaný v mene fyzickej resp. právnickej osoby.

Podľa platnej legislatívy, subjektom kvalifikovaného certifikátu pre elektronický podpis môže byť fyzická osoba, subjektom kvalifikovaného certifikátu pre elektronickú pečať môže byť právnická osoba alebo orgán verejnej moci, za predpokladu, že splnia podmienky na registráciu.

Fyzická osoba môže na základe úradne overeného splnomocnenia, ktoré ju splnomocňuje zastupovať daný subjekt pri konaní na registračnej autorite, konať ako žiadateľ o kvalifikovanú dôveryhodnú službu (napr. vydanie certifikátu, zrušenie certifikátu), t.j. zastupovať na RA jednu alebo viacero osôb – subjektov certifikátu.

V prípade žiadosti o certifikát táto splnomocnená osoba uzatvára zmluvu s CAMOSR v mene subjektu, ktorému je certifikát priradený a ktorý sa stáva jeho vlastníkom, avšak entitou, ktorá je autentifikovaná súkromným kľúčom prislúchajúcim k danému certifikátu, je vždy osoba – subjekt certifikátu.

Podmienky, ktoré musí subjekt a žiadateľ o certifikát splniť, aby subjektu bol vydaný certifikát, stanovuje tento dokument.

Užívateľ časovej pečiatky

Užívateľom časovej pečiatky môže byť individuálna fyzická osoba ako koncový užívateľ, prípadne právnická osoba zastupujúca niekoľkých koncových užívateľov.

Ak je koncovým užívateľom časovej pečiatky individuálna fyzická osoba, je táto priamo zodpovedná za dodržiavanie všetkých stanovených povinností.

Ak je užívateľom právnická osoba zastupujúca niekoľkých koncových užívateľov, je táto zodpovedná za to že povinnosti dané organizácii sú koncovými užívateľmi dodržiavané a očakáva sa, že organizácia ich bude vhodným spôsobom o tejto skutočnosti informovať.

Strany spoliehajúce sa na certifikát

Stranou spoliehajúcou sa na certifikát je entita, ktorá tým, že používa cudzí certifikát na overenie kvalifikovaného elektronického podpisu, sa spolieha na platnosť väzby subjektu (t.j. držiteľa) certifikátu s verejným kľúčom nachádzajúcim sa v danom certifikátu. Strana spoliehajúca sa na certifikát môže použiť informáciu z certifikátu na určenie vhodnosti certifikátu na dané použitie.

Synonymom pojmu strana spoliehajúca sa na certifikát, je pojem používateľ certifikátu. Tento koná na báze dôvery v daný certifikát a/alebo na základe kvalifikovaného elektronického podipsu overeného daným certifikátom.

Typy certifikátu

CAMOSR vydáva KC pre kvalifikovaný elektronický podpis, KC pre kvalifikovanú elektronickú pečať, KC pre OCSP a KC pre kvalifikovanú TSA v súlade so zákonom č. 272/2016 Z.z. o dôveryhodných službách podľa štandardu X.509 v. 3. Platnosť certifikátu je maximálne tri roky.

Podmienkou na vydanie certifikátu je, aby pár kľúčov tvorený privátnym kľúčom a k nemu prislúchajúcim a vo vydávanom certifikátu nachádzajúcim sa verejným kľúčom bol bezpečným spôsobom vygenerovaný a uschovaný na bezpečnom zariadení (QSCD), ktoré NBÚ certifikoval ako bezpečný produkt na vyhotovovanie kvalifikovaných certifikátov pre kvalifikovaný elektronický podpis, kvalifikovanú elektronickú pečať, OCSP respondera či tvorbu časových pečiatok.

CAMOSR, uplatňujúca tento poriadok, nevydáva žiadne certifikáty certifikačných autorít, t.j. nemá podriadené CA.

CAMOSR, uplatňujúca tento poriadok, tiež nevydáva žiadne krížové certifikáty.

1.3.c Použiteľnosť certifikátu

Certifikáty sú určené na účely identifikácie držiteľa verejného kľúča, podpísanie požiadavky na platnosť certifikátu, podpísanie časovej pečate.

KC vydaný fyzickej osobe, kde súkromný kľúč sa nachádza v QSCD je vydávaný za účelom podpory kvalifikovaného elektronického podpisu v zmysle článku 3 bod 12 Nariadenia eIDAS.

KC vydaný právnickej osobe, kde súkromný kľúč sa nachádza v QSCD je vydávaný za účelom podpory kvalifikovanej elektronickej pečate v zmysle článku 3 bod 27 Nariadenia eIDAS.

KC vydaný pre OCSP respondera, kde súkromný kľúč sa nachádza v HSM je vydaný za účelom poskytovania služby overenia platnosti certifikátu.

KC vydaný pre TSA, kde súkromný kľúč sa nachádza v HSM a je vydaný za účelom poskytovania služby kvalifikovanej časovej pečiatky.

Certifikáty sú vydávané iba fyzickým a právnickým osobám organizačne patriacim do rezortu MOSR.

Použiteľnosť vydávaných certifikátov bude regulovaná a implementovaná prostredníctvom rozšírení certifikátu.

1.4 Správa politiky

Na účel tvorby politík je v rámci zriaďovateľa CAMOSR vytvorená autorita pre správu politík (PMA), ktorá plne zodpovedá za jej obsah. Ďalej zodpovedá za rozhodovanie o súlade postupov CAMOSR, ktoré sú uvedené v pravidlách na výkon certifikačných činností (CPS) s touto politikou.

1.4.a Postup schvaľovania CPS a externej politiky

Ešte pred začiatkom prevádzky musí mať CMA schválený svoj CP a CPS a musí spĺňať všetky jeho požiadavky. Obsah CP a CPS schvaľuje osoba menovaná do role PMA.

Po schválení zo strany PMA je príslušný dokument publikovaný v súlade s publikačnou a oznamovacou politikou.

PMA má informovať o svojich rozhodnutiach takým spôsobom, aby boli tieto informácie dobre prístupné stranám spoliehajúcim sa na certifikáty.

1.5 Kontaktné údaje

Zriaďovateľom a prevádzkovateľom CAMOSR je Ministerstvo obrany Slovenskej republiky zastúpené LRA.

1. Kontaktné údaje Certifikačnej autority MOSR

Adresa: **VÚ 8116 Trenčín**
Certifikačná autorita MOSR (CAMOSR)
Olbrachtova 5
911 01 Trenčín

2. Kontaktné údaje LRA Trenčín

Adresa: **VÚ 8116 Trenčín Regionálny úsek KIS ZÁPAD**
Lokálna registračná autorita MOSR (LRAMOSR)
Partizánska 3732
911 01 Trenčín

3. Kontaktné údaje LRA Bratislava

Adresa: **VÚ 8116 Regionálny úsek KIS JUH**
Lokálna registračná autorita MOSR (LRAMOSR)
Za kasárňou 5
Bratislava

4. Kontaktné údaje LRA Zvolen

Adresa: **VÚ 8116 Regionálny úsek KIS STRED**
Lokálna registračná autorita MOSR (LRAMOSR)
Borovianska cesta 1
960 01 Zvolen

5. Kontaktné údaje LRA Prešov

Adresa: **VÚ 8116 Regionálny úsek KIS VÝCHOD**
Lokálna registračná autorita MOSR (LRAMOSR)
Námestie Legionárov 4
080 01 Prešov

6. Telefón, fax, email a web

e-mail: **pki@mil.sk**
www: **http://pki.mil.sk**
Pracovný čas
telefón: **+421 (0)960 401 111 (Kontaktné centrum)**
fax: **+421 (0)960 407 470**
Mimopracovný čas
telefón: **+421 (0)960 406 400, 40 22 00 (DRKIS)**
fax: **+421 (0)960 406 420 (DRKIS)**

2 ZVEREJŇOVANIE INFORMÁCIÍ A ÚLOŽISKÁ

2.1 Zverejňovanie informácií o CA/RA

CAMOSR bude zverejňovať na Internete v on-line režime prostredníctvom svojho webu repozitár, ktorý je prístupný držiteľom certifikátu a stranám spoliehajúcim sa na certifikát a ktorý obsahuje najmä:

- certifikáty ktoré CAMOSR vydala – informácie o certifikátoch sa zverejňujú prostredníctvom služby na vyhľadávanie certifikátu (meno, e-mail),
- aktuálne CRL a všetky predchádzajúce CRL,
- vlastný certifikát CA MOSR (patriaci k jej podpisovému kľúču),
- vlastný certifikát TSAmil a TSAext (patriaci k podpisovým kľúčom TSAMOSR)
- používaný algoritmus hašovacej funkcie,
- presnosť času vo vyhotovovanej časovej pečiatke s ohľadom na UTC.

CAMOSR bude zverejňovať na Internete v on-line režime prostredníctvom svojho webu CP CAMOSR a ďalšie zákonom požadované dokumenty.

Verejne prístupné sú len aktuálne dokumenty. Dokumenty neaktuálne sú uložené v archíve a sprístupnené môžu byť len po dohode s poskytovateľom certifikačných služieb.

CAMOSR musí chrániť ľubovoľnú informáciu uloženú v repozitári, ktorá nie je určená na verejné rozšírenie.

CAMOSR musí vynaložiť maximálne úsilie na to, aby zaistil integritu, dôvernosť a dostupnosť spracovávaných dát v súvislosti s poskytovaním KC službami. Taktiež musí vykonať logické a bezpečnostné opatrenia, aby zabránil neautorizovanému prístupu osobám, ktoré by mohli akýmkoľvek spôsobom zmeniť, poškodiť, pridať resp. vymazať údaje uložené v repozitári.

CAMOSR poskytuje službu potvrdenia existencie a platnosti certifikátu prostredníctvom OCSP respondera, ktorého umiestnenie je uvedené v samotnom certifikáte.

2.2 Periodicita publikovania informácií

Ak sa certifikát publikuje, tak čo najskôr po jeho vytvorení, ako náhle je možné prevzatie certifikátu jeho držiteľom.

CRL sa publikuje, tak aby bolo vždy platné. Platnosť 24 hodín. Bližšie informácie v bode 4.4.e .

Všetky informácie, ktoré majú byť publikované v repozitári, sa publikujú podľa možnosti čo najskôr.

2.3 Úložíská

Repozitáre sú lokalizované tak, aby boli prístupné držiteľom certifikátu a stranám spoliehajúcim sa na certifikát a v súlade s celkovými bezpečnostnými požiadavkami.

Funkciu repozitára CAMOSR zastáva web CAMOSR, ktorého domovská stránka má URL **http://pki.mil.sk** a ktorý je prostredníctvom Internetu verejne prístupný držiteľom certifikátu, stranám spoliehajúcim sa na certifikát a verejnosti vôbec.

3 IDENTIFIKÁCIA A AUTENTIFIKÁCIA

3.1 Iniciálna registrácia

Prijímané žiadosti o certifikát a k nim patriace páry kľúčov sa musia generovať a uschovávať priamo na QSCD, HSM, žiadosti musia vyhovovať štandardu PKCS #10.

QSCD musí byť certifikovaný na NBÚ ako HW produkt na vyhotovovanie kvalifikovaného elektronického podpisu.

Spôsob správneho generovania kľúčov preukazuje žiadateľ o certifikát predloženými dokladmi a podpísanou žiadosťou o certifikát.

3.1.a Typy mien

CAMOSR bude vydávať certifikáty, ktoré obsahujú rozlišovacie mená podľa X.500 (X.500 **Distinguished Name,** ďalej ako rozlišovacie meno). Požiadavky na rozlišovacie mená sú uvedené nižšie. CAMOSR nebude priraďovať pre budúcich držiteľov certifikátov rozlišovacie mená s výnimkou položiek C a O. Subjekty si spravidla sami nevolia rozlišovacie meno, ktoré má byť v ich certifikáte.

Potreba zmysluplnosti mien

Pojem **„zmysluplnosť“** znamená, že forma mena má bežne používanú schému na určenie identity osoby, organizácie alebo jej časti a podobne.

Používané mená majú spoľahlivo identifikovať osoby, ktorým sú priradené. CAMOSR iba zaručuje, že existuje vzťah patričnosti (príslušnosti, členstva) medzi držiteľom certifikátu a ľubovoľnou organizáciou alebo organizačnou jednotkou, ktorá je identifikovaná ľubovoľnou časťou mena v certifikáte daného držiteľa.
Dôraz sa pritom kladie na položku commonName, ktorá má jednoznačne reprezentovať držiteľa certifikátu spôsobom, ktorý je pre človeka ľahko pochopiteľný. V prípade osoby to bude jej právoplatné meno a priezvisko v totožnej podobe, aká je uvedená v predložených dokladoch totožnosti, ale bez použitia diakritiky (mäkčene, dĺžne). V prípade právnickej osoby a orgánu verejnej moci tvorí položku commonName jej oficiálny názov alebo názov systému.

Namiesto mena a priezviska je možné použiť pseudonym, avšak v tomto prípade poslednou časťou hodnoty tejto položky bezpodmienečne musí byť reťazec PSEUDONYM, aby bolo jednoznačné a jasné, že namiesto mena a priezviska je uvedený pseudonym a tak, aby strana spoliehajúca sa na certifikát nemohla byť použitím pseudonymu uvedená do omylu. Neuvedenie reťazca PSEUDONYM za pseudonymom bude dôvodom na odmietnutie danej žiadosti o certifikát. Pseudonym nemusí byť zmysluplný, avšak LRA má právo zamietnuť žiadosť obsahujúcu pseudonym, ktorý je z etického, rasového, náboženského alebo iného dôvodu nevhodný. Pseudonym tiež nesmie obsahovať výraz, ktorým by mohli byť poškodené práva iného subjektu (napr. neoprávnené použitie registrovanej obchodnej značky ako

pseudonymu). Použitie pseudonymu v žiadnom prípade nezbavuje subjekt povinnosti preukázať svoju totožnosť na LRA.

Podľa ustanovení §8 ods.5 zákona č.272/2016 Z.z. mandátny certifikát, podľa odseku 1 písm. b). nemôže obsahovať pseudonym podľa Čl. 3 ods. 14 nariadenia (EÚ) 910/2014.

CAMOSR má právo odmietnuť vydať certifikát, ktorý by obsahoval údaje porušujúce princíp zmysluplnosti mien, zvláštny dôraz sa pritom kladie na údaj v položke commonName. Požiadavka na zmysluplnosť sa pritom vzťahuje na hodnotu ľubovoľnej položky v rozlišovacom mene. Porušenie tohto princípu môže byť príčinou odmietnutia vytvoriť certifikát z danej žiadosti o certifikát.

Pri zadávaní hodnôt do položiek žiadosti certifikátu by mal subjekt resp. žiadateľ o certifikát mať na zreteli, že na LRA bude musieť uspokojivým spôsobom preukázať oprávnenosť všetkých údajov, ktoré zadal do jednotlivých položiek žiadosti o certifikát.

Jednoznačnosť mien

CAMOSR zodpovedá za jednoznačnosť mien v rámci celej komunity subjektov certifikátov.

Podľa zákona č. 272/2016 Z.z je potrebné, ak sa v styku s orgánmi verejnej moci používa kvalifikovaný elektronický podpis, aby KC bol vydaný kvalifikovanou certifikačnou autoritou pričom musí obsahovať rodné číslo držiteľa certifikátu, číslo PASU resp. číslo OP.

Jednoznačnosť mien je plne zabezpečená uvedením rodného čísla držiteľa KC (uvedeného v pase alebo OP).

3.1.b Spôsob riešenia sporov týkajúcich sa mien

CAMOSR prostredníctvom RA musí zabezpečiť, že nepríde k žiadnej kolízii mien. V prípade potreby môže odmietnuť vydanie certifikátu z dôvodu kolízie mien. V prípade sporov týkajúcich sa kolízie mien a mien vo všeobecnosti sa bude postupovať podľa ustanovení bodu 9.4.

Ak bol spor spôsobený chybou CAMOSR, tá sa postará o čo najrýchlejšiu nápravu.

CAMOSR si vyhradzuje právo v prípade nevyhnutnosti zrušiť KC subjektu, ktorý spor spôsobil.

3.1.c Preukazovanie vlastníctva súkromného kľúča k verejnému kľúču v žiadosti o certifikát

Všetky žiadosti o KC musia byť vo formáte PKCS#10, čo znamená, že žiadosť o certifikát bude podpísaná privátnym kľúčom patriacim k verejnému kľúču nachádzajúcemu sa v danej žiadosti o certifikát.

Uplatňujúc rozšírenú normalizovanú certifikačnú politiku (NCP+) všetky páry kľúčov a im zodpovedajúce žiadosti o certifikát sa musia generovať priamo v kvalifikovanom

zariadení na vyhotovenie kvalifikovaného elektronického podpisu, ktoré je certifikované NBÚ a to pod dohľadom LRA.

Ak subjekt sám generuje kľúče priamo vo svojom tokene, potom automaticky vlastní vygenerovaný privátny kľúč uložený v QSCD v čase jeho generovania.

Žiadna zložka CAMOSR v nijakom prípade nearchivuje žiadne privátne kľúče patriace držiteľovi certifikátu, ktorý vzdala.

3.1.d Autentifikačné požiadavky pre organizácie a jej zástupcov

Autentizácia identity právnickej osoby

Žiadosť o kvalifikovaný certifikát pre elektronickú pečať podávaná v mene právnickej osoby musí obsahovať meno právnickej osoby, iný identifikačný údaj, ak taký existuje (spravidla je to napr. IČO), adresu a dôkaz existencie danej právnickej osoby (spravidla výpisom z obchodného registra).

Právnická osoba musí patriť do organizačnej štruktúry Ministerstva obrany SR alebo Generálneho štábu Ozbrojených síl SR.

LRA bude overovať tieto údaje a okrem autentickosti žiadajúcej osoby sa bude overovať, či daná osoba má právo rokovať v mene danej právnickej osoby vo veci príslušného certifikátu.

Fyzické osoby, ktoré konajú na LRA za danú právnickú osobu vo veci kvalifikovanej dôveryhodnej služby, musia preukázať svoju totožnosť.

V mene právnickej osoby môže na LRA konať len osoba, ktorá je jej štatutárom (alebo viac takýchto osôb súčasne, ak to vyžaduje predložený výpis z obchodného registra), prípadne sa právnická osoba môže nechať zastupovať fyzickou alebo inou právnickou osobou, ktorá na LRA predloží oprávnenie na konanie v mene zastupovanej osoby nasledovne:

- poverením, ak je daná fyzická osoba zamestnancom právnickej osoby, v mene ktorej koná a pracovno-právny vzťah má založený pracovnou zmluvou,

- úradne overenej plnej moci, ak daná fyzická osoba nemá pracovno-právny vzťah založený pracovnou zmluvou k právnickej osobe, v mene ktorej koná

Autentizácia identity fyzickej osoby

CAMOSR garantuje, že identita subjektu certifikátu a jeho verejný kľúč sú zodpovedajúco previazané.

CAMOSR špecifikuje vo svojom dokumente CPS procedúry na autentizáciu identity subjektu resp. žiadateľa o certifikát. CAMOSR zverejňuje požiadavky na identifikáciu fyzickej osoby prostredníctvom svojho webu a svojich LRA.

CAMOSR bude zaznamenávať tento proces pre každý certifikát. Dokumentácia o identifikácii musí minimálne obsahovať:

- identita osoby, ktorá vykonáva identifikáciu,
- vyhlásenie podpísané touto osobou, že overila identitu subjektu resp. žiadateľa o certifikát tak, ako to vyžaduje tento certifikačný poriadok,
- jednoznačné identifikačné čísla z predložených osobných dokladov dokladujúcich identitu autentizovanej osoby,
- dátum a čas vykonania identifikácie.

Súčasťou dokumentácie o identifikácii musí byť vyplnený formulár obsahujúci zozbierané identifikačné údaje, ktorý bude vlastnoručne podpísaný identifikovanou osobou v prítomnosti osoby vykonávajúcej autentizáciu identity.

Fyzickou osobou je osoba organizačne patriaca pod Ministerstvo obrany SR alebo Generálny štáb Ozbrojených síl SR.

Fyzická osoba musí preukázať svoju totožnosť osobným dokladom obsahujúcim fotografiu fyzickej osoby a jej rodné číslo:

- občiansky preukaz,
- cestovný pas.

Ak fyzická osoba zastupuje na LRA inú fyzickú osobu, musí sa navyše preukázať úradne overeným (notárom alebo matrikou) splnomocnením z textu ktorého je jednoznačne jasné, že zastupujúca fyzická osoba bola splnomocnená splnomocňujúcou fyzickou osobou konať v danej veci v jej mene.

Subjekt (fyzická alebo právnická osoba), ktorý zastupuje fyzickú osobu, sa vo veci fyzickej osoby, ktorú zastupuje, v žiadnom prípade nemôže nechať zastupovať iným subjektom.

Predkladané doklady

Všetky doklady, predkladané žiadateľmi o certifikát, musia byť buď originály, alebo úradne overené kópie originálov. Nesmie v nich byť žiaden údaj doplňovaný, pozmeňovaný, prečiarknutý a podobne. Doklady, na ktorých je vyznačená lehota ich platnosti, musia byť platné.

Ak má pracovník LRA pochybnosti o totožnosti potenciálneho zákazníka (napr. zjavný nesúlad medzi fotografiou v predloženom osobnom doklade a vzhľadom zákazníka, rozpornosť dvoch predložených dokladov a podobne), môže odmietnuť jeho registráciu.

Na žiadosť žiadateľa o certifikát alebo LRA sa prípadné sporné prípady pri preukazovaní totožnosti riešia postupom podľa ods. 9.4.

Kontrola údajov na predložených dokladoch

V prípade ľubovoľných odôvodnených pochybností o totožnosti žiadateľa o certifikát môže LRA jeho registráciu odmietnuť. Pracovník LRA kontroluje na predložených dokladoch najmä skutočnosti podľa týchto odsekov.

Osobné doklady fyzickej osoby

a) platnosť predloženého dokladu,
b) plnoletosť fyzickej osoby (t.j. vek 18 rokov),
c) či nie je zjavný nesúlad medzi fotografiou v osobnom doklade a vzhľadom majiteľa osobného dokladu,
d) zhodnosť predložených dokladov, t.j. či údaje na jednom doklade neodporujú údajom na inom doklade.

Výpisy z obchodného registra - len ak sa to bude týkať VOP, úradov a zariadení zriadených MOSR

a) či výpis nie je starší ako 3 mesiace,
b) či majú fyzické osoby (stačí jedna fyzická osoba, ak na výpise nie je uvedené inak), ktoré predložili daný výpis, právo konať (podpisovať) za danú právnickú osobu (t.j. či sú jej štatutárnymi zástupcami),
c) či je výpis úradne overený (notárom alebo matrikou), ak nejde o originál.

Plnomocenstvo

a) či je plnomocenstvo úradne overené (notárom alebo matrikou),
b) či sa údaje, uvedené v plnomocenstve, ktoré identifikujú zastupujúcu fyzickú resp. právnickú osobu, zhodujú s údajmi uvedenými na osobných dokladoch zastupujúcej fyzickej osoby resp. s údajmi uvedenými na výpise z obchodného registra zastupujúcej právnickej osoby,
c) rozsah plnomocenstva- t.j. či plnomocenstvo oprávňuje splnomocnenú fyzickú alebo právnickú osobu na požadovaný úkon na LRA v mene splnomocňujúcej fyzickej alebo právnickej osoby,
d) či plnomocenstvo nie je časovo obmedzené alebo ak obsahuje inú podmienku, či je táto splnená.

Prvotná registrácia pracovníka CAMOSR

Prvotná registrácia osoby, zastávajúcej niektorú úroveň (rolu) v rámci CAMOSR je opísaná v príslušných CPS.

3.2 Vydanie následného certifikátu

Vydanie následného certifikátu znamená zmenu páru kľúčov - musí sa vytvoriť nový certifikát, ktorý môže mať zhodné rozlišovacie meno ako starý certifikát, ale nový musí mať odlišný verejný kľúč (zodpovedajúci novému, odlišnému súkromnému kľúču), odlišné sériové číslo a môže mať zmenenú dĺžku platnosti.

Žiadateľ o následný certifikát sa musí podrobiť požiadavkám kladeným na prvotnú registráciu (hlavne autentizáciu jeho identity).

3.3 Vydanie následného certifikátu po zrušení certifikátu

Žiadateľ o následný certifikát po zrušení certifikátu sa v každom prípade musí podrobiť požiadavkám identifikácie kladeným na prvotnú registráciu.

3.4 Žiadosť o zrušenie certifikátu

Žiadosť o zrušenie certifikátu musí byť autentizovaná.

Žiadosť môže byť podaná osobne žiadateľom o zrušenie certifikátu na LRA. V inom prípade – napr. pri podozrení zo zneužitia karty sa overí totožnosť žiadateľa pri komunikácii s CAMOSR, alebo kontaktným centrom pomocou overovacieho kódu.

4 POŽIADAVKY NA ŽIVOTNÝ CYKLUS CERTIFIKÁTU

4.1 Žiadosť o vydanie certifikátu

Cieľom tejto politiky je identifikovať minimálne požiadavky a procedúry, ktoré sú nevyhnutné na podporu dôvery v certifikát. Cieľom je tiež minimalizovať špecifické implementačné požiadavky na CAMOSR, žiadateľov o certifikát, držiteľov certifikátu a strany spoliehajúce sa na certifikát.

Ak žiadateľ o certifikát požiada o certifikát, žiadateľ o certifikát a LRA musia vykonať tieto kroky:

- Overiť a zaznamenať identitu subjektu a aj žiadateľa o certifikát, ak to nie je tá istá osoba (podľa ods. 3.1).
- Subjekt musí mať v svojom bezpečnom zariadení pre zaručený elektronický podpis vygenerovaný a uložený pár kľúčov (verejný a privátny kľúč) pre každý požadovaný certifikát.
- Preukázať, že verejný kľúč tvorí pár kľúčov s privátnym kľúčom vlastneným žiadateľom o certifikát (podľa časti 3.1.c).
- Poskytnúť dostatočné podklady na overenie ľubovoľných identifikačných údajov, ktoré sa majú dostať do certifikátu.

Komunikácia medzi jednotlivými zložkami CAMOSR týkajúca sa žiadosti o certifikát a procesu vydania certifikátu má byť autentizovaná a chránená pred modifikáciou pomocou mechanizmov primeraných požiadavkám dát. Ľubovoľný elektronický prenos spoločne majúcich tajomstiev musí byť uskutočnený šifrovane. Tieto kroky možno vykonať v ľubovoľnom poradí, ktoré je vyhovujúce pre CAMOSR aj pre žiadateľov o certifikát a ktoré nie je v rozpore s bezpečnosťou.

Žiadosť CAMOSR o vlastný certifikát bude predložená NBÚ spôsobom požadovaným NBÚ na základe platnej legislatívy.

4.1.a Detailný postup na získanie certifikátu

Žiadateľ o certifikát, resp. subjekt – budúci držiteľ certifikátu, vykoná tieto kroky ako prípravu na návštevu na LRA:

a) oboznámi sa s týmto postupom, prípadne s princípmi a návodmi pre získanie certifikátu,
b) pripraví si hodnoty jednotlivých položiek žiadosti o certifikát tak, aby tieto hodnoty boli v súlade s týmto dokumentom
c) pripraví si zvolené doklady totožnosti resp. iné potrebné doklady, napr. výpis z obchodného registra (odporúčame overiť platnosť dokladov) podľa ustanovení časti 2.

Žiadateľ o certifikát, resp. subjekt – budúci držiteľ certifikátu, príde na LRA, pričom vezme so sebou a predloží**:**

- zvolené doklady totožnosti resp. iné potrebné doklady, napr. výpis z obchodného registra, plnomocenstvo atď. podľa ustanovení časti 2,

Postup pri registrácii žiadateľa o certifikát na LRA

a) Pracovník LRA overí totožnosť subjektu resp. žiadateľa o certifikát, ktorý ho zastupuje,
b) V prípade úspešného overenia totožnosti pracovník LRA vypíše pre každú overenú fyzickú osobu dvojmo formulár „Súhlas so spracovaním osobných údajov“, tento sám podpíše a dá ho podpísať žiadateľovi o certifikát resp. subjektu, ktorý ho zastupuje. Jeden vyplnený formulár zostáva na LRA, jeden dostane žiadateľ o certifikát.
c) Pracovník LRA overí, či je zariadenie v ktorom budú generované kľúče, certifikovaným QSCD.
d) Je potrebné monitorovať stav certifikácie QSCD až do ukončenia platnosti vydaného KC a musia sa prijať vhodné opatrenia v prípade, že dôjde k zmene tohto stavu.
e) Po overení totožnosti sa prostredníctvom aplikácie RA Client vygeneruje v QSCD žiadateľa o certifikát (jeho čipovej karte) nová žiadosť o certifikát vo formáte PKCS#10. Žiadosť o certifikát sa generuje priamo na LRA pod dohľadom pracovníka LRA
f) Pracovník LRA skontroluje, či sa údaje na vyplnenom formulári "Žiadosť o vydanie certifikátu" zhodujú s údajmi na žiadosti o certifikát v súbore a či sú vyplnené všetky povinné položky.
g) Všetky položky musia byť vyplnené bez diakritiky. Malé a veľké písmená sa rozlišujú.
h) Položky ST (stateOrProvinceName (názov kraja)), L (localityName („Mesto“)), OU (organizationUnitName ("Útvar vo firme")) a Email adresa sú nepovinné.
i) Ostatné položky žiadosti o certifikát **musia byť povinne vyplnené** takto:

Rozlišovacie meno používané v certifikáte pozostáva z týchto položiek s nižšie uvedeným významom:

Tabuľka č. 1: Položky rozlišovacieho mena KC

Názov položky	Skratka názvu položky	Popis položky	Príklad hodnoty položky	Typ a maximálna dĺžka položky
countryName (Štát)	C	Dvojznaková skratka štátu – dvojmiestny kód podľa ISO 3166 definujúci štátnu príslušnosť subjektu, údaj je povinný	SK	PrintableString 2 znaky
stateOrProvinceName (Názov kraja)	S	Názov kraja resp. provincie, údaj je nepovinný	Trenciansky	UTF8String 128 znakov
localityName (Mesto)	L	Názov lokality, údaj je nepovinný	Trencin	UTF8String 128 znakov
Organizational Unit (Organizačná zložka)	OU	Názov resp. číslo útvaru, údaj je nepovinný	VU 8116	UTF8String 64 znakov

organizationName (Organizácia)	O	Názov organizácie	Ministry of Defence	UTF8String 64 znakov
commonName (Meno a priezvisko)	CN	Meno a priezvisko alebo pseudonym, za ktorým je uvedený reťazec PSEUDONYM, údaj je povinný	Jan Strelec alebo napr. Aligator PSEUDONYM	UTF8String 64 znakov
givenName (meno(á))	G	Všetky mená použité v položke CN okrem priezviska, údaj je povinný, ak v položke CN nebol uvedený pseudonym ale v prípade použitia pseudonymu údaj nesmie byť uvedený	Jan	UTF8String 64 znakov
Surname Priezvisko)	SN	Priezvisko z položky CN, údaj je povinný, ak v položke CN nebol uvedený pseudonym ale v prípade použitia pseudonymu údaj nesmie byť uvedený	Strelec	UTF8String 64 znakov
serialNumber (Sériové číslo)	SERIAL NUMBER	Okaz na identitu fyzickej osoby – rodné číslo. Povinný údaj	PNOSK 9959199999, PASSK P3000180, IDCSK SK989783	UTF8String

Položka countryName musí obsahovať SK a položka organizationName Ministry of Defence.

Okrem položiek uvedených v tejto tabuľke môže žiadosť o certifikát obsahovať ako nepovinný údaj email adresu resp. hodnotu jednoznačného identifikátora (ďalej „JIDO“), tieto položky však nebudú súčasťou rozlišovacieho mena, ale zadaná email adresa a/ alebo JIDO budú uvedené v certifikáte v jeho rozšírení SubjectAltName. Hodnota email adresy sa zadáva obvyklým spôsobom (t.j. ako rfc822Name).

Tabuľka č. 2: Položky rozlišovacieho mena KC pre elektronickú pečať

Názov položky	**Skratka názvu položky**	**Popis položky**	**Príklad hodnoty položky**	**Typ a maximálna dĺžka položky**
countryName (Štát)	C	Dvojznaková skratka štátu – dvojmiestny kód podľa ISO 3166 definujúci štátnu príslušnosť subjektu, údaj je povinný	SK	PrintableString 2 znaky
stateOrProvinceName (Názov kraja)	S	Názov kraja resp. provincie, údaj je nepovinný	Trenciansky	UTF8String 128 znakov
localityName (Mesto)	L	Názov lokality, údaj je nepovinný	Trencin	UTF8String 128 znakov
Organizational Unit (Organizačná zložka)	OU	Názov resp. číslo útvaru, údaj je nepovinný	VU 8116	UTF8String 64 znakov
organizationName (Organizácia)	O	Názov orgánu verejnej moci alebo právnickej osoby	Ministry of Defence	UTF8String 64 znakov
commonName (Meno a priezvisko)	CN	Meno, názov systému pre koho je certifikát vydaný	LTA	UTF8String 64 znakov

serialNumber (Sériové číslo)	SERIAL NUMBER	Odkaz na identifikačný údaj orgánu verejnej moci alebo právnickej osoby Povinný údaj	"VATSK-12311321" alebo "SZ:SK-123123".	UTF8String

j) Prostredníctvom informačného systému CAMOSR sa automatizovane overí, či pre verejný kľúč nachádzajúci sa v predloženej žiadosti o certifikát už nebol v minulosti vydaný certifikát. Ak bol, LRA žiadosť o certifikát odmietne prijať z bezpečnostných dôvodov, lebo už raz certifikovaný verejný kľúč nemôže byť použitý v inom certifikáte.

k) Žiadateľ o certifikát a pracovník LRA, v súlade s údajmi zadanými pri generovaní žiadosti o certifikát, podpíšu dva vytlačené exempláre vyplneného formulára "Žiadosť o vydanie certifikátu". Jedna kópia zostáva žiadateľovi o certifikát.

l) Ak žiadateľ o certifikát predloží aj iné doklady (okrem osobných dokladov fyzických osôb, napr. výpis z obchodného registra alebo iný doklad o právnickej osobe, plnomocenstvo v prípade zastupovania iného subjektu), pracovník LRA prevezme a uschová kópie (nemusia byť overené) všetkých predložených dokladov, porovná ich s originálmi a na každú kópiu napíše text „**Potvrdzujem zhodu s originálom**“ a doplní dátum a svoj podpis.

Poznámka. Výpis z obchodného registra získaný z Internetu nie je postačujúci, pretože má len informatívny charakter a nie je použiteľný na právne úkony.

m) Ak je v položke CN (commonName (Meno a priezvisko)) uvedený aj jeden alebo viacero titulov alebo vojenská hodnosť (napr. Ing., Mgr., CSc. a iné), použitie titulu alebo vojenskej hodnosti v žiadosti o certifikát sa akceptuje, ak sa použité tituly alebo hodnosti nachádzajú v aspoň jednom z predložených osobných dokladov patriacich subjektu certifikátu. V opačnom prípade je žiadateľ o certifikát povinný LRA preukázať oprávnenosť použitia každého uvedeného titulu alebo hodnosti predložením originálu alebo úradne overenej kópie diplomu alebo iného dokumentu, ktorý potvrdzuje, že daná osoba má právo používať daný titul alebo hodnosť.

n) LRA odmietne žiadosť o certifikát, ktorá obsahuje uvedenie titulu alebo hodnosti, ktorý žiadateľ nevie dokázať uvedeným spôsobom.

Z dôvodu archivácie všetky doklady v tlačenej forme bude LRA odosielať na CA stanoveným spôsobom v stanovených periódach.

4.1.b Doručenie verejného kľúča

Verejné kľúče (obsiahnuté v žiadostiach o certifikát) sa musia generovať v bezpečnom zariadení, aby sa garantovala väzba overenej identity žiadateľa o certifikát k verejnému kľúču, ktorý sa certifikuje.

4.2 Vydanie certifikátu

CAMOSR nevytvorí certifikát, kým sa k spokojnosti CAMOSR nedokončia všetky verifikácie a prípadné zmeny, ak sú potrebné.

CAMOSR nezodpovedá za prípadné dodatočné náklady žiadateľa o certifikát, ktoré vzniknú v priebehu registrácie, napr. kvôli potrebe opakovanej návštevy LRA napr. v dôsledku neúplných alebo chýbajúcich dokladov alebo iných nedostatkov.

Hoci žiadateľ o certifikát pripravuje väčšinu dátových položiek certifikátu, na CAMOSR zostáva zodpovednosť overiť, že informácie sú správne a precízne.

Za preverenie údajov žiadateľa o certifikát zodpovedá LRA.

CA má právo nevytvoriť certifikát, hoci žiadateľ o certifikát úspešne prešiel procesom registrácie na LRA, ak sa dodatočne zistí závažná skutočnosť, ktorá bráni vydaniu certifikátu (napr. chyba vo formáte žiadosti o certifikát).

4.2.a Doručenie privátneho kľúča držiteľovi certifikátu

Privátny kľúč sa generuje priamo v bezpečnom certifikovanom zariadení za prítomnosti žiadateľa o certifikát a pracovníka LRA, preto nie je potrebné privátny kľúč doručiť.

Privátny kľúč, ktorý je generovaný v HSM nie je potrebné doručiť.

4.2.b Doručenie certifikátu verejného kľúča CAMOSR používateľom

CAMOSR a strany spoliehajúce sa na certifikát musia konať v súčinnosti, aby sa zaručilo autentizované a integrálne doručenie certifikátu CAMOSR.

Prijateľné metódy na doručenie certifikátu CAMOSR a jeho autentizovanie sú:

- osobné prevzatie certifikátu CAMOSR na LRA
- LRA na požiadanie poskytne strane spoliehajúcej sa na certifikát alebo inému ľubovoľnému záujemcovi fingerprint certifikátu CAMOSR a to konkrétne telefonicky, zabezpečeným mailom alebo osobne pri návšteve záujemcu na LRA. Konkrétna voľba spôsobu poskytnutia fingerprintu závisí od dohody so záujemcom. Fingerprint (alebo hash) posielaný spolu s certifikátom nie je prijateľný ako autentizačný mechanizmus.

4.3 Prevzatie certifikátu

CAMOSR bude vydávať certifikát v režime on-line, tzn. žiadateľ o certifikát spravidla bude môcť prevziať vydaný certifikát v rámci návštevy LRA, pri ktorej sa uskutočnil proces registrácie a prijatia žiadosti o certifikát.

Pri preberaní certifikátu žiadateľ podpíše „Potvrdenie o vydaní certifikátu“ a jeho odovzdaní žiadateľovi o certifikát, ktoré tvorí prílohu zmluvy o vydaní a používaní certifikátu. Toto potvrdenie sa vyhotoví v dvoch exemplároch – jeden pre žiadateľa o certifikát a jeden pre LRA.

Subjekt sa pri preberaní svojho certifikátu môže dať zastupovať na LRA inou fyzickou alebo právnickou osobou za rovnakých podmienok ako pri podávaní žiadosti o certifikát

Vytvorený certifikát bude uložený a odovzdaný na tokene subjektu, žiadateľovi o certifikát spolu s vlastným certifikátom CAMOSR. Certifikačný poriadok CAMOSR je v elektronickej forme dostupný na webovej stránke CAMOSR http://pki.mil.sk

4.4 Zrušenie certifikátu

4.4.a Okolnosti zrušenia certifikátu

Certifikát sa má zrušiť, keď sa väzba medzi subjektom a jeho verejným kľúčom stanoveným v certifikáte už nepovažuje za platnú. CAMOSR je zo zákona povinná zrušiť certifikát, ktorý spravuje, v týchto prípadoch:

- zistí, že pri vydaní certifikátu neboli splnené požiadavky zákona,
- zistí, že certifikát bol vydaný na základe nepravdivých údajov,
- o zrušenie certifikátu požiada držiteľ certifikátu alebo osoba, ktorej údaje sú uvedené v certifikáte, alebo iná osoba na to určená v zmluve s držiteľom certifikátu,
- zrušenie certifikátu nariadi CAMOSR svojím rozhodnutím súd,
- dozvie sa, že subjekt certifikátu zomrel, alebo resp. ak právnická osoba zanikla
- zistí, že došlo ku kompromitácii privátneho kľúča patriaceho k danému certifikátu, napr. ak privátny kľúč patriaci k verejnému kľúču uvedenému v certifikáte pozná iná osoba, než subjekt uvedený v certifikáte,
- dozvie sa, že údaje uvedené v certifikáte sa stali neaktuálnymi,
- subjekt porušil svoje povinnosti stanovené certifikačným poriadkom a/alebo zmluvou medzi ním a CA ,
- dozvie sa, že subjekt sa stal nesvojprávnym na základe rozhodnutia súdu,
- došlo ku kompromitácii privátneho kľúča CAMOSR,
- držiteľ porušil svoje povinnosti stanovené v CP a/alebo zmluvou medi ním a CAMOSR
- vlastník certifikátu si nesplnil povinnosť požiadať o zrušenie certifikátu po skončení pracovného pomeru v rezorte MOSR.

Vždy, keď sa CAMOSR dozvie o niektorej z uvedených okolností, daný certifikát sa zruší a dá sa na zoznam zrušených certifikátov (CRL) resp. informácia o jeho zrušení musí byť dostupná prostredníctvom služby OCSP.

Zrušené certifikáty nesmú byť za žiadnych okolností obnovené.

4.4.b Kto môže o zrušenie certifikátu požiadať

Subjekt - držiteľ certifikátu (alebo ním poverená fyzická alebo právnická osoba) môže hocikedy požiadať spôsobom stanoveným v tomto dokumente o zrušenie svojho vlastného certifikátu a to aj bez udania dôvodu v žiadosti o zrušenie certifikátu.

O zrušenie certifikátu môže tiež požiadať:

- CAMOSR (daný pracovník je povinný písomne zdokumentovať túto skutočnosť vrátane dôvodu svojho konania),
- súd prostredníctvom svojho rozsudku alebo predbežného opatrenia (k dokumentom o zrušení certifikátu musí CAMOSR priložiť kópiu príslušného súdneho rozhodnutia),
- subjekt (fyzická alebo právnická osoba) na základe dedičského konania (k dokumentom o zrušení certifikátu musí CAMOSR priložiť kópiu dokladov, z ktorých vyplýva právo daného subjektu žiadať o zrušenie certifikátu),
- súdom poverená osoba, napr. poručník subjektu certifikátu, ktorý sa má zrušiť (k dokumentom o zrušení certifikátu musí CAMOSR priložiť kópiu príslušného súdneho rozhodnutia),
- pracovník rezortu v prípade, že osoba ktorej bol certifikát vydaný už nie je pracovníkom rezortu.

4.4.c Postup na vystavenie a spracovanie žiadosti o zrušenie certifikátu

Žiadosť o zrušenie certifikátu podáva oprávnená osoba na LRA prostredníctvom dvoch rovnopisov vyplneného formulára „Žiadosť o zrušenie certifikátu“, ktorý je k dispozícii na webe CAMOSR alebo na LRA – jeden kus zostáva na LRA, jeden kus pracovník LRA potvrdí s uvedením aktuálneho dátumu a času (s uvedením hodín, minút a sekúnd) a vráti žiadateľovi o zrušenie.

LRA poskytne v prípade potreby žiadateľovi o zrušenie pomoc pri zistení čísla (Serial Number) predmetného certifikátu, aby bolo možné jednoznačne identifikovať certifikát, ktorý sa má zrušiť.

Osoba, požadujúca zrušenie certifikátu, sa buď musí na LRA podrobiť rovnakému procesu autentizácie, aký je požadovaný pri prvotnej registrácii žiadateľa o certifikát, alebo sa musí preukázať dohodnutým heslom na zrušenie daného certifikátu, ktoré je uvedené na formulári Potvrdenie o vydaní certifikátu a jeho odovzdaní žiadateľovi o certifikát.

Autentizácia požiadavky na zrušenie certifikátu je dôležitá, aby sa predišlo svojvoľnému zrušeniu certifikátu neautorizovanou stranou.

Ak sa držiteľ certifikátu nechá na LRA zastupovať vo veci zrušenia certifikátu, zastupujúci subjekt sa musí preukázať overeným plnomocenstvom (notárom alebo matrikou), z textu ktorého je jednoznačne jasná vôľa držiteľa certifikátu zrušiť svoj certifikát. Zastupujúci subjekt je povinný nechať na LRA doklad potvrdzujúci jeho plnomocenstvo alebo jeho kópiu (nemusí byť overená). Pracovník LRA prevezme a uschová tento doklad, v prípade neoverenej kópie túto porovná s originálom a napíše na ňu text „Potvrdzujem zhodu s originálom“ a doplní dátum a svoj podpis.

LRA posúdi oprávnenosť žiadosti o zrušenie certifikátu, v prípade, že je jasné, že žiadateľ o zrušenie certifikátu nie je oprávnenou osobou, LRA môže danú žiadosť o zrušenie odmietnuť.

LRA tiež odmietne žiadosť, ak žiadateľ o zrušenie certifikátu nesplní podmienky autentizácie svojej identity.

Pracovník LRA preverí na aktuálnom CRL platnosť certifikátu ktorý sa má zrušiť. V prípade certifikátu, ktorý už nie je platný, žiadosť o jeho zrušenie odmietne ako bezpredmetnú – nie je možné zrušiť certifikát, ktorého platnosť už vypršala alebo ktorý už bol zrušený.

Držiteľ platného certifikátu môže požiadať o zrušenie svojho certifikátu tiež tak, že pošle na kontaktnú emailovú adresu CAMOSR uvedenú v časti 1.5 obyčajný mail (t.j. mail nemusí obsahovať el. dokument podpísaný (zaručeným) elektronickým podpisom), ktorý obsahuje správu s jednoznačne vyjadrenou vôľou zrušiť certifikát, konkrétne vetu "Žiadam týmto o zrušenie svojho certifikátu číslo nnn." a dohodnuté heslo, ktoré je uvedené na formulári Potvrdenie o vydaní certifikátu a jeho odovzdaní žiadateľovi o certifikát.

Žiadosť o zrušenie certifikátu je možné podať aj telefonicky, písomne alebo faxom. Žiadateľ o zrušenie certifikátu sa pri tom autentizuje pomocou hesla dohodnutého na zrušenie certifikátu ktoré je uvedené na formulári Potvrdenie o vydaní certifikátu a jeho odovzdaní žiadateľovi o certifikát.

Ak k zrušeniu certifikátu nedôjde z vôle držiteľa certifikátu, po vydaní nového CRL bude LRA bezodkladne informovať (mailom alebo písomne) držiteľa certifikátu o zrušení jeho certifikátu, pričom uvedie, kto a kedy o zrušenie daného certifikátu požiadal. Táto povinnosť je povinnosťou tej konkrétnej LRA, ktorá danú žiadosť o zrušenie certifikátu prijala. Ak nebola žiadosť o zrušenie certifikátu prijatá na LRA ale priamo na CAMOSR (napr. v prípade žiadosti o zrušenie certifikátu na kontaktnú email adresu uvedenú v časti 1.5), táto povinnosť patrí osobe, ktorá žiadosť o zrušenie certifikátu vložila do aplikácie RAclient.

Následne výtlačok č . 1 Žiadosti o zrušení certifikátu spolu s Oznámením o zrušení certifikátu je odoslaná na adresu trvalého pobytu žiadateľa uvedenej v Zmluve o vydaní kvalifikovaného certifikátu . Výtlačok č. 2 je uložený na príslušnej LRA ktorá certifikát vydala.

4.4.d Interval na zrušenie certifikátu na základe požiadavky

Na prijatie žiadosti o zrušenie certifikátu, ktorú LRA považuje za oprávnenú (t.j. ktorá vyhovuje príslušným ustanoveniam tohto dokumentu), LRA **bezodkladne reaguje** tak,

že danú žiadosť o zrušenie certifikátu vloží do aplikácie LRA resp. informačného systému CAMOSR, aby sa mohlo vykonať zrušenie certifikátu, tzn. aby sa certifikát dostal na najbližšie CRL.

CAMOSR rozhodne o oprávnenosti požiadavky o zrušenie certifikátu najneskôr do 24 hodín od momentu jej prijatia na LRA.

CAMOSR zruší certifikát na základe oprávnenej požiadavky o zrušenie certifikátu a to do doby 60 minút od potvrdenia jej oprávnenosti.

Čas použitý pri poskytovaní služby zrušenia certifikátu by mal byť synchronizovaný s UTC (koordinovaným svetovým časom) minimálne krát za deň.

4.4.e Určenie periodicity publikovania zoznamu zrušených certifikátov

Informácia o zrušených certifikátoch by mala byť dostupná 24 hodín denne, 7 dní v týždni. CAMOSR zabezpečuje v primeranej miere danú službu voči výpadkom. V prípade výpadkov z dôvodov, ktoré sú mimo kontrolu CAMOSR musí byť zabezpečená obnova služby v čo najkratšom čase.

CRL sa vydáva s periódou maximálne 24 hodín a to aj vtedy, ak od vydania posledného CRL nedošlo k zrušeniu žiadneho certifikátu ani k žiadnej zmene v stave jednotlivých certifikátov.

CAMOSR archivuje všetky CRL, ktoré vydala.

4.4.f Požiadavky používateľov certifikátov na sledovanie zoznamu zrušených certifikátov (CRL) a dostupnosti služby OCSP

Použitie zrušeného certifikátu môže spôsobiť škodu alebo mať fatálne následky pre isté aplikácie. Ak dočasne nie je možné získať informácie o zrušených certifikátoch, potom strana spoliehajúca sa na certifikát musí buď odmietnuť použitie certifikátu, alebo urobiť kvalifikované rozhodnutie, ktorým akceptuje riziko, zodpovednosť a dôsledky použitia certifikátu, ktorého autenticita nemôže byť zaručená podľa štandardov tohto CP.

V čase medzi podaním oprávnenej žiadosti o zrušenie certifikátu a zverejnením zrušeného certifikátu na CRL nesie držiteľ certifikátu všetku zodpovednosť za prípadné škody spôsobené zneužitím jeho certifikátu. Po zverejnení certifikátu v CRL nesie všetku zodpovednosť za prípadné škody spôsobené použitím zrušeného certifikátu strana, ktorá sa na daný zrušený certifikát spoľahla.

Tretie strany, ktoré majú záujem využívať službu OCSP musia zaslať požiadavku na príslušný OCSP responder, ktorého URI je publikovaná v certifikáte, ktorého platnosť požadujú overiť. Zaslaná žiadosť musí byť v súlade s požiadavkami RFC 6960.

4.4.g Overenie aktuálneho stavu certifikátu

Overenie aktuálneho stavu certifikátu sa robí primárne prostredníctvom aktuálneho CRL publikovaného CAMOSR, resp. zaslaním požiadavky na OCSP responder.

CAMOSR zverejňuje aktuálny zoznam zrušených KC a všetky predchádzajúce zoznamy zrušených KC na svojej internetovej stránke (webe). www.pki.mil.sk. Požiadavky na OCSP sú obslúžené webom ocsp.mil.sk. Obe adresy sú uvedené v telách certifikátov vydávaných CAMOSR.

CAMOSR zabezpečuje ochranu autenticity a integrity ňou publikovaných zoznamov zrušených certifikátov.

4.4.h Požiadavky na on-line overenie platnosti certifikátu

Spoliehajúce sa strany sú povinné potvrdiť platnosť certifikátu pomocou CRL resp. OCSP pred tým ako sa spoľahnú na tento certifikát.

4.4.i Iné použiteľné spôsoby oznamovania informácií o zrušení

CAMOSR na požiadanie cez email, telefón alebo fax zašle aktuálne CRL prostredníctvom mailu na dohodnutú email adresu podľa možnosti čo najskôr.

4.4.j Suspendovanie certifikátu

Pod termínom „suspendovanie certifikátu“ sa myslí dočasné pozastavenie jeho platnosti. CAMOSR túto službu neposkytuje.

4.4.k Obnova certifikátu

CAMOSR nesmie vydať certifikát na verejný kľúč, na ktorý už bol ním v minulosti certifikát vydaný.

4.5 Vytváranie časovej pečiatky

4.5.a Časová pečiatka

CAMOSR zabezpečuje, že časová pečiatka je vydaná bezpečne, a že obsahuje správny čas.

Predovšetkým:

a) časová pečiatka obsahuje identifikátor politiky časovej pečiatky,
b) časová pečiatka má jedinečné identifikačné číslo,
c) hodnota času, ktorá sa dáva do vyhotovovanej časovej pečiatky, je odvodená z hodnoty reálneho času poskytovaného prostredníctvom UTC (ako spoľahlivého časového zdroja),
d) čas, ktorý sa dáva do vyhotovovanej časovej pečiatky, je synchronizovaný s hodnotou UTC v rámci presnosti definovanej v tejto politike,
e) ak je zistená odchýlka hodín TSA prekračujúca touto politikou deklarovanú presnosť, TSA časovú pečiatku nevydá,

f) časová pečiatka obsahuje hodnotu hašovacej funkcie, ktorú poskytol žiadateľ, aplikovanú na údaje, ku ktorým sa má vyhotoviť časová pečiatka,
g) časová pečiatka sa podpisuje kľúčom TSA, ktorý je používaný len na tento účel,
h) certifikát časovej pečiatky obsahuje:
    - identifikáciu Slovenskej republiky ako krajiny, v ktorej pôsobí TSA CAMOSR,
    - identifikáciu TSAMOSR.

4.5.b Vyhotovenie a overenie časovej pečiatky

Žiadateľ zašle (prostredníctvom dohodnutého rozhrania) TSA, ako vydavateľovi časovej pečiatky, žiadosť o vyhotovenie časovej pečiatky. Žiadosť obsahuje digitálny odtlačok dokumentu, na ktorý sa má vyhotoviť časová pečiatka, vytvorený pomocou schválenej hašovacej funkcie.

Ak je žiadosť v schválenom formáte a nie sú prekážky na vyhotovenie časovej pečiatky zo strany TSA, táto pomocou bezpečného zariadenia na vyhotovovanie časovej pečiatky a zdroja času vyhotoví časovú pečiatku na predložený digitálny odtlačok dokumentu a pošle ju žiadateľovi v režime on-line.

Ak žiadosť o vyhotovenie časovej pečiatky nemá schválený formát alebo ak v TSA vznikli prekážky vyhotovenia časovej pečiatky (napr. sa zistila odchýlka času mimo deklarovanej presnosti), TSA časovú pečiatku na predložený digitálny odtlačok dokumentu nevyhotoví.

Overenie platnosti časovej pečiatky vykonáva spoliehajúca sa strana na základe danej časovej pečiatky a dokumentu, na ktorý bola daná časová pečiatka vyhotovená, a politiky časovej pečiatky, ktorá sa na danú časovú pečiatku vzťahuje.

Časová pečiatka je platná, ak:
- kvalifikovaný elektronický podpis časovej pečiatky je platný,
- časová pečiatka je v súlade s použitou politikou časových pečiatok.

CAMOSR ako poskytovateľ služby kvalifikovanej časovej pečiatky sa zaručuje, že TSA v jej podriadenosti vydávajúca kvalifikované časové pečiatky nebude zároveň vydávať nekvalifikované časové pečiatky.

4.5.c Synchronizácia času s UTC

CAMOSR zabezpečuje, že čas, ktorý používa, je synchronizovaný s UTC s deklarovanou presnosťou 500 milisekúnd, a to predovšetkým týmito opatreniami:

- kalibrácia hodín TSA sa vykonáva tak, že očakávaná odchýlka času nie je mimo deklarovanej presnosti,
- hodiny zariadenia TSA sú chránené proti hrozbám, ktoré by mohli viesť k nezistiteľným zásahom do hodín, ktoré by mohli mať za následok ich odchýlku od kalibrácie,

- TSA zabezpečuje, že v prípade, ak sa čas, ktorý by bol uvedený v časovej pečiatke, odchýli od synchronizácie s UTC, táto skutočnosť sa zistí a časová pečiatka nebude vydaná,
- TSA zabezpečí, aby bola vykonaná synchronizácia hodín v prípade, ak bude notifikovaná oprávneným orgánom o výskyte opravnej sekundy.

4.6 Verejný kľúč

CAMOSR garantuje integritu a autenticitu verejného kľúča svojich kvalifikovaných autorít splnením nasledujúcich podmienok:

- verejné kľúče by mali byť dostupné dôverujúcim stranám prostredníctvom certifikátov kvalifikovaných autorít
- certifikáty verejných kľúčov by mali byť vydané kvalifikovaným poskytovateľom dôveryhodných služieb
- autority CAMOSR nesmú vydávať KC/časové pečiatky pred zavedením verejného kľúča do svojho HSM

CAMOSR je povinná pri obdŕžaní certifikátu pre svoju certifikačnú autoritu overiť správnosť jeho podpisu (vrátane overenia certifikačnej cesty).

4.7 Audit bezpečnosti

Aby sa vytvorilo optimálne prostredie na výkon auditu, sú implementované mechanizmy zabezpečujúce nepretržité (v režime on-line) kontrolné zaznamenávanie (logovanie) činnosti technických a programových komponentov, ktorými je realizovaná CA resp. RA, čo umožňuje sledovať, dodatočne preskúmať činnosť komponentu a v prípade potreby určiť zodpovednosť konkrétnej osoby za vykonané činnosti.

V rámci CAMOSR sa uskutočňuje priebežná kontrola funkčnosti a bezpečnosti použitých komponentov a opatrení. Vykonáva sa pravidelná analýza kontrolných záznamov (logov) vytváraných jednotlivými technickými a programovými komponentmi s osobitným dôrazom na zistenie anomálnych udalostí, stavov, chýb funkčnosti a nepovolených aktivít, kontroluje sa dodržiavanie platných bezpečnostných opatrení pracovníkmi CAMOSR a tiež v prípade potreby sa budú navrhovať vhodné nápravné opatrenia.

Softvér implementujúci CAMOSR zaznamenáva udalosti týkajúce sa aplikácií vykonávajúcich certifikačné služby. Tieto záznamy budú pokiaľ možno elektronicky podpísané, budú fyzicky chránené a bude zabezpečená ich nedostupnosť zo siete mimo infraštruktúry CAMOSR.

Zaznamenávajú sa všetky udalosti v rámci pracoviska CAMOSR. Záznamy môžu byť buď v elektronickej alebo v písomnej forme a môžu byť vytvárané buď automatizovane, alebo manuálne.

Bude sa uplatňovať kontrola prístupu k záznamom - prezeranie a spracovanie záznamov sa umožní jednotlivým pracovníkom CAMOSR v rozsahu týkajúcom sa nimi vykonávaných činností, v celom rozsahu PMA a osobám vykonávajúcim audit.

4.8 Archivácia záznamov

Archivácia záznamov sa vykonáva vhodným spôsobom v pravidelných intervaloch, aby sa zabezpečilo dlhodobé uloženie záznamov podľa požiadaviek Nariadenia eIDAS a zákona č. 272/2016 Z.z.

Záznamy sa pravidelne archivujú a uchovávajú na bezpečnom mieste s porovnateľnou úrovňou bezpečnosti ako pracovisko CAMOSR. Záznamy slúžiace na audit sa budú uchovávať minimálne 10 rokov.

Prezeranie archivovaných záznamov sa umožní v celom rozsahu PMA a osobám vykonávajúcim audit.

Modifikovanie alebo odstraňovanie archivovaných informácií nie je prípustné.

Je zabezpečená utajenosť a integrita archivovaných záznamov a médií.

4.9 Zmena kľúčov

Celý proces musí prebehnúť bez negatívneho vplyvu na úroveň zabezpečenia.

Dĺžka platnosti certifikátu by mala zodpovedať zvolenému algoritmu a dĺžke kľúča vhodného pre konkrétny účel.

K zmene kľúčov CAMOSR môže dôjsť z dvoch príčin:

- Blíži sa čas skončenia platnosti aktuálne používaných kľúčov CAMOSR. Toto je normálny stav – 2 roky pred uplynutím platnosti doteraz používaného páru kľúčov CAMOSR sa na webe CAMOSR zverejní oznam o blížiacej sa zmene kľúčov CAMOSR. Po tom, čo sa vygeneruje nový kľúčový pár a NBÚ vydá nový vlastný certifikát CAMOSR, sa zverejní nový vlastný certifikát CAMOSR. Každý ďalší vydaný (nový) vlastný certifikát a CRL bude podpísaný novým súkromným kľúčom CAMOSR.
- Je nutné vymeniť aktuálne používané kľúče CAMOSR z dôvodu ich kompromitácie. Toto je výnimočný, havarijný stav – CAMOSR bezodkladne oznámi NBÚ, všetkým držiteľom vydaných certifikátov a verejnosti (NBÚ písomne, okrem toho prostredníctvom svojho webu, elektronickou poštou), že došlo ku kompromitácii kľúčov CAMOSR. Bezodkladne tiež zruší svoj vlastný certifikát CAMOSR ako aj všetky certifikáty podpísané použitím kompromitovaného kľúča. CAMOSR upozorní prostredníctvom svojho webu držiteľov certifikátov, ktoré boli podpísané zrušeným certifikátom CAMOSR ako aj strany spoliehajúce sa na dané certifikáty, že zrušený certifikát CAMOSR sa má odstrániť z každej aplikácie, ktorú používajú strany

spoliehajúce sa na certifikát a má byť nahradený novým certifikátom CAMOSR.
- Došlo k zmene kľúčov koreňovej certifikačnej autority, ktorá vydala certifikát certifikačnej autorite CAMOSR

Zmena kľúčov osôb v dôveryhodných úrovniach (role) CAMOSR sa nevykonáva.

Zmena kľúčov pre TSA nastáva za rovnakých podmienok. Verejný kľúč vytvorený na základe nového kľúčového páru je podpísaný kvalifikovaným certifikátom vlastnej certifikačnej autority.

4.10 Havarijný plán

V prípade kompromitácie kľúča CAMOSR sa certifikát CAMOSR zruší. Informácia o jeho zrušení sa musí publikovať okamžite najrýchlejším možným spôsobom. Ďalšie potrebné opatrenia sú uvedené v časti 4.9.

V prípade havárie, pri ktorej je vybavenie CAMOSR poškodené a neschopné prevádzky, ale nie je zničený jej podpisový kľúč, fungovanie CAMOSR treba obnoviť podľa možnosti čo najrýchlejšie.

V prípade havárie, pri ktorej je inštalácia CAMOSR fyzicky poškodená, jej podpisový kľúč je v dôsledku toho zničený a nie je ho možné obnoviť zo zálohy, sa certifikát CAMOSR zruší.

CAMOSR má vypracovaný dokument „Havarijné postupy a plány obnovy na výkon certifikačných činností a ochranu osobných údajov držiteľov certifikátov.“ zaoberajúci sa postupmi pre zabezpečenie činnosti CAMOSR v prípade mimoriadnych udalostí.

4.11 Ukončenie činnosti CAMOSR

Ešte pred skončením poskytovania služieb sa vykoná:

- CAMOSR patričným spôsobom, minimálne 3 mesiace vopred, oznámi informácie o plánovanom skončení svojej činnosti NBÚ, držiteľom všetkých ňou vydaných platných certifikátov a stranám spoliehajúcim sa na certifikáty. Toto oznámenie sa vykoná prostredníctvom webu CAMOSR, elektronickej pošty.
- Skončia sa všetky mandátne zmluvy, splnomocnenia a pod., na základe ktorých mohli konať v mene CAMOSR (napr. poskytovať služby LRA).
- Ďalej postupuje podľa §4 ods. 2 zákona 272/2016. CAMOSR uzavrie zmluvu s iným kvalifikovaným poskytovateľom dôveryhodných služieb o poskytovaní informácie o štatúte platnosti alebo zrušenia vydaných kvalifikovaných certifikátov a prevzatí súvisiacej prevádzkovej dokumentácie. Ak CAMOSR neuzavrie dohodu, poskytovanie informácie o štatúte platnosti alebo zrušenia vydaných kvalifikovaných certifikátov a prevzatie súvisiacej prevádzkovej dokumentácie zabezpečí úrad.

- Všetky dokumenty a archivované dáta od LRA aj ostatných zložiek CAMOSR sa sústredia a archivujú v zmysle platného registratúrneho poriadku.
- Vykoná kontrolu dodržania zákona o ochrane osobných údajov.

Po skončení svojej činnosti CAMOSR nevydá žiaden certifikát, časovú pečiatku a zabezpečí preukázateľné zničenie podpisových dát (privátneho kľúča) CAMOSR.

Ak je dôvodom skončenia činnosti CAMOSR nejaký dôvod bez vzťahu k bezpečnosti, potom ani certifikát CAMOSR, ktorá končí činnosť, ani certifikáty podpísané touto CAMOSR nemusia byť zrušené.

5 FYZICKÉ, PROCEDURÁLNE A PERSONÁLNE BEZPEČNOSTNÉ OPATRENIA

Bezpečnosť CAMOSR je založená na súhrne bezpečnostných opatrení v oblasti fyzickej a objektovej, procedurálnej a personálnej bezpečnosti. Tieto bezpečnostné opatrenia sú navrhnuté, dokumentované a aplikované na základe bezpečnostných pravidiel.

5.1 Opatrenia na fyzickú bezpečnosť

Pracovisko CAMOSR sa nachádza v budove, ktorú nepretržite stráži strážna služba. Pracovisko CAMOSR je režimové pracovisko.

Vybavenie CAMOSR je nepretržite chránené pred neautorizovaným prístupom a to aj pred neautorizovaným fyzickým prístupom. Vybavenie pozostáva len z vybavenia vyhradeného na funkcie CAMOSR, nesmie slúžiť na žiadne účely, ktoré sa netýkajú CAMOSR.

Je zakázané používať neautorizované vybavenie CAMOSR. Sú implementované opatrenia na fyzickú bezpečnosť, ktoré ochránia hardvér a softvér pred neautorizovaným použitím. Kryptografické moduly sú chránené pred krádežou, stratou a neautorizovaným použitím.

Zariadenia a priestory, v ktorých je umiestnené vybavenie CAMOSR, je dostatočne zásobované elektrickou energiou a klimatizované v záujme vytvorenia spoľahlivého operačného prostredia.

Médiá sú uskladnené tak, aby boli chránené pred náhodným, neúmyselným poškodením (vodou, ohňom, elektromagneticky). Médiá, ktoré obsahujú informácie týkajúce sa bezpečnostného auditu, archív alebo zálohované informácie sú uložené v lokalite oddelenej od vybavenia CAMOSR.

Zálohy a archivované dokumenty sú uložené na mieste s fyzickými a procedurálnymi opatreniami primeranými prevádzkovanej CAMOSR a oddelene od priestorov CAMOSR.

Záložné pracovisko je umiestnené geograficky oddelené od hlavného pracoviska.

5.2 Procedurálne opatrenia

Kontrola prístupu k informačným systémom CAMOSR je riadená pomocou doménových politík a ďalších rozšírených interných pravidiel, brániacich neautorizovanému prístupu. Firewally by mali byť nastavené striktne povoľujúc iba protokoly a prístupy nevyhnutné pre vykonávané operácie a poskytované služby CAMOSR.

Dôležitým princípom procedurálnych bezpečnostných opatrení, ktorý podporuje celkovú bezpečnosť CAMOSR, je princíp „need to know“. CAMOSR pozostáva z organizačného hľadiska zo služobných rolí („funkcií“), ktoré zastávajú navzájom nezávislé skupiny osôb. Týmto sa oddelí prístup k citlivým informáciám, t.j. každá osoba má prístup len k tým informáciám, ktoré potrebuje na výkon úrovne (role), ktorú zastáva.

Tento prístup poskytuje tiež možnosť, že pri niektorých osobitne dôležitých činnostiach sa môže vyžadovať, aby pri ich vykonávaní bolo prítomných viacero osôb zastávajúcich danú rolu (tzv. princíp “K” z “N”). Dôvodom tu je bezpečnostné hľadisko – prítomné osoby sa navzájom kontrolujú – týmto sa minimalizuje tak možnosť úmyselného zneužitia právomoci nejakou osobou ako aj pravdepodobnosť neúmyselnej chyby alebo omylu. Príslušnosť k roly ďalej bráni vzniku konfliktu záujmov a definuje, konkrétne zodpovednosti.

Každá činnosť v ľubovoľnom systéme, ktorý je súčasťou CAMOSR, je prístupná len predstaviteľovi tej služobnej úrovne (role), ktorá má na danú činnosť oprávnenie. Všetky činnosti sa pritom musia realizovať v súlade s príslušnými zavedenými procedúrami a postupmi.

Pred sprístupnením kritických aplikácií musí byť používateľ autentifikovaný, na základe čoho je zaradený do konkrétnej roly a jeho činnosť v systéme je monitorovaná.

Pre všetky služobné úrovne (role), ktoré kľúčovým spôsobom vplývajú na poskytovanie dôveryhodných služieb, sú zavedené dokumentované procedúry a postupy.

Zálohy systému postačujúce na obnovu v prípade zlyhania systému sa vykonávajú podľa periodického rozvrhu a s použitím vopred definovaných a dokumentovaných postupov a procedúr.

Každá rola musí mať definovaný spôsob identifikácie a autentifikácie pri prístupe k informačným systémom CAMOSR a stanovené kritéria, ktoré zohľadňujú potrebu oddelenia funkcií z hľadiska samotnej role t. j. musia byť uvedené role, ktoré nemôžu byť vykonávané rovnakými jednotlivcami.

Zoznam rolí a ich jednotlivých členov schvaľuje PMA. Musí sa dbať na jeho aktuálnosť a striktné dodržiavanie pridelených oprávnení. Priradenie nového člena do role bez jeho predošlého uverejnenia v schválenom zozname rolí je neprípustné.

5.3 Personálne bezpečnostné opatrenia

Personálne bezpečnostné opatrenia sú zabezpečované internými mechanizmami subjektu – zriaďovateľa.

Prevádzku CAMOSR zabezpečujú pracovníci s odbornou znalosťou problematiky elektronického podpisu, so znalosťou bezpečnostných procedúr v prípade pracovníkov s bezpečnostnými povinnosťami, skúsenosťami s informačnou bezpečnosťou a s vedomosťami z oblasti legislatívy.

Všetky služobné úrovne (role) sa personálne obsadzujú tak, aby sa vylúčil prípadný konflikt záujmov, ktorý by mohol vytvárať oprávnené pochybnosti o dôveryhodnosti

CAMOSR. Služobné úrovne (role), ktoré sú vo vzťahu vzájomnej podriadenosti, sa personálne obsadzujú tak, aby nemohla byť spochybnená nezávislosť a nestrannosť pri výkone kontrolných funkcií.

Osoby, vybrané na zastávanie úrovní (role), ktoré si vyžadujú dôveryhodnosť, musia byť zodpovedné a dôveryhodné. Funkcie, vykonávané týmito úrovňami (role), formujú základ dôvery v celú PKI. Aby sa zvýšila pravdepodobnosť, že tieto úrovne (role) sa budú vykonávať úspešne, uplatňujú sa dva prístupy. Prvým prístupom je zabezpečenie, aby osoba vykonávajúca funkciu na požadovanej úrovni (role) bola dôveryhodná a primerane vyškolená a poučená. Druhým prístupom je rozdelenie funkcie s úrovňami (role) medzi niekoľko ľudí tak, aby sa zabránilo ľubovoľnej škodlivej činnosti, ktorá by si vyžadovala dohodu s inou osobou.

Personál pre ľubovoľnú úroveň (role) sa vyberá na základe spoľahlivosti, lojality a dôveryhodnosti. Všetky osoby zastávajúce služobné úrovne (role) musia byť občanmi Slovenskej republiky.

Osoby vybrané na zastávanie služobných úrovní (role) musia mať odborné vedomosti, primerané skúsenosti a kvalifikáciu potrebnú na vykonávanie ponúkaných služieb a úrovní (role).

Všetky osoby zastávajúce služobné úrovne (role) musia byť primerane poučené a zaškolené.

Zmluvne zabezpečené činnosti sa môžu vykonávať len prostredníctvom pracovníkov CAMOSR.

Pracovníci CAMOSR majú prístup k dokumentácii podľa zastávanej role.

5.4 Postup získavania auditných záznamov

CAMOSR musí zaznamenávať a mať k dispozícii počas nevyhnutnej doby, aj po skončení činnosti, všetky dôležité informácie týkajúce sa poskytovania dôveryhodných služieb.

CAMOSR musí v systéme na poskytovanie dôveryhodných služieb zaznamenávať presný čas. Čas zaznamenávaný pri jednotlivých udalostiach musí byť synchronizovaný s UTC minimálne každých 24 hodín.

5.4.a Typy zaznamenávaných udalostí

CAMOSR musí zaznamenávať a vyhodnocovať nasledovné dôležité udalosti:

- procesy týkajúce sa životného cyklu kľúčov autorít (generovanie, zálohovanie, obnova, likvidácia, ...)
- procesy týkajúce sa samotného HSM modulu
- údaje získané pri poskytovaní dôveryhodných služieb
- odchýlky synchronizácie času
- aplikačné logy systému CAMOSR
- systémové logy jednotlivých častí systému CAMOSR

5.4.b Frekvencia spracovávania auditných záznamov

Administrátori CA sú povinní sledovať zasielané logy priebežne, tak aby včas odhalili potenciálne nebezpečenstvo ohrozenia poskytovania služieb. Všetky zaznamenávané logy v elektronickej podobe musia byť v pravidelných intervaloch, minimálne 1 krát mesačne, ukladané na záznamové médiá, aby mohli byť k dispozícii audítorom. Rovnako musia byť audítorom k dispozícii všetky písomné auditné záznamy z procesov týkajúcich sa životného cyklu kľúčov CA, TSAmil, TSAext a OCSP responderov.

Auditné záznamy musia byť uchovávané a chránené tak, aby nedošlo k ich znehodnoteniu najlepšie vo viacerých kópiách umiestnených v rozdielnych priestoroch po dobu 10 rokov.

6 TECHNICKÉ BEZPEČNOSTNÉ OPATRENIA

Technická časť infraštruktúry CAMOSR (hardvér a softvér) bude pozostávať len z bezpečných systémov a oficiálneho softvéru. Architektúru infraštruktúry CAMOSR navrhli skúsení odborníci s použitím komponentov, ktoré vyhovujú bezpečnostným štandardom na úrovni súčasných poznatkov.

Osobitná pozornosť musí byť venovaná kryptografickému modulu (HSM modulu), ktorý slúži na generovanie, úschovu a použitie privátneho kľúča CAMOSR a ktorý patrí k najcitlivejším aktívam. Privátny kľúč CAMOSR je uložený v HSM module, ktorý je certifikovaný minimálne podľa štandardu FIPS 140-2 level 3.

CAMOSR používa na ochranu svojho privátneho kľúča kombináciu fyzických, logických a procedurálnych opatrení, ktoré zaručujú bezpečnosť privátneho kľúča. Tieto opatrenia sú popísané v dokumente CPS.

Súčasťou systému CAMOSR sú zariadenia na nepretržitú detekciu, monitorovanie a signalizáciu neautorizovaných a neobvyklých pokusov o prístup k jej prostriedkom.

Aplikácie súvisiace s udávaním stavu zrušenia musia zabezpečiť kontrolu prístupu pred pokusmi o modifikovanie informácií o stave zrušenia.

Publikačné aplikácie zabezpečia kontrolu prístupu pred pokusmi o pridanie alebo zmazanie certifikátu alebo modifikovaním iných združených údajov.

6.1 Generovanie a inštalácia kľúčov

- Vydavateľ certifikátov a časových pečiatok

Generovanie a inštalácia páru kľúčov CAMOSR sa musí vykonávať štandardizovaným spôsobom, ktorý je podrobne popísaný v dokumentácii CAMOSR. Spôsob generovania musí zabezpečiť dostatočnú dôveru v procedúru generovania a celý proces musí byť písomne zaznamenaný. Generovanie kľúča musia zabezpečiť pracovníci CAMOSR zaradení v roliach, ktoré majú oprávnenie na účasť na ceremónii generovania žiadosti. Generovanie kľúčov musí byť vykonané v bezpečnom zariadení na uchovávanie kryptografických kľúčov, ktoré je certifikované NBÚ.

- Koncoví používatelia - Pozri kapitolu **Chyba! Nenašiel sa žiaden zdroj odkazov.**

Vygenerovaný kľúčový pár koncového držiteľa certifikátu mu musí byť odovzdaný osobne v QSCD zariadení po vydaní certifikátu.

Kľúčový pár generovaný v HSM generuje žiadateľ v zariadení bez nutnosti priniesť zariadenie do priestorov LRA.

Súkromný kľúč subjektu nikdy nie je doručovaný vydavateľovi certifikátu.

Certifikát CAMOSR ako aj nadriadený certifikát je možné bezpečne získať z webového sídla CAMOSR alebo NBÚ SR.

Dĺžka kľúča je definovaná v profiloch certifikátu v kapitole 7.

Aplikácie súvisiace s udávaním stavu zrušenia zabezpečia kontrolu prístupu pred pokusmi o modifikovanie informácií o stave zrušenia.

Všetky funkcie CAMOSR, pri ktorých sa používa počítačová sieť, sú zabezpečené pred neautorizovaným prístupom a inými škodlivými činnosťami.

6.2 Ochrana súkromného kľúča

Kľúčový pár určený pre vydavateľa certifikátov a časových pečiatok musí:

- byť generovaný v bezpečnostnom module, ktorý je certifikovaný NBÚ a spĺňa požiadavky štandardu FIPS 140-2 level 3,
- akákoľvek manipulácia so súkromným kľúčom môže byť umožnená len z princípu viacnásobnej kontroly, pričom minimálny počet potrebných osôb musí byt tri. Manipulácia sa týka obnovy kľúče do iného HSM modulu v prípade poškodenia modulu, v ktorom sú kľúče aktuálne uložené.
- Dáta potrebné na zálohu súkromného kľúča sú zálohované v pravidelných intervaloch, tak aby bolo možné v prípade potreby vykonať obnovu kľúčov. Zálohovanie sa vykonáva automaticky, po vykonaní zálohy sa dáta potrebné na obnovu kľúčov zašifrujú.
- Aktivácia súkromných kľúčov sa vykonáva prostredníctvom operátorských kariet, kľúč je aktivovaný spustením služby potrebnej na podpisovanie žiadostí. Kľúč je aktívny, kým je služby spustená. Súkromný kľúč možno deaktivovať vypnutím služby.
- Súkromný kľúč možno zničiť zmazaním kľúčov z bezpečnostného modulu.
- Súkromné kľúče CAMOSR sa môžu používať výlučne na podpisovanie certifikátov a CRL vydávaných CA, ktorú prevádzkuje CAMOSR.
- Vybavenie CA musí byť neprestajne chránené pred neautorizovaným prístupom a to aj pred neautorizovaným fyzickým prístupom.
- HSM modul musí byť chránený pred odchytávaním elektromagnetického vyžarovania.

6.3 Manažment párových dát

Verejné kľúče koncových držiteľov musia byť bezpečne uchovávané v databáze spravovanej CAMOSR.
Pre jednotlivé typy certifikátov je určený maximálny interval používania párových dát (súkromný a verejný kľúč) definovaný v profile certifikátu .

6.4 Aktivačné údaje

Aktivačné údaje držiteľov certifikátov (PIN a Sekundárny autentifikačný PIN), ktoré sa viažu ku konkrétnemu QSCD musia byť definované pri aktivovaní zariadenia priamo žiadateľom. PUK je generovaný aplikáciou a je odovzdaný žiadateľovi po vydaní certifikátu. Držiteľ musí byť poučený o potrebe a spôsobe ich zmeny a o rizikách pokiaľ uvedené zmeny nevykoná.

Aktivačné údaje držiteľov kariet k HSM chránia pred zneužitím samotní majitelia kariet.

Nikto nesmie mať prístup k súkromnému kľúču okrem jeho držiteľa.

Ak sa aktivačné dáta zapíšu, musia byť zabezpečené na úrovni ochrany dát, na ochranu ktorých sa používa daný kryptografický modul a nemú byť uložené spolu s ním.

Aktivačné dáta pre súkromné kľúče patriace k certifikátom potvrdzujúcim individuálnu identitu nesmú byť nikdy zdieľané.

6.5 Počítačové bezpečnostné opatrenia

Systémy určené na správu certifikačnej autority a lokálnych registračných autorít musia byť pravidelne aktualizované a kontrolované voči známym hrozbám. Prístup k systému je riadený PMA. Všetky aktivity musia byť zaznamenávané a vyhodnocované. Stav kritických služieb musí byť monitorovaný.

CAMOSR vydávajúca kvalifikované certifikáty musí spĺňať špecifické požiadavky na bezpečnosť informácií kladené na dôveryhodného poskytovateľa služieb, ktoré sú definované v štandarde ETSI EN 319411-2 „Electronic Signatures and Infrastuctures (ETSI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates“.

6.6 Bezpečnostné opatrenia na vývoj a riadenie bezpečnosti

Bezpečnostné opatrenia vývojového prostredia sú identické s bezpečnostnými opatreniami ostrej prevádzky. Riadenie bezpečnosti vychádza z platných nariadení a smerníc platných pre MOSR.

6.7 Sieťové bezpečnostné opatrenia

Opatrenia na ochranu infraštruktúry sú zdokumentované v internom dokumente.

6.8 Opatrenia pre kryptografické moduly

CAMOSR musí používať kryptografické moduly v zmysle štandardu FIPS 140-2.

7 Profily certifikátov a zoznamov zrušených certifikátov

Profily certifikátov a zoznamov zrušených certifikátov sú stanovené centrálne – ani osoby zastávajúce služobné úrovne (role) nemôžu svojvoľne meniť štruktúru certifikátov. Štruktúra certifikátov vydávaných CAMOSR sa môže meniť len na základe rozhodnutia PMA.

7.1 Profil certifikátu

Tento dokument povoľuje len certifikáty vyhovujúce štandardu X.509 verzie 3.

7.1.a Vlastný certifikát CAMOSR (CAMOSR2)

Algoritmy a dĺžky kľúčov uplatňované vo vlastnom certifikáte CAMOSR:

Algoritmus podpisu (Signature Algorithm): **Sha256RSA**
Verejný kľúč: **RSA, dĺžka je 4 096 bitov**
Algoritmus fingerprintu (Thumbprint Algorithm): **SHA1**

Lehota platnosti certifikátu CAMOSR: je stanovená NBÚ, ktorý certifikát vydáva.

Tabuľka č. 3: Obsah položiek vo vlastnom certifikáte CAMOSR

Názov položky	Skratka názvu položky	Hodnota položky
Štát (countryName)	C	SK
Mesto (localityName)	L	Trencin
Organizácia (organizationName)	O	Ministry of Defence
Názov (commonName)	CN	CAMOSR2

Poznámka. Použité rozšírenia (certificate extensions) a ich hodnoty vo vlastnom certifikáte CAMOSR stanovil NBÚ ako vydavateľ certifikátu.

7.1.b Kvalifikovaný certifikát

Štruktúra certifikátov vydávaných CAMOSR sa môže meniť len na základe rozhodnutia PMA. V prípade, ak je vydaný pseudonym certifikát, neobsahuje DN položky G a SN a v CN je napísané PSEUDONYM.

Algoritmy a dĺžky kľúčov uplatňované v certifikáte:

Algoritmus podpisu (Signature Algorithm): **Sha256RSA**

Verejný kľúč: **RSA, dĺžka je 2 048 bitov**

Algoritmus fingerprintu (Thumbprint Algorithm): **SHA1**

Lehota platnosti certifikátu je maximálne 3 roky, ak nebola zmluvne dohodnutá iná lehota platnosti.

Tabuľka č. 4: Obsah položiek rozlišovacieho mena v KC

Názov položky	Skratka názvu položky	Popis položky	Príklad hodnoty položky	Typ a max. dĺžka položky
countryName (Štát)	C	Dvojznaková skratka štátu – dvojmiestny kód podľa ISO 3166 definujúci štátnu príslušnosť subjektu, údaj je povinný	SK	PrintableString 2 znaky
stateOrProvinceName (Kraj)	S	Názov kraja resp. provincie, údaj je nepovinný	Trenciansky	UTF8String 128 znakov
localityName (Mesto)	L	Názov lokality, údaj je nepovinný	Trencin	UTF8String 128 znakov
organizationName (Organizácia)	O	Názov organizácie, údaj je povinný	Ministry of Defence	UTF8String 64 znakov
organizationUnitName (Útvar v organizácii)	OU	Názov útvaru, údaj je nepovinný	VÚ 8116	UTF8String 64 znakov
commonName (Meno a priezvisko)	CN	Meno a priezvisko údaj je povinný	Jan Strelec alebo napr. Aligator PSEUDONYM	UTF8String 64 znakov

givenName (Meno(á))	G	Všetky mená použité v položke CN okrem priezviska, údaj je povinný, ak v položke CN nebol uvedený pseudonym, ale v prípade použitia pseudonymu údaj nesmie byť uvedený	Jan	UTF8String 64 znakov
Surname (Priezvisko)	SN	Priezvisko z položky CN, údaj je povinný, ak v položke CN nebol uvedený pseudonym, ale v prípade použitia pseudonymu údaj nesmie byť uvedený	Strelec	UTF8String 64 znakov
serialNumber (Sériové číslo)	SERIALNUMBER	Odkaz na identitu fyzickej osoby – rodné číslo. Povinný údaj	PNOSK 9959199999, PASSK P3000180, IDCSK SK989783	UTF8String

Tabuľka č. 5: Použité rozšírenia v KC CAMOSR

Názov rozšírenia	Hodnota rozšírenia	Kritickosť
authorityKeyIdentifier	určí sa výpočtom	nekritické
subjectKeyIdentifier	určí sa výpočtom	nekritické

keyUsage	Non-Repudiation	kritické
certificatePolicies	Policy Identifier=1.3.158.36061701.0.0.0.1.2.2 Policy Identifier=1.3.158.30845572.1.7.3.01 CPS=http://pki.mil.sk/ACA2/CP2.pdf,	nekritické
crlDistributionPoints	URI: http://pki.mil.sk/ACA2/camosr2.crl, URI: http://crl.mil.sk/ACA2/camosr2.crl,	nekritické
AuthorityInfoAccess	URI: http://pki.mil.sk/ACA2/camosr2.p7c OCSP: http://ocsp.mil.sk/ocsp	nekritické
QCstatements	esi4-qcStatement-1 (id-etsi-qcs-QcCompliance) esi4-qcStatement-4 (id-etsi-qcs-QcSSCD)	nekritické
SubjectAltNames	email adresa držiteľa certifikátu (rfc822Name), ak bola zadaná v žiadosti o certifikát Registered ID s hodnotou JIDO držiteľa certifikátu Držitelia bez priradeného JIDO – Registered ID sa neuvádza.	nekritické
BasicConstraints	Subject Type=End Entity Path Length Constraint=None	kritické

Tabuľka č. 6: Obsah položiek rozlišovacieho mena v KC pre elektronickú pečať

Názov položky	Skratka názvu položky	Popis položky	Príklad hodnoty položky	Typ a max. dĺžka položky
countryName (Štát)	C	Dvojznaková skratka štátu – dvojmiestny kód podľa ISO 3166 definujúci štátnu príslušnosť subjektu, údaj je povinný	SK	PrintableString 2 znaky
stateOrProvinceName (Kraj)	S	Názov kraja resp. provincie, údaj je nepovinný	Trenciansky	UTF8String 128 znakov
localityName (Mesto)	L	Názov lokality, údaj je nepovinný	Trencin	UTF8String 128 znakov

organizationName (Organizácia)	O	Názov organizácie, údaj je povinný	Ministry of Defence	UTF8String 64 znakov
organizationUnitName (Útvar v organizácii)	OU	Názov útvaru, údaj je nepovinný	VÚ 8116	UTF8String 64 znakov
commonName (Meno a priezvisko)	CN	Meno, názov systému, pre ktoré je certifikát vydávaný údaj je povinný	LTA	UTF8String 64 znakov
serialNumber (Sériové číslo)	SERIALNUMBER	Odkaz na identifikačný údaj orgánu verejnej moci alebo právnickej osoby Povinný údaj	"VATSK-12311321" alebo "SZ:SK-123123".	UTF8String

Tabuľka č. 7: Použité rozšírenia v KC pre elektronickú pečať CAMOSR

Názov rozšírenia	Hodnota rozšírenia	Kritickosť
authorityKeyIdentifier	určí sa výpočtom	nekritické
subjectKeyIdentifier	určí sa výpočtom	nekritické
keyUsage	Non-Repudiation	kritické
certificatePolicies	Policy Identifier=1.3.158.36061701.0.0.0.1.2.2 Policy Identifier=1.3.158.30845572.1.7.3.01 CPS=http://pki.mil.sk/ACA2/CP2.pdf,	nekritické
crlDistributionPoints	URI: http://pki.mil.sk/ACA2/camosr2.crl, URI: http://crl.mil.sk/ACA2/camosr2.crl,	nekritické
AuthorityInfoAccess	URI: http://pki.mil.sk/ACA2/camosr2.p7c OCSP: http://ocsp.mil.sk/ocsp	nekritické
QCstatements	esi4-qcStatement-1 (id-etsi-qcs-QcCompliance) esi4-qcStatement-4 (id-etsi-qcs-QcSSCD)	nekritické
SubjectAltNames	email adresa držiteľa certifikátu (rfc822Name),	nekritické
BasicConstraints	Subject Type=End Entity Path Length Constraint=None	kritické

7.1.c OCSP certifikát

Algoritmy a dĺžky kľúčov uplatňované v certifikáte:

Algoritmus podpisu (Signature Algorithm): **Sha256RSA**
Verejný kľúč: **RSA, dĺžka je 2 048 bitov**
Algoritmus fingerprintu (Thumbprint Algorithm): **SHA1**

Lehota platnosti certifikátu je maximálne 3 roky, ak nebola zmluvne dohodnutá iná lehota platnosti.

Tabuľka č. 8: Obsah položiek v certifikáte OCSP

Názov položky	Skratka názvu položky	Popis položky	Príklad hodnoty položky	Typ a max. dĺžka položky
countryName (Štát)	C	Dvojznaková skratka štátu –	SK	PrintableString 2 znaky
localityName (Mesto)	L	Názov lokality, údaj je nepovinný	Trencin	UTF8String 128 znakov
organizationName (Organizácia)	O	Názov organizácie, údaj je povinný	Ministry of Defence	UTF8String 64 znakov
organizationUnitName (Útvar v organizácii)	OU	Názov útvaru, údaj je nepovinný	ACA-206/2006-2	UTF8String 64 znakov
commonName (Meno a priezvisko)	CN	meno OCSP údaj je povinný	OCSP ACA MOSR	UTF8String 64 znakov

Tabuľka č. 9: Použité rozšírenia v OCSP certifikáte CAMOSR

Názov rozšírenia	Hodnota rozšírenia	Kritickosť
authorityKeyIdentifier	určí sa výpočtom	nekritické
subjectKeyIdentifier	určí sa výpočtom	nekritické
keyUsage	Non-Repudiation	kritické
certificatePolicies	Policy Identifier=1.3.158.36061701.0.0.0.1.2.2 Policy Identifier=0.4.0.2042.1.2 Policy Identifier=1.3.158.30845572.1.7.3.01 CPS=http://pki.mil.sk/ACA2/CP2.pdf,	nekritické
crlDistributionPoints	URI: http://pki.mil.sk/ACA2/camosr2.crl, URI: http://crl.mil.sk/ACA2/camosr2.crl,	nekritické

AuthorityInfoAccess	URI: http://pki.mil.sk/ACA2/camosr2.p7c OCSP: http://ocsp.mil.sk/ocsp	nekritické
Extended key usage	OCSP Signing (1.3.6.1.5.5.7.3.9)	kritické
BasicConstraints	Subject Type=End Entity Path Length Constraint=None	kritické

7.1.d Certifikát TSA

Algoritmy a dĺžky kľúčov uplatňované v certifikáte:

Algoritmus podpisu (Signature Algorithm): **Sha256RSA**
Verejný kľúč: **RSA, dĺžka je minimálne 2 048 bitov**
Algoritmus fingerprintu (Thumbprint Algorithm): **SHA1**

Lehota platnosti certifikátu je maximálne 3 roky, ak nebola zmluvne dohodnutá iná lehota platnosti.

Tabuľka č. 10: Obsah položiek v certifikáte pre TSAMOSR

Názov položky	Skratka názvu položky	Popis položky	Príklad hodnoty položky	Typ a max. dĺžka položky
countryName (Štát)	C	Dvojznaková skratka štátu –	SK	PrintableString 2 znaky
localityName (Mesto)	L	Názov lokality, údaj je nepovinný	Trencin	UTF8String 128 znakov
organizationName (Organizácia)	O	Názov organizácie, údaj je povinný	Ministry of Defence	UTF8String 64 znakov
organizationUnitName (Útvar v organizácii)	OU	Názov útvaru, údaj je nepovinný	ACA-206/2006-2	UTF8String 64 znakov
commonName (Meno a priezvisko)	CN	meno OCSP údaj je povinný	TSAMOSR	UTF8String 64 znakov

Tabuľka č. 11: Použité rozšírenia v certifikáte pre TSAMOSR

Názov rozšírenia	Hodnota rozšírenia	Kritičnosť
AuthorityInfoAccess	URL=http://pki.mil.sk/camosr2.cer	nekritické
AuthorityKeyIdentifier	KeyID = určí sa výpočtom Certificate Issuer= Directory Address vydavateľa certifikátu CA Certificate SerialNumber= SerialNumber vydavateľa certifikátu CA	nekritické
CertificatePolicies	Policy Identifier=1.3.158.36061701.0.0.0.1.2.2 Policy Identifier= 1.3.158.30845572.1.7.3.01 CPS= http://pki.mil.sk/ACA2/CP2.pdf	nekritické
crlDistributionPoints	URI: http://pki.mil.sk/ACA2/camosr2.crl URI: http://crl.mil.sk/ACA2/camosr2.crl	nekritické
KeyUsage	Non-Repudiation	nekritické
subjectKeyIdentifier	určí sa výpočtom	nekritické
BasicConstraints	Subject Type=End Entity Path Length Constraint=None	kritické
ExtendedKeyUsage	Time Stamping (1.3.6.1.5.5.7.3.8)	kritické

7.2 Profil zoznamu zrušených certifikátov

CRL vydávané CAMOSR sú CRL verzie 2.

CRL budú vydávané tou istou CAMOSR ako certifikáty.

Tabuľka č. 12: Použité rozšírenia (CRL extensions) v kvalifikovanom CRL

Názov rozšírenia	Hodnota rozšírenia	Kritickosť
authorityKeyIdentifier	určí sa výpočtom	nekritické
CRLNumber	určuje sa automaticky	nekritické

7.3 Profil OCSP

V prípade vydávaných OCSP odpovedí, tieto musia byť v zmysle RFC 6960.

Tabuľka č. 13: Rozšírenia v OCSP odpovedi

Názov	Vyžadovanie	Kritickosť
id-commonpki-at-certHash	ÁNO	NIE
id-pkix-ocsp-nonce	NIE	NIE
id-pkix-ocsp-archive-cutoff	NIE	NIE

8 AUDIT ZHODY

8.1 Frekvencia a periodicita auditu

CAMOSR sa podrobí externému auditu bezpečnosti poskytovania kvalifikovaných dôveryhodných služieb a to raz za dva roky v súlade s požiadavkami platnej legislatívy.

Okrem toho CAMOSR má právo požadovať pravidelné a nepravidelné revízie činností jej LRA, aby sa potvrdilo, že LRA funguje v súlade s bezpečnostnými praktikami a procedúrami popísanými v tomto CP a v príslušnom dokumente CPS.

8.2 Identita a kvalifikácia audítora a vzťah k auditovanému subjektu

Audítor musí byť podľa platnej legislatívy oprávnený na výkon auditu bezpečnosti kvalifikovaných dôveryhodných služieb, musí byť kompetentný v oblasti auditov zhody a musí byť dôkladne oboznámený s týmto dokumentom a dokumentom CPS.

Osoba audítora musí byť nezávislá od CAMOSR a zriaďovateľa CAMOSR, aby bola zaručená nestrannosť a objektívnosť auditu.

Audítora musí vybrať PMA.

8.3 Zoznam oblastí, ktoré sú predmetom auditom zhody

Témy pokrývané auditom definuje platná legislatíva.

Cieľom auditu má byť záruka, že CAMOSR má vyhovujúci systém práce, ktorý garantuje kvalitu služieb, ktoré CAMOSR poskytuje a ktorý garantuje, že CAMOSR koná v súlade s platnou legislatívou a so všetkými požiadavkami tohto dokumentu.

Predmetom auditu majú byť všetky aspekty prevádzky CAMOSR vzťahujúce sa k tomuto dokumentu.

8.4 Zoznam opatrení realizovaných na základe výsledkov auditu

Keď audítor zistí rozpor medzi prevádzkou CAMOSR a platnou legislatívou alebo ustanoveniami CP a vydaných CPS, musia sa uskutočniť tieto akcie:

- audítor zaznamená rozpor,
- audítor upovedomí o rozpore subjekty definované v časti 2.7.e
- PMA určí vhodné opatrenie na nápravu a to prípadne až po zrušenie vlastného certifikátu CAMOSR,
- po náprave nedostatkov PMA obnoví činnosť CAMOSR resp. LRA.

8.5 Výsledky auditu

Audítor odovzdá PMA podľa platnej legislatívy záverečnú správu o audite o zhode. Výsledky budú oznámené auditovanému subjektu a v prípade LRA aj jej nadriadenej CAMOSR.

Vykonanie opatrení na nápravu má byť dané na vedomie príslušnej autorite. Na potvrdenie vykonania a účinnosti opatrení na nápravu sa môže požadovať špeciálny audit alebo čiastkový audit zameraný na daný aspekt činnosti auditovaného subjektu.

8.6 Interný audit

Počas obdobia, v ktorom CA vydáva certifikáty, musí Poskytovateľ monitorovať dodržiavanie svojej CP a CPS a požiadaviek uvedených v dokumente [3] a kontrolovať poskytované služby vykonávaním interných auditov minimálne na štvrťročnej báze na náhodne vybranej vzorke vydaných certifikátov v počte vyššom ako jeden a najviac v počte tri percentá z vydaných certifikátov v období od predchádzajúceho interného auditu.

9 OSTATNÉ OBCHODNÉ A PRÁVNE NÁLEŽITOSTI

9.1 Povinnosti

Do procesov súvisiacich s poskytovaním a využívaním kvalifikovaných dôveryhodných služieb vstupujú tieto entity:

- samotná certifikačná autorita – je tvorená viacerými úrovňami (role), ktoré sa spoločne označujú ako služobné alebo dôveryhodné úrovne (role) CAMOSR.
- Tieto úrovne (role) definuje dokument CPS. Ich kompetenciu, povinnosti a zodpovednosť vymedzí dokument CPS,
- registračná autorita (RA),
- subjekt (držiteľ certifikátu),
- strana spoliehajúca sa na certifikát (používateľ certifikátu).

9.1.a Povinnosti certifikačnej autority

CAMOSR, ktorá vydáva certifikáty založené na tomto poriadku, musí vyhovovať ustanoveniam tohto dokumentu vrátane týchto ustanovení:

- konať v súlade s ustanoveniami schváleného dokumentu CPS a tohto poriadku,
- zaručiť, že sa akceptujú registračné informácie jedine od LRA, ktoré rozumejú tomuto poriadku a sú zaviazané konať v súlade s ním,
- dávať do certifikátov len správne a príslušné informácie a archivovať doklady dokazujúce správnosť údajov dávaných do certifikátu,
- garantovať, že držiteľ certifikátu je viazaný povinnosťami v súlade s časťou 9.1.d tohto poriadku a informovaný o následkoch neplnenia týchto povinností,
- zrušiť certifikát držiteľovi, ak sa zistí, že tento konal v rozpore so svojimi povinnosťami,
- prevádzkovať v režime on-line repozitár, ktorý vyhovuje ustanoveniam uvedeným v časti 9.1.h,
- zachovávať mlčanlivosť o všetkých informáciách, najmä osobných údajoch, ktoré získa v rámci výkonu svojich povinností,
- pravidelne a včas publikovať a aktualizovať zoznamy zrušených certifikátov (CRL) a poskytovať OCSP odpovede v sieti MOSR.

Ak sa zistí, že CAMOSR nekoná v súlade s týmito povinnosťami, uplatnia sa na ňu príslušné opatrenia.

9.1.b Povinnosti registračnej autority

V mene CAMOSR konajú lokálne registračné autority, pôsobiace v teritóriu regionálnych úsekov KIS, v ktorého pôsobnosti sú zriadené. Lokálne registračné autority poskytujúce dôveryhodné služby CAMOSR (ďalej len LRA) zabezpečujú funkciu

podateľne pre CAMOSR – konkrétne najmä zhromažďovanie a overovanie informácií od zákazníkov – žiadateľov o certifikát, ktoré majú byť uvedené v certifikáte.

LRA, ktorá vykonáva registračné funkcie opísané v tomto poriadku, musí vyhovovať ustanoveniam tohto dokumentu a konať podľa príslušného schváleného dokumentu CPS. Ak sa zistí, že LRA nekoná v súlade s týmito povinnosťami, uplatnia sa na ňu príslušné opatrenia vrátane zastavenia jej činnosti ako RA.

Na LRA sa realizuje priamy kontakt medzi subjektmi certifikátu, resp. žiadateľa o certifikát a CAMOSR.

LRA prijíma žiadosti o certifikát, preveruje totožnosť žiadateľov o certifikát, sprostredkuje odovzdávanie certifikátov a zoznamu zrušených certifikátov subjektom, prijíma a vybavuje ich reklamácie a sťažnosti.

LRA zodpovedá za to, že ňou zbierané informácie RA overila a teda, že tieto informácie sú v danom čase pravdivé.

Pracovníci LRA sú povinní zachovávať mlčanlivosť o všetkých informáciách, najmä o osobných údajoch, ktoré získajú v rámci výkonu svojej roly pre CAMOSR.

Poskytovanie služieb zdravotne ťažko postihnutým osobám je realizované v priestoroch LRA Trenčín resp. v ostatných LRA po dohode so žiadateľom.

9.1.c Povinnosti poskytovateľa služby časovej pečiatky

CAMOSR, ako poskytovateľ služby časovej pečiatky, sa zaväzuje:

- uskutočňovať všetky príslušné požiadavky kladené na TSA uvedené v ods. 4,
- zabezpečiť súlad praxe TSA s procedúrami predpísanými touto politikou a ďalšími súvisiacimi dokumentmi,
- poskytovať služby časovej pečiatky v súlade s prevádzkovou smernicou TSA a ďalšími súvisiacimi dokumentmi.

CAMOSR si plní svoje záväzky v súlade s podmienkami poskytovania služby časovej pečiatky tak, že služba je dostupná pre určených užívateľov vykonáva sa s maximálnou dôslednosťou.

9.1.d Povinnosti žiadateľa o certifikát alebo držiteľa certifikátu

Povinnosťou žiadateľa o certifikát je:

- predložiť LRA presné, pravdivé a úplné informácie v súlade s požiadavkami tohto dokumentu,
- predložiť LRA všetky požadované dokumenty,
- predložiť LRA žiadosť certifikát, na základe ktorej sa má tento vydať, pričom žiadosť o certifikát musí obsahovať údaje, ktoré sú v súlade s údajmi na predkladaných dokumentoch a formulároch,

- prevziať certifikát vydaný na základe jeho žiadosti.

Povinnosťou držiteľa certifikátu (subjektu certifikátu) je:

- neustále chrániť svoje privátne kľúče a QSCD, v ktorých sú uložené, heslá na prístup k privátnym kľúčom v súlade s týmto CP a tiež ako je stanovené v jeho zmluve o vydaní a používaní certifikátu,
- používať len kvalitné, silné heslá na prístup k privátnym kľúčom,
- v prípade straty QSCD, straty, zneužitia alebo kompromitácie privátneho kľúča, zabudnutia hesla na prístup k privátnemu kľúču alebo, ak nastali zmeny alebo sa vyskytli nepresnosti v údajoch uvedených v danom certifikáte, bezodkladne požiadať o zrušenie daného certifikátu. Toto musí byť urobené prostredníctvom mechanizmu, ktorý je v súlade s týmto dokumentom,
- po kompromitácii okamžite a natrvalo zastaviť používanie daného privátneho kľúča,
- dodržovať všetky lehoty, podmienky a obmedzenia uložené na používanie svojich privátnych kľúčov, certifikátov a QSCD,
- Požiadať o zrušenie certifikátu ak nie je súčasťou MOSR, resp. OSSR.

Držiteľ certifikátu, ktorý nedodržiava resp. nedodržiaval svoje povinnosti, nemá nárok na náhradu prípadnej škody.

9.1.e Povinnosti žiadateľa o časovú pečiatku

V tomto dokumente nie sú definované žiadne ďalšie povinnosti pre žiadateľa služby časovej pečiatky okrem tých, ktoré sú stanovené v podmienkach poskytovania tejto služby.

Žiadateľovi sa odporúča po získaní digitálneho odtlačku dokumentu vybaveného časovou pečiatkou overiť si, že táto časová pečiatka je správne podpísaná, a že súkromný kľúč použitý na podpis digitálneho odtlačku dokumentu nie je kompromitovaný.

Žiadateľ je povinný a oprávnený žiadať o vyhotovenie časovej pečiatky len prostredníctvom rozhrania alebo softvérovej aplikácie, ktoré boli dohodnuté medzi ním a CAMOSR resp. rozhranie, ktoré odporúča CAMOSR.

Žiadateľ je povinný počítať s možnou limitáciou použitia časovej pečiatky uvedenou v tomto CP.

Po prijatí časovej pečiatky, o ktorú žiadateľ požiadal, sa žiadateľ stáva automaticky spoliehajúcou sa stranou a teda sa na neho vzťahujú aj povinnosti spoliehajúcich sa strán.

9.1.f Povinnosti subjektu, ktorý koná na báze dôvery v daný certifikát a na základe elektronického podpisu overeného daným certifikátom

Strany spoliehajúce sa na certifikáty vydané podľa tohto poriadku sú povinné:

- predtým, ako sa na daný kvalifikovaný elektronický podpis resp. kvalifikovanú pečať spoľahnú, overiť KC resp. KCPe patriaci k danému podpisu/pečati na jeho platnosť (tzn. overovať, že certifikát bol v danom čase platný a že sa nenachádzal na aktuálnom zozname zrušených KC/KCPe vydanom CAMOSR a to prostredníctvom publikovaných CRL resp. na základe OCSP odpovede - umiestnenie CRL repozitára a OCSP respondera sú uvedené v príslušnom KC/KCPe),
- uchovávať originálne podpísané dáta, aplikácie potrebné na čítanie a spracovanie týchto dát a kryptografické aplikácie potrebné na overovanie kvalifikovaných elektronických podpisov týchto dát, pokiaľ môže byť potrebné overovať podpis týchto dát.

9.1.g Povinnosti subjektu, ktorý koná na báze dôvery v danú časovú pečiatku

- overiť si, že časová pečiatka je správne podpísaná, a že súkromný kľúč použitý na podpis digitálneho odtlačku dokumentu nebol kompromitovaný v čase jeho podpísania
- brať do úvahy všetky obmedzenia používania časovej pečiatky uvedené v politike časovej pečiatky
- brať do úvahy všetky ďalšie predpísané bezpečnostného opatrenia

9.1.h Povinnosti správcov adresárov

Správa adresárov, ktorý podporuje CAMOSR pri publikovaní informácií podľa tohto CP, je povinná:

- udržiavať prístupnosť informácií podľa ustanovení tohto poriadku na publikovanie informácií o certifikátoch,
- poskytovať mechanizmus riadenia prístupu dostatočný na ochranu informácií uložených v repozitári.

Prevádzkovanie a spravovanie repozitára patrí medzi povinnosti CAMOSR.

9.2 Právne záruky

Tento CP sa riadi platnými zákonmi Slovenskej republiky, najmä Nariadením eIDAS a zákonom č. 272/2016 Z.z.

9.2.a Záruky a obmedzenia poskytovaných záruk

CAMOSR garantuje jednoznačnosť čísla (Serial Number) každého ňou vydaného certifikátu, tzn. garantuje, že neexistujú a nikdy nebudú existovať žiadne dva certifikáty, ktoré by mali rovnaké číslo a vydavateľa.

CAMOSR zaručuje výkon kvalifikovaných dôveryhodných služieb v súlade s týmto CP a vydanými CPs.

CAMOSR ručí za to, že pri podpisovaní ňou vydávaných certifikátov a CRL použije vlastný privátny kľúč uložený v HSM module patriaci k jej vlastnému certifikátu CAMOSR.

CAMOSR poskytuje záruku, že ňou vydaný certifikát bude vyhovovať štandardu X.509 v.3.

9.2.b Typy krytých škôd

CAMOSR je zodpovedná výlučne za škody spôsobené spoliehaním sa na informácie, ktoré obsahujú certifikáty ňou vydané. CAMOSR si vyhradzuje právo každý takýto prípad najskôr prešetriť a posúdiť. V prípade, keď CAMOSR nespôsobila chybu v informáciách uvedených v certifikátoch, za prípadné vzniknuté škody CAMOSR nezodpovedá.

9.2.c Ohraničenie možných strát

CAMOSR v žiadnom prípade nezodpovedá za škody spôsobené neoprávneným alebo neopatrným použitím certifikátu, použitím certifikátu mimo rámca definovaného certifikátom a certifikačným poriadkom, neoprávneným alebo neopatrným použitím CRL, použitím neplatného certifikátu (exspirovaného alebo zrušeného), zneužitím súkromného kľúča subjektu, treťou osobou, vyššou mocou (živelná pohroma, vojna prípadne iné nekontrolovateľné udalosti alebo sily).

CAMOSR ani jej LRA nie sú zodpovedné za nesprávne údaje predložené žiadateľom o certifikát, ktoré sa pri registrácii nedajú overiť.

CAMOSR nie je zodpovedná za nepriame, následné alebo náhodné škody, stratu zisku, stratu dát alebo iné škody vzniknuté v súvislosti s používaním alebo nefunkčnosťou certifikátu, zaručeného elektronického podpisu alebo aplikácií, ktoré certifikát používajú.

9.2.d Ďalšie obmedzenia zodpovednosti

CAMOSR nevykonáva funkciu prostredníka medzi držiteľmi certifikátov a používateľmi certifikátov.

CAMOSR nie je zodpovedná za škody vzniknuté v čase od podania žiadosti o zrušenie certifikátu do okamihu zverejnenia daného certifikátu v novom CRL, ak bol daný certifikát zverejnený v novom CRL v stanovenej lehote, spresnenej v tomto dokumente.

Rozsah právnych záruk CAMOSR, ako poskytovateľa kvalifikovaných dôveryhodných služieb, je definovaný v Zmluve o vydaní a používaní certifikátu.

9.3 Finančná zodpovednosť

CAMOSR poskytuje záruku na použitie ňou vydaných certifikátov podľa platnej legislatívy. Predpokladom je, že boli dodržané príslušné ustanovenia tohto CP. Organizácia disponuje dostatočnými prostriedkami na plnenie prípadných záväzkov vyplývajúcich z poskytovanej záruky.

Záruku a z nej vyplývajúce plnenie, je možné uznať len za predpokladu, že subjekt neporušil svoje povinnosti (hlavne ochranu svojho privátneho kľúča), a že každý, kto sa v danom prípade spoliehal na certifikát vydaný CAMOSR, urobil všetko, aby prípadnej škode zabránil, hlavne že si overil aktuálny stav predmetného certifikátu (t.j. či daný certifikát nebol v rozhodujúcom čase, keď sa na neho spoliehalo, na zozname zrušených certifikátov).

Neoverenie stavu certifikátu pomocou zoznamu zrušených certifikátov sa kvalifikuje ako hrubé porušenie povinností vyplývajúcich z tohto dokumentu, dôsledkom čoho zanikajú akékoľvek nároky na prípadné uplatňovanie si záruky voči CAMOSR.

CAMOSR a ani zriaďovateľ CAMOSR nemajú žiadnu finančnú zodpovednosť za prípadné škody, ktoré by vznikli držiteľovi certifikátu alebo strane spoliehajúcej sa na certifikát v súvislosti s používaním certifikátu s nejakou konkrétnou aplikáciou resp. hardvérom alebo v súvislosti s tým, že certifikát nie je možné používať s nejakou konkrétnou aplikáciou resp. hardvérom.

Akákoľvek žiadosť o náhradu škody musí byť podaná písomne.

9.4 Riešenie sporov

PMA rozhoduje s konečnou platnosťou v prípade akýchkoľvek sporov o interpretácii ustanovení alebo použiteľnosti tejto CP.

Pre potreby interpretácie ustanovení tohto poriadku alebo riešenia sporov sa možno obrátiť na LRA a v prípade nesúhlasu s jej rozhodnutím na najbližšiu vyššiu inštanciu. Inštancie sú usporiadané vzostupne v poradí:

- LRA
- CAMOSR (vybavuje len písomne podané žiadosti a podnety)
- NBÚ SR

CAMOSR si vyhradzuje právo každý sporný prípad najprv preskúmať.

Prednostne bude snahou riešiť spory dohodou.

Povinnosťou každej inštancie je prípad zaprotokolovať a dať žiadateľovi o certifikát resp. sťažovateľovi vysvetlenie resp. návrh na riešenie sporu a v prípade jeho nesúhlasu prípad postúpiť na vyššiu inštanciu.

Žiadnym rozhodnutím niektorej z tu definovaných inštancií nie je dotknuté právo sťažovateľa postúpiť sťažnosť nezávislému súdu.

9.5 Poplatky

Nevyberajú sa žiadne poplatky.

9.6 Dôvernosť

9.6.a Typy informácií, ktoré má certifikačná autorita chrániť

Dôvernými informáciami podliehajúcimi zodpovedajúcej ochrane sú:

- privátny kľúč CAMOSR používaný na podpisovanie žiadostí o výdaj certifikátu a zoznamu zrušených certifikátov,
- privátny kľúč autority časovej pečiatky používaný na podpisovanie vydaných časových pečiatok,
- privátny kľúč OCSP respondera, používaný na podpisovanie odpovedí na požiadavky na potvrdenie existencie a platnosti KC,
- privátne kľúče patriace k služobným certifikátom (napr. certifikáty patriace LRA a pod.),
- infraštruktúra (napr. dokumenty, procedúry, postupy, súbory, skriptá, heslá, pass frázy a pod.) slúžiaca na prevádzku CAMOSR, vrátane jej LRA,
- osobné údaje subjektov a žiadateľov o certifikát podliehajúce ochrane podľa zákona č. 18/2018 Z.z. o ochrane osobných údajov.

Za účelom náležitej správy certifikátov sa môže požadovať, aby sa pri správe certifikátov v rámci CAMOSR používali aj informácie, ktoré nie sú uvedené v certifikáte (napr. identifikačné čísla dokladov, adresy, telefónne čísla).

Ľubovoľná takáto informácia sa explicitne definuje v časti 3.1 tohto dokumentu. So všetkými informáciami uloženými v rámci CAMOSR, a nie v repozitári, sa má zaobchádzať ako s citlivými informáciami a prístup k nim má byť obmedzený len na osoby, ktoré tieto informácie nevyhnutne potrebujú na výkon svojich oficiálnych povinností.

Podmienkou na vydanie certifikátu podľa zákona č. 18/2018 Z. z. o ochrane osobných údajov je oboznámenie žiadateľa, že CAMOSR bude zo zákonných dôvodov uschovávať jeho osobné údaje, ktoré získala pri jeho registrácii. CAMOSR bude tieto údaje archivovať a spracovávať v rozsahu požadovanom zákonmi a vyhláškami, ktoré platia pre činnosť kvalifikovaných certifikačných autorít.

9.6.b Typy informácií, ktoré nie sú klasifikované ako dôverné

Zoznam zrušených certifikátov (ďalej len CRL) a OCSP nie sú klasifikované ako dôverné a považuje sa za verejnú informáciu.

Všetky informácie, ktoré sú zverejňované prostredníctvom repozitára, nie sú klasifikované ako dôverné a považujú sa za verejné.

9.6.c Kto bude oboznamovaný o zrušení certifikátu

CAMOSR prostredníctvom pracovníka LRA oboznámi o zrušení certifikátu držiteľa certifikátu alebo jeho splnomocnenca.

9.6.d Prípady, v ktorých sa dôverná informácia môže zverejniť

CAMOSR nezverejní žiadne informácie týkajúce sa žiadateľa o certifikát alebo držiteľa certifikátu žiadnej tretej strane, ak dané informácie nie sú považované za verejné.

CAMOSR musí s osobnými údajmi žiadateľov o certifikát alebo subjektov certifikátu zaobchádzať v súlade s platnými zákonmi a nesmie ich poskytnúť žiadnej tretej strane s výnimkou subjektov, ktoré zo zákona majú právo kontrolovať činnosť CAMOSR, a kompetentných štátnych orgánov ako sú polícia, súdy, prokuratúra.

Každá požiadavka na uvoľnenie informácií, ktoré nie sú považované za verejné, má byť autentizovaná a dokumentovaná.

9.7 Ochrana práv duševného vlastníctva

Vlastník CAMOSR je vlastníkom všetkých autorských práv na všetky dokumenty, dáta, procedúry, postupy, politiky, poriadky, certifikáty a privátne kľúče, ktoré sú súčasťou infraštruktúry CAMOSR a ktoré boli ním vytvorené.

9.8 Dodatočné testovanie

S ohľadom na špecifickosť skupiny užívateľov (zamestnanci rezortu MOSR), ktorým sú poskytované dôveryhodné služby, CAMOSR nezverejňuje testovacie certifikáty. Test zabezpečuje VÚ 8116.

9.9 Zmenové procedúry

CAMOSR si vyhradzuje právo v prípade potreby tento dokument aktualizovať alebo zrušiť.

PMA je orgán, ktorý s konečnou platnosťou schvaľuje znenie tohto dokumentu a jeho prípadné zmeny.

Chyby, požiadavky na aktualizáciu alebo navrhované zmeny tohto dokumentu sa majú oznámiť kontaktu uvedenému v časti 1.5. Takáto komunikácia musí obsahovať opis zmeny, zdôvodnenie zmeny a kontaktné údaje osoby, ktorá zmenu požaduje resp. navrhuje.

Všetky zmeny motivované PMA budú dané na vedomie subjektom, ktorých sa týkajú v lehote aspoň jedného mesiaca.

Každá zmenená verzia tohto dokumentu bude očíslovaná a evidovaná.

Oprava preklepov, gramatických a štylistických chýb, zmena kontaktných údajov sa nepovažujú za zmeny iniciujúce zmenu verzie tohto dokumentu.

Po uplynutí lehoty určenej na posúdenie návrhu na zmenu má PMA navrhovanú zmenu prijať, prijať s úpravou alebo odmietnuť.

9.10 Procedúry na zverejňovanie a upozornenie

CAMOSR bude publikovať informácie týkajúce sa tejto politiky (vrátane tejto politiky ako celku) prostredníctvom webu a v súlade s pravidlami organizácie týkajúcimi sa obsahu webu. Tento dokument bude k dispozícii tiež na každej LRA.

9.11 Procedúry na schvaľovanie

PMA urobí rozhodnutie, či dokument CPS je v súlade s touto politikou. Ešte pred začatím svojej prevádzky má mať CAMOSR schválený svoj dokument CPS a musí spĺňať všetky jeho požiadavky.

PMA je autorizovaná robiť rozhodnutia, či sú externé dokumenty CPS v súlade s touto politikou.

PMA má informovať o takýchto rozhodnutiach takým spôsobom, aby boli tieto informácie dobre prístupné stranám spoliehajúcim sa na certifikát.

9.12 Úľavy

PMA má rozhodnúť, či je odchýlka v praxi CAMOSR podľa aktuálnej politiky prijateľná alebo či je potrebné urobiť zmenu politiky.

PMA môže upustiť od niektorej požiadavky politiky, aby sa vyhovelo urgentným, nepredvídateľným prevádzkovým požiadavkám. Keď sa povolí úľava, PMA má toto zverejniť pomocou webu prístupného stranám spoliehajúcim sa na KC a má buď iniciovať trvalú zmenu do politiky, alebo má pre zmenšenie povinností stanoviť konkrétny časový limit.

ODKAZY

1. Zákon č. 272/2016 Z. z. o dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zmene a doplnení niektorých zákonov
2. IETF RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and certification Practices Framework, pozri https://tools.ietf.org/html/rfc3647
3. IETF RFC 3161 (2001): „Internet X.509 Public Key Infrastructure: Time-Stamp Protocol (TSP)“.
4. RFC 3628, November 2003 „Policy requirements for time-stamping authorities (TSAs)“
5. Recommendation ITU-T X.509 | ISO/IEC 9594-8 Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks, pozri http://www.itu.int/itu-t/recommendations/rec.aspx?rec=X.509
6. Nariadenie Európskeho parlamentu a Rady (EÚ) č. 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES, Nariadenie (EÚ) č. 910/2014 a Korigendum
7. SD Schéma dohľadu kvalifikovaných dôveryhodných služieb definovaná orgánom dohľadu, pozri http://ep.nbusr.sk/kca/tsl/SchemaDohladu.pdf
8. ETSI TS 102 023 V1.2.2 (2008-10) „Policy requirements for time-stamping authorities“
9. ETSI EN 319 411-2 V2.1.1 (2016-02) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trustservice providers issuing EU qualified certificates, pozri http://www.etsi.org/deliver/etsi_en/319400_319499/31941102/02.01.01_60/
10. ETSI EN 319 411-1 V1.1.1 (2016-02) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates;
11. ETSI EN 319 421 V1.1.1 (2016-03) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing Time-Stamps;
12. ETSI EN 319 422 V1.1.1 (2016-03) Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles;
13. Zákon č. 18/2018 Z. z. o ochrane osobných údajov