VOJENSKÝ ÚTVAR 9066
TRENČÍN

Č. p.: 6.spojp-EL 7/11-1-86/2025

Trenčín, 13. marec 2025
Výtlačok jediný.
Počet listov: 36

Schvaľujem:

Pravidlá na výkon certifikačných činností CAMOSR

„Verejný dokument“

Spracovateľ: Centrum IB / Úsek PKIaCA

Verzia: 5.1

Dátum platnosti: 17. APR. 2025

© 2025 Vojenský útvar 9066 TRENČÍN
6. spojovací pluk
Olbrachtova 5, 911 01 TRENČÍN
tel.: +421 960 40 79 89
e-mail: pki@mil.sk
web: http://pki.mil.sk

Všetky práva vyhradené.
Vytlačené v Trenčíne, Slovenská republika.

Informácie v tomto dokumente nesmú byť menené bez písomného súhlasu VÚ 9066 Trenčín.

Tento dokument neprešiel jazykovou úpravou.

Ochranné známky

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

História zmien

Verzia	Dátum	Opis revízie
0.1.	20.09.2005	prvý návrh – na pripomienkovanie
1.0.	25.10.2005	na schválenie
1.1.	14.11.2005	schválený
2.0.	17.10.2006	zrevidovaný
2.1.	11.09.2007	zrevidovaný
2.2.	15.03.2009	zrevidovaný, doplnený o LRA
2.3.	27.11.2009	aktualizovaný, zmena VÚ, aktualizované vyhlášky NBÚ
2.4.	03.05.2010	doplnenie LRA ZV
2.5.	01.03.2011	zrevidovaný
2.6.	19.08.2011	zrevidovaný
2.7.	25.07.2012	zrevidovaný
2.8.	04.03.2013	zrevidovaný
2.9.	25.03.2014	zrevidovaný
3.0.	22.06.2015	zrevidovaný
3.1.	02.05.2017	zrevidovaný, Nahradenie zákona 215/2003 zákonom 272/2016
4.0.	09.05.2018	zrevidovaný, nahradenie zákona 122/2013 zákonom 18/2018
4.1.	30.07.2018	Zrevidovaný
4.2.	07.05.2020	aktualizovaný, zmena SN a DigitalID pre CA, TSA a OCSP
4.3.	28.06.2021	zmena veľkosti kľúča pre kvalifikovaný certifikát na 4096 bitov
4.4.	13.07.2022	zrevidovaný
4.5	25.07.2023	zrevidovaný
5.0	03.07.2024	Upgrade infraštruktúry CAMOSR
5.1	13.03.2025	zrevidovaný

Obsah

Obsah 4
Obrázky 6
Tabuľky 6
Skratky a pojmy 7
Skratky 7
Pojmy 8
1. Úvod 10
1.1. Prehľad 10
1.2. Identifikácia 11
1.3. Komunita a použiteľnosť 12
1.4. Správa certifikačných poriadkov 15
1.5. Kontaktné údaje 16
2. Zverejňovanie informácií a úložiská 18
2.1. Zverejňovanie informácií o CA/RA 18
2.2. Periodicita publikovania informácií 18
2.3. Úložiská 19
3. Identifikácia a autentizácia 20
3.1. Iniciálna registrácia 20
3.2. Vydanie následného certifikátu 25
3.3. Vydanie následného certifikátu po zrušení certifikátu 25
3.4. Žiadosť o zrušenie certifikátu 25
4. Požiadavky na životný cyklus certifikátu 26
4.1. Žiadosť o vydanie certifikátu 26
4.2. Vydanie certifikátu 28
4.3. Prevzatie certifikátu 29
4.4. Zrušenie certifikátu 29
4.5. Audit bezpečnosti 34
4.6. Archivácia záznamov 34
4.7. Zmena kľúča 34
4.8. Havarijný plán 35
4.9. Ukončenie činnosti CAMOSR 36

5. Fyzické, procedurálne a personálne bezpečnostné opatrenia 37
5.1. Fyzické bezpečnostné opatrenia 37
5.2. Procedurálne opatrenia 37
5.3. Personálne bezpečnostné opatrenia 38
5.4. Postup získavania auditných záznamov 39
6. Technické bezpečnostné opatrenia 40
6.1. Generovanie páru kľúčov a inštalácia 40
6.2. Mazanie privátnych kľúčov CAMOSR 41
6.3. Ochrana privátneho kľúča 41
6.4. Manažment párových dát 42
6.5. Aktivačné údaje 42
6.6. Počítačové bezpečnostné opatrenia 42
6.7. Bezpečnostné opatrenia pre vývoj a riadenie bezpečnosti 44
6.8. Sieťové bezpečnostné opatrenia 44
6.9. Opatrenia pre kryptografické moduly 44
7. Profily certifikátov a zoznamov zrušených certifikátov 46
7.1. Profil certifikátu 46
7.2. Profil OCSP 56
7.3. Profil zoznamu zrušených certifikátov 56
8. Audit zhody 57
8.1. Frekvencia a periodicita auditu 57
8.2. Identita a kvalifikácia audítora a vzťah k auditovanému subjektu 57
8.3. Zoznam oblastí, ktoré sú predmetom auditu zhody 57
8.4. Zoznam opatrení realizovaných na základe výsledkov auditu 57
8.5. Výsledky auditu 58
8.6. Interný audit 58
9. Ostatné obchodné a právne náležitosti 59
9.1. Povinnosti 59
9.2. Právne záruky 62
9.3. Finančná zodpovednosť 63
9.4. Rozhodcovské konanie a riešenie sporov 64
9.5. Poplatky 64
9.6. Dôvernosť 64

9.7. Ochrana práv duševného vlastníctva 66
9.8. Dodatočné testovanie 66
9.9. Procedúry na zmenu špecifikácie 66
9.10. Procedúry pre zverejňovanie a upozornenie 66
9.11. Úľavy 67

Zoznam obrázkov a tabuliek

Obrázky

Tento dokument neobsahuje obrázky

Tabuľky

Tabuľka č. 1: Obsah položiek vo vlastnom certifikáte CAMOSR3 46
Tabuľka č. 2: Obsah položiek vo vlastnom certifikáte CAMOSR4 47
Tabuľka č. 3: Obsah položiek rozlišovacieho mena v KC 47
Tabuľka č. 4: Použité rozšírenia v KC 49
Tabuľka č. 5: Obsah položiek rozlišovacieho mena v KC pre elektronickú pečať 50
Tabuľka č. 6: Použité rozšírenia v KC pre elektronickú pečať 51
Tabuľka č. 7: Obsah položiek rozlišovacieho mena v KMC 52
Tabuľka č. 8: Použité rozšírenia v KMC 54
Tabuľka č. 9: Obsah položiek v certifikáte OCSP 55
Tabuľka č. 10: Použité rozšírenia v certifikáte OCSP 55
Tabuľka č. 11: Rozšírenia v OCSP odpovedi 56
Tabuľka č. 12: Použité rozšírenia (CRL extensions) v kvalifikovanom CRL 56

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 Regionálneho centra KIS, 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
CAMOSR X	–	Následník certifikačnej autority, poskytovateľa dôveryhodných služieb Ministerstva obrany Slovenskej republiky (X – poradové číslo následnej CA)
TSA	–	Time Stamp Authority (autorita časovej pečiatky)
QSCD	–	Kvalifikované zariadenie na vyhotovenie elektronického podpisu
DRKIS	–	Dozorný riadenia komunikačných a informačných systémov

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 sídel, 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 údajom 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 I 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 c) 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 vyhotovenie elektronického podpisu, ktoré spĺňa požiadavky stanovené v prílohe 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 definuje pravidlá na výkon kvalifikovaných certifikačných činností (Certificate Practice Statement, ďalej len CPS) pre kvalifikovanú certifikačnú autoritu vydávajúcu kvalifikované certifikáty (ďalej len certifikáty), ktorá vychádza z Certifikačného poriadku CAMOSR.

Certifikačný poriadok je dostupný na http://pki.mil.sk OID {**1.3.158.30845572.1.7.3.1**}.

Pravidlá na výkon certifikačných činností CAMOSR sú dostupné na https://pki.mil.sk OID {**1.3.158.30845572.1.7.3.3**}.

Pravidlá na výkon služby poskytovania časovej pečiatky CAMOSR sú dostupné na https://pki.mil.sk OID {**1.3.158.30845572.1.7.3.2**}.

1.1. Prehľad

Táto CPS predstavuje pravidlá na výkon poskytovania dôveryhodných služieb (časť týkajúcu sa vlastnej certifikačnej autority), na základe ktorých je zriadený a prevádzkovaný poskytovateľ dôveryhodných služieb Ministerstva obrany Slovenskej republiky CAMOSR.

CPS bola vytvorená 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“) a v súlade so zákonom č. 272/2016 Z.z o dôveryhodných službách. Týka sa 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**
- **certifikátov pre službu OCSP, kde súkromný kľúč je uložený na HSM**
- **certifikátov pre službu časovej pečiatky, kde súkromný kľúč je uložený na HSM**
- **časových pečiatok**

Tento dokument definuje vytváranie a správu certifikátov s verejnými kľúčmi podľa štandardu X.509 verzie 3 pre ich použitie v aplikáciách vyžadujúcich si kvalifikované certifikáty.

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

Názov	**Sériové číslo certifikátu**	**Vydavateľ**	**DigitalID (SHA-256) v SK dôveryhodnom zozname**
CAMOSR3	0860	KCA NBU SR 3	3031300D06096086480165030402010500042054116 6F8326C1C4DB6C769AA82D5F26D7656BAA19B190 9EB0EDAC93D0CFD599E
CAMOSR4	00feb3b8f7b 0abf0f1b031	Self-Signed	3051300D06096086480165030402030500044 03F78C2501407945102CD61BC22C1EB951817B8314 DBB0AE928631EC1CF89353484F3479F4678C3CD8 7C97A90BCA9934F396D3B871850220617D33ED6D 069D7E9
tsa.mil.sk	4e 4f 91 35 d2 f9 6a 73 4d 41	Self-Signed	3031300D06096086480165030402010500042064 55C6AE6E503444E443E1802138543FA0D1F42F38E4BC C6C096C39279630659
OCSP	01 c0 9e 22 97 0f 00 00 00 00 00 00 00 00 cf	CAMOSR3	3031300D06096086480165030402010500042020042 DCF494868E87717A5E60548F9C98839584CCD505 D57C18632FDC071A5AB
OCSP	0112e0cec1 3200000000 0000000001	CAMOSR4	3051300D06096086480165030402030500044 0EC0ED215B853C87CB20676E9BA727926FA50FC79 DBC50DCB6AC6710A63CEC171D3D008C1A904E84 940C4BFCC61AACF22D446019F7B0CBB76A7E2D2 818C6C383A

1.2. Identifikácia

Názov:	**Pravidlá na výkon certifikačných činností CAMOSR - verejný**
Skratka názvu:	**CPS CAMOSR - verejný**
Verzia:	**5.1 - Marec 2025**
Tomuto dokumentu je priradený identifikátor objektu (OID):	**1.3.158.30845572.1.7.3.3**

Pojmom KC resp. KC CAMOSR sa v tomto dokumente označuje kvalifikovaný certifikát vydaný kvalifikovanou certifikačnou autoritou poskytovateľa 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. 3.158.30845572.1.7.3.3 - CPS CAMOSR

1.3. Komunita a použiteľnosť

1.3.a. Autority

Autorita pre správu poriadkov

Autorita pre správu poriadkov (Policy Management Authority) (ďalej ako 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 CPS CAMOSR, aby sa zaručilo, že prax CAMOSR vyhovuje príslušnému certifikačnému poriadku,
- revízie CPS TSA CAMOSR, aby sa zaručilo, že prax CAMOSR vyhovuje príslušnému certifikačnému poriadku,
- revízie výsledkov auditov, aby sa určilo, či CAMOSR adekvátne dodržiava ustanovenia schváleného dokumentu CPS,
- vydávanie odporúčaní pre CAMOSR ohľadne nápravných akcií a iných vhodných opatrení,
- riadenia a usmerňovania činnosti vlastných certifikačných a registračných autorít,
- na požiadanie robí výklad ustanovení CPS a svojich pokynov pre CAMOSR a RA,
- vykonáva funkciu audítora, prípadne touto činnosťou poverí samostatného pracovníka,

- vykonávania revízie CPS CAMOSR prostredníctvom analýzy CPS, 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.

Zriaďovateľ CAMOSR

Zriaďovateľ CAMOSR (ďalej len „zriaďovateľ“) predstavuje zložku, ktorá s konečnou platnosťou schvaľuje politiky CAMOSR a je zodpovedná za komunikáciu s orgánom dohľadu za CAMOSR.

Vlastná certifikačná autorita

Vlastná certifikačná autorita je entita autorizovaná PMA na vytváranie, podpisovanie a vydávanie kvalifikovaných certifikátov 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 služieb špecifikovaných v bode 1.1.

CAMOSR je zodpovedná za všetky aspekty vydávania a správy certifikátov, vrátane kontroly nad procesom registrácie, procesom identifikácie a autentizácie, procesom vytvárania, publikácie, zrušovania certifikátov. CAMOSR zaručuje, že všetky aspekty jej služieb a operácií a infraštruktúry zviazanej s certifikátmi vydanými podľa tejto CPS sa vykonávajú v súlade s požiadavkami a ustanoveniami jej pravidiel na výkon poskytovania kvalifikovaných dôveryhodných služieb.

CAMOSR je implementovaná prostredníctvom týchto entít:

- vlastná CA – entita, ktorá vykonáva správu CA, jej aktivitami a všetkými aspektmi činnosti sa zaoberá tento dokument,
- registračná autorita – 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 Centra 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).

1.3.b. Koncové entity

Subjekty, žiadatelia a držitelia certifikátu

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 byť 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 spĺňajú 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.

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 certifikáte. 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 podpisu overeného daným certifikátom.

Typy certifikátu

CAMOSR vydáva KC pre kvalifikovaný elektronický podpis, KC pre kvalifikovanú elektronickú pečať a certifikát pre OCSP 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 verejným kľúčom bol bezpečným spôsobom vygenerovaný a uschovaný na

bezpečnom zariadení (QSCD), ktoré sa nachádza v zozname certifikovaných kvalifikovaných zariadení na vyhotovovanie elektronických podpisov, ktorý zverejňuje NBÚ na svojom webovom sídle.

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.

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

Certifikát TSA, kde súkromný kľúč sa nachádza v HSM je vygenerovaný za účelom poskytovania služby 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 certifikačných poriadkov

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

1.4.a. Postup schvaľovania CPS a externej politiky

Ešte pred začiatkom prevádzky musí mať CA schválený svoj CP a CPS a musí spĺňať všetky jeho požiadavky. Obsah CP a CPS schvaľuje zriaďovateľ.

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

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

Pre zefektívnenie schvaľovacieho procesu dokumentácie CAMOSR, boli dokumenty rozdelené na dve skupiny:

- dokumenty, ktorých platnosť schvaľuje zriaďovateľ,
- prevádzkovú dokumentáciu, ktorá podlieha častejším zmenám a schvaľuje ju PMA.

Dokumenty schvaľované zriaďovateľom:

Interné údaje prevádzkovateľa CAMOSR.

Dokumenty schvaľované PMA:

Interné údaje prevádzkovateľa CAMOSR.

1.5. Kontaktné údaje

Zriaďovateľom a prevádzkovateľom CAMOSR je Ministerstvo obrany Slovenskej republiky.

1. Kontaktné údaje Certifikačnej autority MOSR

   Adresa: **VÚ 9066 Trenčín**
   Certifikačná autorita MOSR (CAMOSR)
   Olbrachtova 5
   911 01 Trenčín

2. Kontaktné údaje LRA Trenčín

   Adresa: **VÚ 9066 Centrum KIS ZÁPAD**
   Lokálna registračná autorita MOSR (LRAMOSR)
   Partizánska 3732
   911 01 Trenčín

3. Kontaktné údaje LRA Bratislava

   Adresa: **VÚ 9066 Centrum KIS JUH**
   Lokálna registračná autorita MOSR (LRAMOSR)
   Za kasárňou 5

Bratislava

4. Kontaktné údaje LRA Zvolen

Adresa: **VÚ 9066 Centrum KIS STRED**
Lokálna registračná autorita MOSR (LRAMOSR)
Borovianska cesta 1
960 01 Zvolen

5. Kontaktné údaje LRA Prešov

Adresa: **VÚ 9066 Centrum 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 - repozitára držiteľom certifikátov a stranám spoliehajúcim sa na certifikát nasledujúce informácie:

- aktuálne CRL, predchádzajúce CRL sú poskytované iba na vyžiadanie,
- certifikát CAMOSR (patriaci k jej podpisovému kľúču).

Okrem toho CAMOSR bude zverejňovať na Internete v on-line režime prostredníctvom svojho webu „Certifikačný poriadok 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 služieb KC. 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 CRL je 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. Úložiská

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.

3. Identifikácia a autentizácia

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 uvedené v zozname certifikovaných kvalifikovaných zariadení 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 spravidla priraďuje pre žiadateľov o certifikát rozlišovacie mená v zmysle X.500

(X.500 Distinguished Name, ďalej len ako rozlišovacie meno).

Žiadatelia o certifikát si spravidla sami nezvolia rozlišovacie meno, ktoré má byť v ich certifikáte. Hodnoty jednotlivých položiek zvoleného rozlišovacieho mena musia byť v súlade s ustanoveniami tohto dokumentu.

Povinne vyplnené položky s definovaným obsahom sú C= SK, O= Ministry of Defence.

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 má zaručovať, 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 RA.

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

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 emailovej adresy sa zadáva prostredníctvom aplikácie RA Client.

Jednoznačnosť mien

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

CAMOSR prostredníctvom RA musí presadzovať jednoznačnosť mien v rámci celého menného priestoru, aby nedošlo k neprijateľným menným duplicitám.

Podľa zákona č. 272/2016 Z. z. je potrebné, ak sa v styku s orgánmi verejnej moci používal 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 kvalifikovaného certifikátu (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, CAMOSR zjedná čo najrýchlejšie nápravu.

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

3.1.c. Preukazovanie vlastníctva privátneho kľúča

Privátny kľúč je bežne generovaný na pracovisku LRA pred vydaním certifikátu priamo na QSCD.

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. Všetky páry kľúčov a im zodpovedajúce žiadosti o certifikát sa musia generovať priamo v QSCD, HSM.

Žiadna zložka CAMOSR v nijakom prípade nearchivuje žiadne privátne kľúče patriace žiadateľom – cudzím subjektom.

Autentizácia identity právnickej osoby (organizácie)

Identita právnickej osoby sa bude autentizovať na základe názvu právnickej osoby, iného identifikačného údaja, ak taký existuje (spravidla je to napr. IČO), adresy a dôkazu existencie danej právnickej osoby (spravidla výpisom z obchodného registra).

LRA bude overovať tieto údaje a okrem autentickosti žiadajúcej osoby sa bude overovať, že daná osoba má právo jednať v mene danej právnickej osoby v danej veci.

Právnická osoba musí byť registrovaná na území Slovenskej republiky a musí preukázať svoju totožnosť výpisom z obchodného registra nie starším ako tri mesiace.

Právnická osoba musí spadať do organizačnej štruktúry Ministerstva obrany SR alebo Generálneho štábu ozbrojených síl SR.

Fyzické osoby (jedna alebo viac, podľa predloženého výpisu z obchodného registra), ktoré na základe predloženého výpisu z obchodného registra konajú na LRA za danú právnickú osobu, 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 podložený pracovnou zmluvou,
- úradne overenej plnej moci, ak daná fyzická osoba nemá pracovno-právny vzťah podložený pracovnou zmluvou k právnickej osobe, v mene ktorej koná

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

V prípade, že právnická osoba nemôže preukázať svoju totožnosť výpisom z obchodného registra, musí takáto právnická osoba písomne preukázať okrem svojej totožnosti aj legálnosť (resp. „dôvod“) svojej existencie (s využitím a poukázaním na zákon alebo iný predpis, ktorý o subjekte daného typu pojednáva).

Autentizácia identity fyzickej osoby

Fyzickou osobou je osoba organizačne spadajúca pod Ministerstvo obrany SR alebo Generálny štáb ozbrojených síl SR.

Fyzická osoba musí preukázať svoju totožnosť dvomi z týchto osobných dokladov, pričom minimálne jeden musí obsahovať fotografiu fyzickej osoby, jej rodné číslo a adresu trvalého bydliska:

- občiansky preukaz,
- služobný preukaz profesionálneho vojaka,
- cestovný pas,
- vodičský preukaz,
- rodný list,
- zbrojný preukaz,
- kartičku poistenca.

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.

Ak fyzická osoba zastupuje na LRA inú fyzickú osobu, musí sa navyše preukázať úradne overeným (notárom alebo matrikou) plnomocenstvom, z textu ktorého jednoznačne vyplýva, 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.

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.

Kontrola údajov na predložených dokladoch

V prípade ľubovoľných odôvodnených pochybností o totožnosti žiadateľa môže LRA jeho registráciu odmietnuť. Pracovník LRA kontroluje na predložených dokladoch najmä nasledovné:

Osobné doklady fyzickej osoby:

a) platnosť predloženého dokladu

Upozornenie: V prípade neplatného osobného dokladu sa postupuje ako pri chýbajúcom osobnom doklade - RA registráciu odmietne

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

Upozornenie: Ak áno, RA môže odmietnuť registráciu.

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

e) či výpis nie je starší ako 3 mesiace

f) 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)

g) či je výpis úradne overený (notárom alebo matrikou), ak sa nejedná o originál

Poznámka. Výpis z obchodného registra získaný z Internetu je pri konaní na RA nepoužiteľný.

Plnomocenstvo:

h) či je plnomocenstvo úradne overené (notárom alebo matrikou)

i) či sa údaje, uvedené v plnomocenstve, ktoré definujú 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

j) rozsah plnomocenstva - t.j. či plnomocenstvo oprávňuje splnomocnenú fyzickú alebo právnickú osobu k požadovanému úkonu na RA v mene splnomocňujúcej fyzickej alebo právnickej osoby

k) či plnomocenstvo nie je časovo obmedzené alebo ak obsahuje inú podmienku, či je táto splnená

Druh predložených dokladov (napr. občiansky preukaz, pas) a príslušné údaje z nich zaznamená pracovník RA na príslušný formulár, ktorý zostáva na RA.

3.2. Vydanie následného certifikátu

Pre vydanie následného certifikátu platia rovnaké podmienky ako v prípade prvotnej registrácie.

3.3. Vydanie následného certifikátu po zrušení certifikátu

V každom prípade subjekt sa po zrušení certifikátu musí podrobiť všetkým požiadavkám prvotnej registrácie.

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

Páry kľúčov pre certifikát na služobné účely (napr. pre Administrátora CA, Operátora CA a pod.) si daný subjekt generuje vo svojom pridelenom QSCD, tzn. privátny kľúč nebude možné zálohovať a všetky kryptografické operácie s ním sa budú realizovať priamo na zariadení.

Certifikát na služobné účely (napr. pre Administrátora CA, Operátora CA a pod.) sa vždy vydáva technologickou certifikačnou autoritou ako technologický certifikát pre danú konkrétnu osobu, ktorá zastáva príslušnú úroveň (role).

Všetka 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, ktoré sa majú chrániť použitím predtým vydaných certifikátov. Ľubovoľný elektronický prenos zdieľaných tajomstiev musí byť uskutočnený šifrovane.

Žiadosť o vydanie certifikátu je generovaná v aplikácií RA client automaticky v priebehu výdaja certifikátu, pred samotným výdajom je potrebné poučiť žiadateľa o spracovaní osobných údajov.

4.1.a. Detailný postup na získanie certifikátu

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

1. Oboznámi sa s týmto postupom, prípadne s princípmi a návodmi pre získanie certifikátu.

2. Subjekt si pripraví hodnoty jednotlivých položiek žiadosti o certifikát tak, aby tieto hodnoty boli v súlade s týmto dokumentom.

Poznámka:	Pri zadávaní hodnôt do položiek žiadosti o certifikát 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. Všetky údaje sa musia zadávať bez diakritiky (mäkčene, dĺžne a pod.).

3. Pripraví si zvolené doklady totožnosti resp. iné potrebné doklady, napr. výpis z obchodného registra (odporúčame overiť platnosť dokladov) podľa ustanovení časti 3.1.d

Poznámka:	Je potrebné, aby si žiadateľ o certifikát, resp. subjekt certifikátu pripravil kópie (nemusia byť overené) všetkých dokladov (okrem osobných dokladov fyzických osôb), ktoré mieni predložiť na RA (napr. výpis z obchodného registra a iné doklady o právnickej osobe, plnomocenstvo, ak sa dá zastupovať na RA), aby ich mohol odovzdať na RA. Výpis z obchodného registra získaný z Internetu nie je postačujúci, nakoľko má len informatívny charakter a nie je použiteľný na právne úkony.

Odporúčanie: Odporúča sa, aby si žiadateľ o certifikát, resp. subjekt certifikátu ešte pred návštevou LRA overil a vyjasnil prípadné pochybnosti a problémy, najmä tie, ktoré sa týkajú vhodnosti hodnôt jednotlivých položiek v žiadosti o certifikát.

4. Dohodne si termín návštevy RA.
5. V dohodnutom termíne príde na RA, pričom vezme so sebou a predloží:
   - zvolené doklady totožnosti resp. iné potrebné doklady, napr. výpis z obchodného registra, plnomocenstvo atď.,

4.1.b. Postup pri registrácii žiadateľa o certifikát, resp. subjektu certifikátu na LRA

1. Pracovník RA overí totožnosť subjektu resp. žiadateľa o certifikát, ktorý ho zastupuje.
2. Po overení totožnosti sa prostredníctvom aplikácie RA Client vygeneruje v QSCD žiadateľa (jeho čipovej karte) nová žiadosť o certifikát vo formáte PKCS#10. Žiadosť o certifikát sa generuje priamo na RA pod dohľadom pracovníka LRA. Ak je žiadosť generovaná v HSM nie je potrebné túto generovať na pracovisku LRA.

Upozornenie: Žiadosť o certifikát resp. v nej sa nachádzajúci verejný kľúč, pre ktorý už bol vydaný certifikát, nemôže byť z bezpečnostných dôvodov použitá opakovane na vydanie iného certifikátu a bude na RA odmietnutá!

Poznámka: Žiadosť musí obsahovať vhodne vyplnené položky v súlade s tabuľkou "Položky rozlišovacieho mena kvalifikovaného certifikátu" uvedenou v časti 7.

3. 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.
4. Položky ST (stateOrProvinceName (názov kraja)), L (localityName („Mesto“)), OU (organizationUnitName ("Útvar vo firme")) a Email adresa sú nepovinné.
5. Ostatné položky žiadosti o certifikát **musia byť povinne vyplnené v zmysle jednotlivých profilov certifikátov.**
6. 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, RA žiadosť o certifikát odmietne prijať z bezpečnostných dôvodov, lebo už raz certifikovaný verejný kľúč nemôže byť použitý v inom certifikáte.
7. 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". Formulár je k dispozícii na LRA alebo ho je možné skopírovať z webu http://pki.mil.sk. Jedna kópia zostáva žiadateľovi.

Upozornenie: Žiadateľ o certifikát musí na RA uspokojivým spôsobom preukázať všetky údaje, ktoré zadal do jednotlivých položiek žiadosti o certifikát. Ak žiadateľ 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 RA 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. Výpis z obchodného registra získaný z Internetu nie je postačujúci, nakoľko má len informatívny charakter a nie je použiteľný na právne úkony. Ak je v položke CN (commonName (Meno a priezvisko)) uvedený aj jeden alebo viacero titulov (napr. Ing., Mgr., CSc. a iné), použitie titulu v žiadosti o certifikát sa akceptuje, ak sa použité tituly nachádzajú v aspoň jednom z predložených osobných dokladov patriacich subjektu certifikát. V opačnom prípade je žiadateľ povinný RA preukázať oprávnenosť použitia každého uvedeného titulu predložením originálu alebo úradne overenej kópie diplomu, alebo iného dokumentu, ktorý potvrdzuje, že daná osoba má právo používať daný titul. LRA odmietne žiadosť o certifikát, ktorá obsahuje uvedenie titulu, ktorý žiadateľ nevie dokladovať vyššie uvedeným spôsobom.

Z dôvodu archivácie všetky doklady v tlačenej forme bude RA odosielať na CAMOSR stanoveným spôsobom v definovaných periódach.

4.1.c. Doručenie verejného kľúča žiadateľa o certifikát vydavateľovi certifikátu

Verejné kľúče (obsiahnuté v žiadostiach o certifikát) sa musia generovať v bezpečnom zariadení na pracovisku RA, aby sa garantovala väzba overenej identity žiadateľa k verejnému kľúču, ktorý sa certifikuje, toto neplatí ak je kľúč generovaný v HSM. Verejný kľúč generovaný v HSM je dodaný vo formáte PKCS#10.

4.1.d. Certifikát pre pracovníka CAMOSR

Služobný certifikát pre LRA sa vždy vydáva ako technologický certifikát na dané konkrétne pracovisko LRA pre konkrétnu osobu, ktorá zastáva určitú úroveň (rolu) RA na danom pracovisku LRA. Príslušnosť k role pracovník CAMOSR preukazuje záznamom v dokumente „Rozdelenie rolí CAMOSR - menný zoznam“. Daný dokument je schvaľovaný PMA a výhradne na jeho základe je možné použitie certifikátu v systéme CAMOSR. Priradenie príslušných oprávnení vykoná Administrátor systému CA prostredníctvom SwacaManagementPortalu.

4.2. Vydanie certifikátu

Splnením podmienok spojených s identifikáciou, autentifikáciou a generovaním žiadosti bude certifikát vydaný prostredníctvom aplikácie RA Client, pracovník LRA zabezpečí potrebnú dokumentáciu potrebnú na ukončenie procesu výdaja certifikátu.

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).

4.3. Prevzatie certifikátu

CAMOSR bude vydávať certifikát v režime on-line, tzn. žiadateľ spravidla bude môcť prevziať vydaný certifikát v rámci jednej návštevy RA, 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 QSCD 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 definovaným v certifikáte už nepovažuje za platnú.

CAMOSR je zo zákona povinná zrušiť certifikát, ktorý spravuje, v nasledovných 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,
- vlastník certifikátu si nesplnil povinnosť požiadať o zrušenie certifikátu po skončení pracovného pomeru v rezorte MOSR,
- zistí, že certifikácia QSCD bola zrušená/odobratá. V takom prípade PMA rozhodne o zrušení všetkých KC vydaných na QSCD, ktorého certifikácia bola zrušená/odobratá a zabezpečí prevydaj všetkých platných KC na QSCD s aktuálne platnou certifikáciou.

Vždy, keď sa CAMOSR dozvie o niektorej z vyššie uvedených okolností, daný certifikát sa zruší a dá sa na zoznam zrušených certifikátov (CRL).

Zrušené certifikáty sa budú vyskytovať na všetkých nových vydaniach CRL.

4.4.b. Kto môže žiadať o zrušenie certifikátu

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

O zrušenie certifikát 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 je generovaná aplikáciou RA Client, certifikát môže zrušiť vettor podľa príslušnej LRA v pracovnej dobe. Mimopracovnú dobu rieši pohotovosť PKI. V prípade, že žiadateľ nepožiadal o zrušenie certifikátu osobne, operátor môže zrušiť certifikát len pomocou autentifikačného hesla uvedeného v zmluve o výdaji certifikátu.

Žiadosť o zrušenie certifikátu môže oprávnená osoba podať na LRA prostredníctvom 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.

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.

Pracovník 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.

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 Kontaktné údaje v bode 6 obyčajný mail (t.j. mail nemusí obsahovať el. dokument podpísaný (kvalifikovaným 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 žiadateľ o zrušenie certifikátu požaduje zrušiť certifikát ku konkrétnemu dátumu, uvedie to pri podaní žiadosti o zrušenie kvalifikovaného certifikátu (telefonicky, písomne, faxom, mailom). K tejto žiadosti sa následne vytvorí servisná požiadavka, ktorá bude vybavená k požadovanému dátumu.

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 Kontaktné údaje v bode 6), táto povinnosť patrí osobe, ktorá žiadosť o zrušenie certifikátu vložila do aplikácie RA Client.

Následne výtlačok č. 1 Žiadosť o zrušenie 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 RA Client resp. informačného systému CAMOSR, aby sa mohlo vykonať zrušenie certifikátu, tzn. aby sa certifikát dostal na najbližšie CRL.

CAMOSR zruší certifikát najneskôr do 24 hodín od momentu prijatia náležitej žiadosti o zrušenie certifikátu na LRA.

Certifikát možno zrušiť ihneď prostredníctvom pohotovosti PKI v prípade splnenia požadovanej autentifikácie.

4.4.e. Určenie periodicity publikovania zoznamu zrušených certifikátov

Administrátor CAMOSR nastaví systém tak, aby bolo CRL vydané každé 4 hodiny s platnosťou na 24 hodín a to aj vtedy, ak od vydania posledného CRL nedošlo k zrušeniu žiadneho certifikátu ani k žiadnej zmene v stave jednotlivých certifikátov. Interval výdaja CRL je definovaný službou whisper.

CAMOSR zverejňuje aktuálny zoznam zrušených kvalifikovaných certifikátov a všetky predchádzajúce zoznamy zrušených kvalifikovaných certifikátov na svojej internetovej stránke (webe).

CAMOSR archivuje všetky CRL, ktoré vydala.

4.4.f. Požiadavky používateľov certifikátov na sledovanie zoznamu zrušených certifikátov (CRL)

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 dokumentu.

4.4.g. Overenie aktuálneho stavu certifikátu

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

CAMOSR pri poskytovaní informácií overenia aktuálneho stavu certifikátu zabezpečí:

- dostupnosť informácií overenia aktuálneho stavu certifikátu 24 hodín denne, 7dní v týždni. V prípade poruchy systému, služby alebo iných nepredvídateľných okolností, ktoré CAMOSR nemá pod kontrolou, CAMOSR zabezpečí obnovu dostupnosti služby overenia aktuálneho stavu certifikátov do 24 hodín,

- bezpečnosť integrity a autenticity informácie o aktuálnom stave certifikátu,

- dostupnosť informácií overenia aktuálneho stavu certifikátu aj po období platnosti certifikátu,

- prítomnosť X.509 rozšírenia „*ExpiredCertsOnCRL*“ v CRL, ktoré obsahuje exspirované certifikáty,

- prítomnosť rozšírenia „*ArchiveCutOff*“ pre OCSP s dátumom „*archiveCutOff*“ nastaveným na hodnotu času a dátumu certifikátu CA „*notBefore*“,

- aktuálnosť a konzistentnosť informácií overenia aktuálneho stavu certifikátu pre všetky spôsoby overenia aktuálneho stavu certifikátu. Pri okamžitej aktualizácií OCSP je dovolený rozdiel medzi OCSP a CRL do nasledujúceho vydania CRL,

- verejnú a medzinárodnú dostupnosť informácií overenia aktuálneho stavu certifikátu.

Ak sa CAMOSR rozhodne alebo je povinná zrušiť CRL (podľa podmienok uvedených v ETSI EN 319 411-2, CSS-6.3.10-07), vydá a zverejni v príslušných distribučných CRL bodoch posledné CRL s hodnotou poľa *nextUpdate* „99991231235959Z“. CAMOSR nevydá posledné CRL, pokiaľ všetkým KC v rozsahu CRL nevyprší platnosť alebo nebudú revokované.

Ak platnosť certifikátu CAMOSR čoskoro vyprší, môže sa vypočítať posledná odpoveď OCSP pre každý vydaný certifikát s hodnotou poľa *nextUpdate* „99991231235959Z“.

Administrátor CAMOSR zabezpečí kontrolu monitoringu CRL. V prípade zlyhania publikácie CRL zabezpečí túto prostredníctvom pracovnej pohotovosti.

V prípade kompromitácie privátneho kľúča CAMOSR je CRL rovnako považované za kompromitované a CAMOSR nebude vydávať ďalšie CRL. CAMOSR bude v takomto prípade postupovať podľa bodu 4.8.c.

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.

4.5. Audit bezpečnosti

Interné údaje prevádzkovateľa CAMOSR.

4.6. 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.

RA odosiela na archiváciu pravidelne a stanoveným spôsobom všetky dokumenty (napr. zmluvy a prílohy k nim, vyplnené formuláre, kópie výpisov z obchodného registra, plnomocenstvá a pod.) patriace k jednotlivým certifikátom, ktoré boli vydané resp. spravované jej prostredníctvom.

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

Modifikovanie alebo odstraňovanie archivovaných informácií nie je prípustné.

Je zabezpečená dôvernosť a integrita archivovaných záznamov a médií.

4.7. Zmena kľúča

Celý proces musí prebehnúť bez negatívneho vplyvu na úroveň zabezpečenia.

K zmene kľúčov CAMOSR môže dôjsť z dvoch príčin:

- Blíži sa čas ukončenia platnosti (expirácie) aktuálne používaných kľúčov CAMOSR: toto je normálny stav – 2 roky pred uplynutím platnosti doteraz používaného páru kľúčov CAMOSR na webe CAMOSR sa zverejní oznam o blížiacej sa zmene kľúčov CAMOSR. Po tom čo sa vygeneruje nový kľúčový pár a certifikát CAMOSR je certifikát podrobený procesu udelenia kvalifikovaného štatútu od NBÚ. Až po udelení kvalifikovaného štatútu a pridaní nového certifikátu na Trust List EU sa zverejní nový certifikát

CAMOSR. Každý ďalší vydaný (nový) 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 certifikát CAMOSR ako aj všetky certifikáty podpísané použitým kompromitovaným kľúčom. 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. Po tom čo sa vygeneruje nový kľúčový pár a certifikát CAMOSR je certifikát podrobený procesu udelenia kvalifikovaného štatútu od NBÚ. Až po udelení kvalifikovaného štatútu a pridaní nového certifikátu na Trust List EU sa zverejní nový certifikát CAMOSR. Každý ďalší vydaný (nový) certifikát a CRL bude podpísaný novým súkromným kľúčom CAMOSR.

Zmena kľúčov osôb v dôveryhodných úrovniach (role) sa nevykonáva – v prípade potreby zmeny kľúča je nutné postupovať rovnako ako v prípade potreby vydania nového certifikátu (resp. následného certifikát).

4.8. Havarijný plán

Interné údaje prevádzkovateľa CAMOSR.

4.8.a. Poškodenie výpočtových zdrojov

Interné údaje prevádzkovateľa CAMOSR.

4.8.b. Zrušenie certifikátu CAMOSR

Interné údaje prevádzkovateľa CAMOSR.

4.8.c. Kompromitácia súkromného kľúča CAMOSR

Interné údaje prevádzkovateľa CAMOSR.

4.8.d. Prírodná katastrofa

Interné údaje prevádzkovateľa CAMOSR.

4.9. Ukončenie činnosti CAMOSR

Ešte pred ukončením poskytovania služieb sa vykoná:

- CAMOSR patričným spôsobom, minimálne 3 mesiace vopred, oznámi informácie o plánovanom ukončení svojej činnosti NBÚ, držiteľom všetkých ňou vydaných platných kvalifikovaných certifikátov, stranám spoliehajúcim sa na certifikáty a verejnosti. Toto oznámenie sa vykoná prostredníctvom webu CAMOSR, elektronickej pošty, obyčajnej pošty, registračných autorít, prípadne elektronických médií a tlače.
- Ukončia sa všetky mandátne zmluvy, splnomocnenia a pod., na základe ktorých mohli konať v mene CAMOSR (napr. poskytovať služby RA).
- Ďalej sa postupuje podľa § 4 ods. 2 zákona č. 272/2016 Z. z.. 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 RA aj ostatných zložiek CAMOSR sa sústredia a archivujú podľa platného registratúrneho poriadku.
- Vykonanie kontroly dodržania zákona o ochrane osobných údajov.

Po ukončení svojej činnosti CAMOSR nevydá žiaden certifikát a zabezpečí preukázateľné zničenie podpisových dát (privátneho kľúča) CAMOSR za prítomnosti aspoň troch poučených osôb určených PMA, spravidla osôb zastávajúcich služobné úrovne (role).

Do Prevádzkovej knihy udalostí CAMOSR sa vykoná príslušný podrobný záznam.

V deň ukončenia činnosti Administrátor CA vykoná úplné zálohy všetkých zariadení IS CAMOSR, dáta eviduje a archivuje minimálne 10 rokov v zmysle platného registratúrneho poriadku.

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

Až do skončenia svojej činnosti sa podieľa RA na základe prijatých pokynov na informovaní verejnosti.

Pred ukončením svojej činnosti RA poskytne archivované dáta, svoju korešpondenciu a dokumenty (napr. zmluvy a prílohy k nim, vyplnené formuláre, kópie výpisov z obchodného registra, plnomocenstvo a pod.) patriace k jednotlivým certifikátom, ktoré boli vydané resp. spravované jej prostredníctvom, určenej zložke CAMOSR podľa pokynu PMA.

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. Fyzické bezpečnostné opatrenia

Interné údaje prevádzkovateľa CAMOSR.

5.2. Procedurálne opatrenia

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.

Pre všetky služobné úrovne (role), ktoré kľúčovým spôsobom vplývajú na poskytovanie certifikačných služieb, sú zavedené procedúry a postupy popísané v príručkách používateľa a smerniciach pokrývajúcich príslušné činnosti.

Pri práci s HSM resp. privátnym kľúčom CAMOSR, ktorý je v ňom uložený používajú všetky oprávnené osoby na svoju autentizáciu svoje administrátorské resp. operátorské karty patriace k HSM.

Osoby zastávajúce služobné úrovne (role) sa autentizujú pri práci na zariadeniach (počítačoch, telekomunikačných zariadeniach a pod.) vlastnej CA resp. RA prostredníctvom im patriacich hesiel do príslušného operačného systému a/alebo aplikácie.

Pri použití privátneho kľúča patriaceho k ich certifikátu sa autentizujú pomocou svojho tokenu a hesla pre prístup k svojmu privátnemu kľúču uloženému na danom tokene.

Pre úroveň (rola) RA, ktorá kľúčovým spôsobom vplýva na poskytovanie kvalifikovaných dôveryhodných služieb, sú zavedené procedúry a postupy popísané v príručkách používateľa a smerniciach pokrývajúcich príslušné činnosti RA.

Každá LRA, ktorá funguje podľa tohto dokumentu, je predmetom jeho ustanovení. Zodpovednosťou RA je v prvom rade:

- overovanie identity buď prostredníctvom osobného kontaktu s osobou – subjektom certifikátu alebo prostredníctvom zastupujúcej osoby,
- zaznamenávanie informácií od žiadateľov o certifikát a overovanie ich správnosti,

- zber, uschovávanie a odosielanie dokumentov a vyplnených formulárov patriacich k jednotlivým certifikátom,
- vkladanie prijatých žiadostí o certifikát do aplikácie RA client a informačného systému CAMOSR,
- odovzdávanie vydaných certifikátov žiadateľom,
- prijímanie žiadostí o zrušenie certifikátov a ich vkladanie do aplikácie RA client,
- komunikácia s CAMOSR,
- vedenie požadovanej dokumentácie RA,
- komunikácia so žiadateľmi o certifikát, držiteľmi certifikátu a verejnosťou a dokumentovanie tejto komunikácie.

Ďalšie podrobnejšie informácie, nastavenia v rámci procedurálnej bezpečnosti, prístupu k systémom sú obsiahnuté v bezpečnostnej dokumentácii CAMOSR.

5.3. Personálne bezpečnostné opatrenia

Personálne bezpečnostné opatrenia sú zabezpečované internými mechanizmami subjektu – zriaďovateľa.

Prevádzku CAMOSR budú zabezpečovať riadiaci pracovníci (členovia PMA) s odbornou znalosťou problematiky elektronického podpisu, znalosťou bezpečnostných procedúr pre pracovníkov s bezpečnostnými povinnosťami, skúsenosťami s informačnou bezpečnosťou a s vedomosťami z oblasti legislatívy.

Všetky služobné úrovne (role) sa budú personálne obsadzovať 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 budú personálne obsadzovať tak, aby nemohla byť spochybnená nezávislosť a nestrannosť pri výkone kontrolných funkcií.

Osoby vybrané na zastávanie služobných úrovní (rolí) musia byť zodpovedné a dôveryhodné, lebo tieto úrovne (role) si vyžadujú zvýšenú dôveryhodnosť. Funkcie vykonávané týmito úrovňami (rolami) patria k funkciám, ktoré formujú v personálnej rovine základ dôvery na celú CAMOSR.

Jednotlivé služobné úrovne (role) a ich povinnosti sú popísané v časti 9.

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

Osoby vybrané na zastávanie služobných úrovní (rolí) musia mať odborné vedomosti, primerané skúsenosti a kvalifikáciu potrebnú pre ponúkané služby a vykonávané úrovne (role).

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

Témy školení majú obsahovať fungovanie softvéru a hardvéru používaného CAMOSR, prevádzkové a bezpečnostné procedúry, ustanovenia tohto dokumentu.

Pracovníci CAMOSR majú prístup k dokumentácii na adrese https://pkipub.mil.sk/doc

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

Interné údaje prevádzkovateľa CAMOSR.

5.4.b. Frekvencia spracovávania auditných záznamov

Interné údaje prevádzkovateľa CAMOSR.

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. Opatrenia na jeho ochranu sú obsiahnuté v bezpečnostnej dokumentácii CAMOSR.

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 páru kľúčov a inštalácia

- Vydavateľ certifikátov

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 ceremónií generovania žiadosti. Generovanie kľúčov musí byť vykonané v bezpečnom zariadení na uchovávanie kryptografických kľúčov. Generovanie nového kľúčového páru a certifikátu CAMOSR je nutné vykonať najneskôr 3 roky pred ukončením doby platnosti aktuálne používaného kľúčového páru a certifikátu CAMOSR.

Kľúčové páry sú generované výhradne hardvérovými prostriedkami. Parametre kľúčov sú definované v aplikácii RA client, aplikácia tiež kontroluje parametre kľúča. Kľúčový pár možno použiť len na jeden účel.

- Koncoví používatelia - Pozri kapitolu 4

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.

- Služobné role – certifikát je vydávaný technologickou certifikačnou autoritou prostredníctvom aplikácie RA Client – rolou PMA.

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.

Dĺžka kľúča je definovaná v profiloch certifikátu v kapitole 7.

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

6.2. Mazanie privátnych kľúčov CAMOSR

Proces vymazania privátnych kľúčov a Security World-u z HSM je opísaný v dokumente „Návrh a realizácia opatrení na ochranu HSM“ kap. 5.6.6 Vymazanie HSM. Proces vymazania Security World-u a privátnych kľúčov je aplikovateľný pri ukončení činnosti CAMOSR alebo pri výmene HSM.

6.3. Ochrana privátneho kľúča

CAMOSR používa na ochranu svojho súkromného kľúča kombináciu fyzických, logických a procedurálnych opatrení, ktoré zaručujú bezpečnosť jej súkromného kľúča. Tieto opatrenia sú popísané v jednotlivých častiach tohto dokumentu.

Privátny kľúč CAMOSR je uložený v špeciálnom zariadení – HSM, ktorý je certifikovaný podľa štandardu FIPS 140-2 level 3.

Pri operáciách správy privátneho kľúča CAMOSR (napr. generovanie, zálohovanie, zničenie) budú vždy prítomné aspoň dve určené oprávnené osoby, ak sa nevyžaduje väčší počet prítomných. Používať privátny kľúč CAMOSR a akýmkoľvek spôsobom s ním manipulovať môžu len na to oprávnené osoby.

Privátny kľúč CAMOSR sa používa výlučne na podpisovanie certifikátov a CRL vydávaných CAMOSR.

Pred ľubovoľnou operáciou s privátnym kľúčom CAMOSR sa bude musieť vykonať autentizácia príslušného počtu oprávnených osôb na princípe „k“ z „n“ použitím administrátorských resp. operátorských kariet patriacich k HSM modulu, v ktorom je uložený privátny kľúč CAMOSR.

Privátny kľúč CAMOSR je zálohovaný prostredníctvom softvéru na správu HSM modulu v zašifrovanej forme a to tak, že k jeho dešifrovaniu je nevyhnutná autentizácia príslušného počtu oprávnených osôb na princípe „k“ z „n“ použitím administrátorských kariet patriacich k HSM modulu, v ktorom je uložený privátny kľúč CAMOSR.

Záloha privátneho kľúča CAMOSR má byť uložená aj na inom bezpečnom mieste mimo pracoviska CAMOSR resp. budovy, kde sa nachádza pracovisko CAMOSR.

Exspirované privátne podpisové kľúče CAMOSR sa nezálohujú ani nearchivujú.

HSM, ktorý sa aktivoval, nesmie byť ponechaný bez dozoru alebo inak otvorený pre neautorizovaný prístup. Karta patriaca k HSM, v ktorom je uložený privátny kľúč CAMOSR, ako odpojiteľný prvok vybavenia nesmie byť ponechaná bez dozoru v čítačke kariet, ale vždy, keď jej prítomnosť v čítačke nie je nutná, sa musí vybrať z čítačky.

CAMOSR nepodporuje metódu `Key escrow`.

Privátny kľúč osoby v služobnej role uložený na QSCD sa nikdy nedostane mimo zariadenie, na ktorom bol vygenerovaný, dokonca sa ani nedá zálohovať. Prístup k privátnemu kľúču uloženému na zariadení je navyše chránený pomocou hesla (`pass phrase`).

QSCD ako odpojiteľný prvok vybavenia nesmie byť ponechaný bez dozoru v porte počítača alebo v čítačke ale vždy, keď sa nepoužíva, sa musí deaktivovať vybraním.

QSCD musí jeho majiteľ uložiť čo najbezpečnejšie, podľa možnosti v uzamykateľnom zariadení (bezpečnostná skriňa, trezor a pod.).

6.4. Manažment párových dát

Verejné kľúče 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 .

6.5. Aktivačné údaje

Aktivačné dáta patriace k tokenu (t.j. heslo na prístup k privátnemu kľúču uloženému na tokene) v žiadnom prípade nesmú byť zaznamenané a uložené spolu s tokenom, aby sa predišlo zneužitiu privátneho kľúča uloženého na tokene v prípade straty alebo krádeže tokenu.

Za heslo patriace k danému tokenu, jeho kvalitu a utajenie zodpovedá majiteľ daného tokenu.

Držitelia aktivačných údajov k HSM sú poučení o nutnosti ochrany týchto údajov a o ich zodpovednosti za ich stratu, zneužitie prípadne odcudzenie.

6.6. Počítačové bezpečnostné opatrenia

CAMOSR/LRA používa len bezpečné systémy a oficiálny softvér od spoľahlivých producentov a dodávateľov.

Prístup k systémom CAMOSR je obmedzený na oprávnené osoby zastávajúce príslušné roly. Tieto osoby sa pri prístupe k systémom CAMOSR musia riadne autorizovať.

Používané operačné systémy sú v maximálnej miere zabezpečené (hardening), napr. odinštalovaním nepotrebných komponentov systému, uzavretím nepotrebných portov.

Citlivé údaje (vrátane registračných údajov) sú zabezpečené počas prenosu cez nezabezpečenú sieť minimálne použitím protokolu SSL.

Uplatňuje sa princíp „need to know“ prostredníctvom mechanizmu úrovní (role): prístup k informačným a aplikačným funkciám systému je obmedzený v závislosti od úrovne (role) používateľa. Na oddelenie dôveryhodných úrovní (rolí) sa využívajú riadiace prvky bezpečnosti poskytované systémom, ktorým sa implementuje CAMOSR.

Personál CAMOSR je identifikovaný a autentifikovaný vždy pred použitím kritických aplikácii vzťahujúcich sa na manažment certifikátov.

Personál CAMOSR je povinný udržiavať požadované prevádzkové záznamy o svojej činnosti.

Komponenty lokálnej siete sú uchovávané vo fyzicky bezpečnom prostredí a ich konfigurácia je pravidelne kontrolovaná na zhodu s požiadavkami špecifikovanými CAMOSR.

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

Súčasťou systému CAMOSR sú zariadenia pre nepretržitú detekciu, monitorovanie a signalizáciu využívania výpočtového výkonu a zaplnenia dátového úložiska. Získané informácie sú využívané pre podklady do plánov obstarávania.

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

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

Administrátori (administrátor CA, systémový administrátor) zodpovedajú za:

- aplikovanie bezpečnostných aktualizácií v rozumnom čase po ich vydaní,
- neaplikovanie aktualizácií, ktoré by priniesli ďalšie bezpečnostné riziká či nestabilitu prevažujúce benefity získané ich nasadením,
- zdokumentovanie všetkých dôvodov neaplikovania aktualizácií,
- vedenie zmenového manažmentu aplikovaného na nové verzie, modifikácie a vydané opravy používaného softwaru a zmeny konfigurácie aplikované na základe politík CAMOSR,
- kontrolu zmien konfigurácií minimálne raz za 24h (kontrola je vykonávaná automaticky prostredníctvom AIDE).

6.7. Bezpečnostné opatrenia pre vývoj a riadenie bezpečnosti

Vedenie CAMOSR bude vydávať náležité bezpečnostné opatrenia pre vývoj, ktoré sa budú týkať takých aspektov, ako sú bezpečnosť vývojového prostredia, bezpečnosť systému riadenia konfigurácií a údržby, vývojové postupy.

Pri vývoji sa bude uplatňovať princíp modularity a metódy návrhu zabezpečujúceho odolnosť proti výpadkom a chybám.

Vedenie CAMOSR bude usmerňovať informačnú bezpečnosť, pričom zodpovedá za definovanie bezpečnostnej politiky CAMOSR a zabezpečenie jej publikácie a komunikácie so všetkými, ktorých sa politika týka.

Informačná bezpečnostná infraštruktúra potrebná na riadenie bezpečnosti v rámci CAMOSR bude neustále udržiavaná. Všetky zmeny s dopadom na úroveň poskytnutej bezpečnosti budú schválené vedením CAMOSR.

Každá RA je povinná dodržiavať všetky bezpečnostné opatrenia a usmernenia týkajúce sa RA.

Proces riadenia rizík informačnej bezpečnosti CAMOSR v nadväznosti na platné všeobecne záväzné právne predpisy, normy a štandardy je realizovaný v súlade s bezpečnostnou dokumentáciou CAMOSR.

6.8. Sieťové bezpečnostné opatrenia

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

Na ochranu vnútornej počítačovej siete CAMOSR pred prienikmi z vonkajšej siete prístupnej tretím stranám (napr. Internet) sú implementované náležité prostriedky a opatrenia (napr. firewally, systém detekcie prienikov (IDS)), ktorých úroveň zodpovedá aktuálnej úrovni poznatkov (`state-of-the-art`) v tejto oblasti.

Firewally budú nakonfigurované tak, aby boli zablokované protokoly, porty a prístupy, ktoré nie sú potrebné pre fungovanie CAMOSR.

Citlivé údaje (vrátane registračných údajov) sú zabezpečené počas prenosu cez nezabezpečenú sieť minimálne použitím protokolu SSL.

6.9. Opatrenia pre kryptografické moduly

Požiadavky na túto oblasť už boli definované vyššie (napr. vlastnosti kľúčov, generovanie kľúčov, režim práce s kľúčmi a uchovávanie kľúčov CAMOSR).

Požiadavky na túto oblasť sú vo všeobecnosti odvodené zo skutočnosti, že na generovanie a uchovávanie kľúčov CAMOSR bude použité bezpečné kryptografické zariadenie (HSM modul), ktoré spĺňa požiadavky štandardu FIPS 140-2 level 3.

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 (CAMOSR3)

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. 1: Obsah položiek vo vlastnom certifikáte CAMOSR3

Názov položky	Skratka názvu položky	Hodnota položky
Štát (countryName)	C	SK
Mesto (localityName)	L	Trencin
Organizácia (organizationName)	O	Ministry of Defence
Názov (commonName)	CN	CAMOSR3
Sériové číslo (serialNumber)	SERIALNUMBER	NTRSK-30845572

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

7.1.b. Vlastný certifikát CAMOSR (CAMOSR4)

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

Tabuľka č. 2: Obsah položiek vo vlastnom certifikáte CAMOSR4

Názov položky	Skratka názvu položky	Hodnota položky
Štát (countryName)	C	SK
Mesto (localityName)	L	Trencin
Organizácia (organizationName)	O	Ministry of Defence
Názov (commonName)	CN	CAMOSR4
Označenie organizácie (organizationIdentifier)	2.5.4.97	NTRSK-30845572

7.1.c. 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 4 096 bitov**
Algoritmus fingerprintu (Thumbprint Algorithm): **SHA1**

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

Tabuľka č. 3: 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

Názov položky	Skratka názvu položky	Popis položky	Príklad hodnoty položky	Typ a max. dĺžka položky
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 9066	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

Názov položky	Skratka názvu položky	Popis položky	Príklad hodnoty položky	Typ a max. dĺžka položky
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. 4: Použité rozšírenia v KC

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=1.3.158.30845572.1.7.3.1 CPS=http://pki.mil.sk/CAMOSR/CP2.pdf,	nekritické
crlDistributionPoints	URI: http://pki.mil.sk/CAMOSR/camosr3.crl, URI: http://crl.mil.sk/CAMOSR/camosr3.crl,	nekritické
AuthorityInfoAccess	URI: http://pki.mil.sk/CAMOSR/camosr3.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

Názov rozšírenia	Hodnota rozšírenia	Kritickosť
BasicConstraints	Subject Type=End Entity Path Length Constraint=None	kritické

Tabuľka č. 5: 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 9066	UTF8String 64 znakov
commonName (Meno a priezvisko)	CN	Meno, názov systému, pre ktoré je certifikát vydávaný údaj je povinný	LTA	UTF8String 64 znakov

Názov položky	Skratka názvu položky	Popis položky	Príklad hodnoty položky	Typ a max. dĺžka položky
organizationIdentifier (Identifikátor organizácie)	2.5.4.97	Odkaz na identifikačný údaj orgánu verejnej moci alebo právnickej osoby Povinný údaj	"VATSK-12311321" alebo "SZ:SK-123123".	UTF8String

Tabuľka č. 6: Použité rozšírenia v KC pre elektronickú pečať

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=1.3.158.30845572.1.7.3.1 CPS=http://pki.mil.sk/CAMOSR/CP2.pdf,	nekritické
crlDistributionPoints	URI: http://pki.mil.sk/CAMOSR/camosr3.crl, URI: http://crl.mil.sk/CAMOSR/camosr3.crl,	nekritické
AuthorityInfoAccess	URI: http://pki.mil.sk/CAMOSR/camosr3.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.d. Kvalifikovaný mandátny certifikát

Štruktúra certifikátov vydávaných CAMOSR sa môže meniť len na základe rozhodnutia PMA.

Algoritmy a dĺžky kľúčov uplatňované v certifikáte:

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

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

Tabuľka č. 7: Obsah položiek rozlišovacieho mena v KMC

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 9066	UTF8String 64 znakov
commonName (Meno a priezvisko)	CN	Meno a priezvisko údaj je povinný	MANDATAR Jan Strelec OPRAVNENIE 1057	UTF8String 64 znakov

Názov položky	Skratka názvu položky	Popis položky	Príklad hodnoty položky	Typ a max. dĺžka položky
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 – sap číslo. Povinný údaj	IDCSK 00989783	UTF8String

Názov položky	Skratka názvu položky	Popis položky	Príklad hodnoty položky	Typ a max. dĺžka položky
serialNumber (Sériové číslo)	SERIALNUMBER	Odkaz na identitu právnickej osoby – IČO. Povinný údaj	MANDANT NTRSK-30845572	UTF8String

Tabuľka č. 8: Použité rozšírenia v KMC

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=1.3.158.30845572.1.7.3.1 CPS=http://pki.mil.sk/CAMOSR/CP2.pdf Policy Identifier=1.3.158.36061701.1.1.wxyz (číslo oprávnenia podľa zoznamu oprávnení NBÚ) User Notice=SK: Opravnenie wxyz, Označenie poverenia podľa zoznamu oprávnení	nekritické
crlDistributionPoints	URI: http://pki.mil.sk/CAMOSR/camosr3.crl, URI: http://crl.mil.sk/CAMOSR/camosr3.crl,	nekritické
AuthorityInfoAccess	URI: http://pki.mil.sk/CAMOSR/camosr3.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

7.1.e. OCSP certifikát

Algoritmy a dĺžky kľúčov uplatňované v certifikáte:

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

Verejný kľúč: **RSA, dĺžka je 4 096 bitov**

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

Tabuľka č. 9: 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. 10: Použité rozšírenia v certifikáte OCSP

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=1.3.158.30845572.1.7.3.1 CPS=http://pki.mil.sk/CAMOSR/CP2.pdf,	nekritické
crlDistributionPoints	URI: http://pki.mil.sk/CAMOSR/camosr3.crl, URI: http://crl.mil.sk/CAMOSR/camosr3.crl,	nekritické
AuthorityInfoAccess	URI: http://pki.mil.sk/CAMOSR/camosr3.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.f. Certifikát TSA

V zmysle certifikačného poriadku CAMOSR, http://pki.mil.sk.

7.2. Profil OCSP

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

Tabuľka č. 11: 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

7.3. 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

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.

8.2. Identita a kvalifikácia audítora a vzťah k auditovanému subjektu

Audítor musí byť v zmysle 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.

Osoba audítora musí byť nezávislá voči CAMOSR a zriaďovateľovi CAMOSR, aby bola zaručená nestrannosť a objektívnosť auditu.

8.3. Zoznam oblastí, ktoré sú predmetom auditu zhody

Témy pokrývané auditom definuje platná legislatíva. Účelom 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 tohto dokumentu, musia sa uskutočniť nasledujúce akcie:

- audítor zaznamená rozpor,
- audítor upovedomí o rozpore subjekty definované v časti 9.1.e,
- administrátor CAMOSR navrhne PMA zodpovedajúce opatrenie na nápravu vrátane očakávaného času potrebného na jeho realizáciu.

PMA určí vhodné opatrenie na nápravu a to prípadne až po zrušenie certifikátu CAMOSR. Po náprave nedostatkov PMA obnoví činnosť CAMOSR resp. RA.

8.5. Výsledky auditu

Audítor odovzdá PMA v zmysle platnej legislatívy záverečnú správu o výsledkoch auditu. Výsledky budú oznámené auditovanému subjektu (CAMOSR resp. RA) a v prípade RA 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 externá RA vykonáva svoju činnosť musí Poskytovateľ monitorovať jej činnosť a kontrolovať ňou poskytované služby vykonávaním pravidelnej kontroly dodaných podkladov k vydaným certifikátom. V prípade zistenia závažnejších nedostatkov môže Poskytovať kedykoľvek vykonať audit predmetnej RA na zistenie príčin daných nedostatkov. Audítora vyberá PMA.

9. Ostatné obchodné a právne náležitosti

9.1. Povinnosti

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

1. ***Vlastná certifikačná autorita - je tvorená úrovňami (rolami), ktoré sa spoločne označujú ako služobné alebo dôveryhodné úrovne (role) CAMOSR***
    - **PMA,**
    - **Administrátor CA,**
    - **Systémový administrátor,**
    - **Bezpečnostný manažér:**
        - **Hlavný bezpečnostný manažér,**
        - **Bezpečnostný manažér IDS,**
        - **Bezpečnostný manažér FW,**
    - **Interný audítor,**
    - **Operátor CA,**
2. ***Registračná autorita,***
    - **Operátor RA - vettor**

- Subjekt (držiteľ certifikátu),
- Strana spoliehajúca sa na certifikát (používateľ certifikát)

Konkrétne obsadenie jednotlivých úrovní (rolí) je uvedené v dokumente „Rozdelenie rolí Certifikačnej autority MOSR – menný zoznam“

9.1.a. Povinnosti PMA

Interné údaje prevádzkovateľa CAMOSR.

9.1.b. Povinnosti Administrátora CA

Interné údaje prevádzkovateľa CAMOSR.

9.1.c. Povinnosti Systémového administrátora

Interné údaje prevádzkovateľa CAMOSR.

9.1.d. Povinnosti Bezpečnostného manažéra

Interné údaje prevádzkovateľa CAMOSR.

9.1.e. Povinnosti audítora

Interné údaje prevádzkovateľa CAMOSR.

9.1.f. Povinnosti Operátora CA

Interné údaje prevádzkovateľa CAMOSR.

9.1.g. Povinnosti operátora registračnej autority (vettor)

Interné údaje prevádzkovateľa CAMOSR.

9.1.h. Povinnosti RA

Interné údaje prevádzkovateľa CAMOSR.

9.1.i. Povinnosti žiadateľa o certifikát

Povinnosťou žiadateľa o certifikát je:

- predložiť RA presné, pravdivé a úplné informácie v súlade s požiadavkami tohto dokumentu,
- predložiť RA všetky požadované dokumenty,
- zabezpečiť, aby pri generovaní kľúčov boli použité vhodná dĺžka kľúča a vhodné algoritmy, ktoré sú v súlade s predpísanou podpisovou politikou, ak si ich generuje sám,
- predložiť RA vygenerovanú žiadosť o certifikát, na základe ktorej sa má vydať certifikát, táto žiadosť o certifikát musí obsahovať údaje, ktoré sú v súlade s údajmi na predkladaných dokumentoch a formulároch, kľúče musia byť vygenerované v QSCD,
- prevziať certifikát vydaný na základe jeho žiadosti.

9.1.j. Povinnosti držiteľa certifikátu

Povinnosťou držiteľa certifikátu (subjektu) je:

- neustále chrániť svoje privátne kľúče a QSCD, v ktorých sú uložené, a heslá na prístup k privátnym kľúčom v súlade s touto CPS 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,
- precízne sa identifikovať a vyjadrovať pri ľubovoľnej komunikácii s RA resp. CAMOSR,
- získať a do používaných aplikácií nainštalovať certifikát CAMOSR (ktorá vydala jeho certifikát) aby bola zabezpečená správna činnosť používaných aplikácií.

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

9.1.k. Povinnosti strán spoliehajúcich sa na certifikát

Strany spoliehajúce sa na certifikát vydané podľa tejto CPS sú povinné:

- získať a do používaných aplikácií nainštalovať certifikát CA (ktorá vydala jeho kvalifikovaný certifikát) a tiež koreňový certifikát CA NBÚ (ktorá vydala certifikát pre CAMOSR), aby bola zabezpečená správna činnosť používaných aplikácií (aby aplikácia mohla verifikovať celú certifikačnú cestu v súlade so štandardom X.509 verzie 3),
- používať certifikát len na účel, pre ktorý bol vydaný, ako je to dané informáciami v certifikáte,
- predtým, ako sa na daný kvalifikovaný elektronický podpis spoľahnú, overiť certifikát patriaci k danému KEPu na jeho platnosť (tzn. overovať, že certifikát bol v danom čase platný a že sa nenachádzal na aktuálnom zozname zrušených certifikát vydanom CAMOSR),

9.1.l. Povinnosti správy repozitára

Správa repozitára, ktorý podporuje CAMOSR pri publikovaní informácií podľa tejto CPS, je povinná:

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

Povinnosti každej úrovne (role) z pohľadu správy repozitára sú uvedené vyššie pri popise povinností danej úrovne (role).

9.1.m. Nezlučiteľnosť úrovní (role)

Interné údaje prevádzkovateľa CAMOSR.

9.1.n. Požiadavky na personál pre jednotlivé role

Interné údaje prevádzkovateľa CAMOSR.

9.2. Právne záruky

Táto CPS sa riadi platnými zákonmi Slovenskej republiky, najmä Nariadením eIDAS a zákonom č. 272/2016 Z. z. o dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zmene a doplnení niektorých zákonov (zákon o dôveryhodných službách).

CAMOSR sa zaväzuje, že pri výkone svojich činností bude dodržiavať ustanovenia platnej legislatívy SR, bezpečnostnej dokumentácie CAMOSR, „Certifikačného poriadku CAMOSR“ a postupy stanovené „Pravidlami na výkon certifikačných činností CAMOSR“ a „Pravidlami na výkon služby poskytovania časovej pečiatky“.

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 certifikát, ktoré by mali rovnaké číslo.

CAMOSR zaručuje výkon kvalifikovaných dôveryhodných služieb v súlade so svojím CP a 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 poskytuje záruku, že ňou vydaný certifikát bude vyhovovať štandardu X.509 verzie 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 certifikáte, 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 klienta, treťou osobou, vyššou mocou (živelná pohroma, vojna prípadne iné nekontrolovateľné udalosti, alebo sily).

CAMOSR ani jej RA nie je zodpovedná 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, kvalifikovaného elektronického podpisu alebo aplikácií, ktoré certifikát používajú.

9.2.d. Ďalšie obmedzenia zodpovednosti

CAMOSR nevykonáva funkciu prostredníka medzi držiteľmi 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 do doby stanovenej týmto dokumentom.

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 v zmysle platnej legislatívy. Predpokladom je, že boli dodržané príslušné ustanovenia v CP a CPS. Organizácia disponuje dostatočnými prostriedkami na plnenie prípadných záväzkov vyplývajúcich z poskytovanej záruky.

Záruku a z nej vyplývajúce plnenie je možné uznať len za predpokladov, že subjekt neporušil svoje povinnosti (hlavne ochranu svojho privátneho kľúča) a každý, kto sa v danom prípade spoliehal na certifikát vydaný CAMOSR, urobil všetko, aby prípadnej škode zabránil, hlavne že si overil aktuálny stav predmetného certifikát (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 nemá 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.

9.4. Rozhodcovské konanie a riešenie sporov

Pre potreby interpretácie ustanovení poriadku alebo tohto dokumentu alebo riešenia sporov sa možno obrátiť na RA 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.

CAMOSR si vyhradzuje právo každý sporný prípad najprv preskúmať.

Snahou bude riešiť spory prednostne dohodou.

PMA rozhoduje s konečnou platnosťou v prípade akýchkoľvek sporov o interpretácii ustanovení tohto dokumentu alebo jeho použiteľnosti.

Povinnosťou každej inštancie je prípad zaprotokolovať a dať žiadateľovi 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 sa majú 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,
- prístupové heslá k služobným účtom (napr. služobné účty patriace Administrátorovi CA, Operátorovi CA a pod.),

- infraštruktúra (napr. dokumenty, procedúry, postupy, súbory, skripty, heslá, pass frázy a pod.) slúži CAMOSR na prevádzku CAMOSR, vrátane jej RA,
- informačný systém CAMOSR a údaje uložené v ňom, z týchto údajov špeciálne osobné údaje subjektov a žiadateľov podliehajúce ochrane v zmysle Zákona č. 18/2018 Z. z. o ochrane osobných údajov.

Za účelom náležitej správy certifikátov môže byť požadované, 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 považujú 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. Politika poskytovania informácií podľa zákona

CAMOSR zasiela zoznam všetkých vydaných certifikátov a zoznamov zrušených certifikátov do systému ZKC zriadeným NBÚ každý mesiac do 14 dňa.

9.6.e. 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 práv na všetky dokumenty, dáta, procedúry, politiky, poriadky, certifikáty a privátne kľúče, ktoré sú súčasťou infraštruktúry CAMOSR a 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. Testy zabezpečuje prevádzkovateľ CAMOSR.

9.9. Procedúry na zmenu špecifikácie

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

Zriaďovateľ 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 popis zmeny, zdôvodnenie zmeny a kontaktné údaje osoby, ktorá zmenu požaduje resp. navrhuje.

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

Každá zmenená verzia tohto dokumentu má byť očíslovaná a evidovaná.

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

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

9.10. Procedúry pre zverejňovanie a upozornenie

CAMOSR publikuje verejné informácie týkajúce sa tohto dokumentu na internetovej adrese https://www.pki.mil.sk.

Tento dokument bude plne k dispozícii pre osoby zastávajúce služobné úrovne (role) a pre osoby vykonávajúce audit.

9.11. Úľavy

PMA má právo rozhodnúť, či je odchýlka v praxi CAMOSR prijateľná podľa tohto dokumentu alebo akým spôsobom sa má prax zosúladiť s týmto dokumentom.

PMA môže povoliť úľavu od niektorej požiadavky tohto dokumentu, aby sa vyhovelo urgentným, nepredvídateľným prevádzkovým požiadavkám.

Keď sa povolí úľava, má sa to zverejniť pomocou webu CAMOSR, aby sa o úľave dozvedeli strany spoliehajúce sa na certifikát a má sa buď iniciovať zmena do tohto dokumentu alebo sa má pre platnosť danej úľavy stanoviť konkrétny časový limit.

Príloha č.1 Vzor prevádzkovej knihy CA/RAMOSR

VOJENSKÝ ÚTVAR XXXX
XXXXXXXX
Č. p:

Trenčín,
Výtlačok jediný!
Počet listov:

PREVÁDZKOVÁ KNIHA
CA/RAMOSR - VZOR

Dátum a čas prijatia			Pôvodné číslo písomnosti	Počet listov	Vec		Dátum a čas prevzatia			Podpis oprávnenej osoby na prevzatie	Poznámka
					PRIEZVISKO a Meno						
hod	min	sek			hodnosť	titul	hod	min	sek		

Príloha č.2 Vzor prevádzkovej knihy udalostí CAMOSR

VOJENSKÝ ÚTVAR XXXX
XXXXXXXXXXXXX
Č. p.:

Trenčín,
Výtlačok jediný!
Počet listov:

PREVÁDZKOVÁ KNIHA UDALOSTÍ CA/RAMOSR - VZOR

Dátum a čas vzniku udalosti			Priezvisko meno pracovníka	Vec	Dátum a čas ukončenia udalosti			Podpis oprávnenej osoby na prevzatie	Poznámka
hod	min	sek			hod	min	sek		