VOJENSKÝ ÚTVAR 9066
TRENČÍN
Č. p.: 6.spojp-EL 7/11-1-58/2023

Trenčín, 25. júl 2023
Výtlačok jediný.
Počet listov: 19

Schvaľujem: _____

Pravidlá na výkon služby poskytovania časovej pečiatky CAMOSR

„Verejný dokument“

Spracovateľ: Centrum správy IB a systémov OUS/ Úsek PKIaCA

Verzia: 3.4

Dátum platnosti: 15. AUG. 2023

Olbrachtova 5, 911 01 TRENČÍN
tel.: +421 960 40 79 89
e-mail: pki@mil.sk
web: http://pki.mil.sk

Ochranné známky

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

História zmien

Verzia	Dátum	Opis revízie
0.1.	20.10.2005	prvý návrh – na pripomienkovanie
1.0.	03.11.2005	na schválenie
1.1.	14.11.2005	schválený
2.0.	17.10.2006	zrevidovaný
2.1.	15.12.2008	úprava doby platnosti certifikátu TSA
2.2.	27.11.2009	aktualizovaný, zmena VÚ, aktualizované vyhlášky NBÚ
2.3.	01.03.2011	formálna analýza, zmena OID
2.4.	19.08.2011	zrevidovaný
2.5.	06.07.2012	zrevidovaný
2.6.	01.03.2013	zrevidovaný
3.0.	02.05.2017	zrevidovaný, zrušený zákon č. 215/2002 Z. z.
3.1.	07.05.2020	aktualizovaný, zmena SN a DigitalID pre CA a OCSP, pridanie politiky ETSI 0.4.0.2023.1.1
3.2.	28.06.2021	zrevidovaný
3.3.	13.07.2022	aktualizovaný, zmena SN a DigitalID pre TSA
3.4.	25.07.2023	zrevidovaný

Obsah

Zoznam obrázkov a tabuliek

Obrázky

Tento dokument neobsahuje obrázky

Tabuľky

Skratky a pojmy

Skratky

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

Pojmy

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

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

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

Časová pečiatka – informácia pripojená alebo inak logicky spojená s elektronickým dokumentom spĺňajúca požiadavky nariadenia európskeho parlamentu a rady (EÚ) č. 910/2014, ktorá umožňuje preukázať, že elektronický dokument (alebo elektronický podpis) existoval pred určitým konkrétnym časovým momentom uvedeným v časovej pečiatke. Časová pečiatka je dátový objekt, ktorý zväzuje reprezentáciu informácie s konkrétnym časom, čím sa vytvorí dôkaz, že daná informácia (napr. elektronický dokument, elektronický podpis) existovala pred daným konkrétnym časom.

Spoliehajúca sa strana – príjemca (používateľ) časovej pečiatky spoliehajúci sa na jej presnosť.

Referenčný čas – čas, ktorý poskytuje niektoré z referenčných pracovísk.

Vydavateľ časovej pečiatky – (Certifikačná) autorita, ktorá poskytuje službu vydávania časových pečiatok, označuje sa skratkou TSA (Time Stamp Authority). V zmysle nariadenia EÚ č. 910/2014 ju môže vyhotoviť iba akreditovaná certifikačná autorita použitím súkromného kľúča určeného na tento účel.

Hašovacia (hash) funkcia – matematická transformácia, ktorá digitálnym dokumentom rozličnej dĺžky priradí také čísla vopred ustanovenej nenulovej pevnej dĺžky, že umožňujú overiť integritu digitálneho dokumentu, z ktorého boli odvodené transformáciou a nemožno z nich spätne odvodiť digitálny dokument (Vyhláška NBÚ č. 135/2009 Z. z.)

Digitálny odtlačok (dokumentu resp. súboru) – číslo (funkčná hodnota) vypočítané hash funkciou z dokumentu resp. súboru.

Žiadateľ – právnická alebo fyzická osoba, ktorá žiada o vyhotovenie časovej pečiatky prostredníctvom žiadosti zaslanej vydavateľovi časovej pečiatky a ktorá súhlasila s podmienkami poskytovanej služby.

Žiadosť o vyhotovenie časovej pečiatky (resp. skrátene žiadosť) – dátová štruktúra obsahujúca digitálny odtlačok dokumentu, na ktorý sa má vyhotoviť časová pečiatka, vytvorený žiadateľom pomocou schválenej hash funkcie.

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

1. Úvod

Pri tvorbe hodnoverných a v praxi overiteľných digitálnych dôkazov je nevyhnutnosťou mať dohodnutý spôsob priradenia časových údajov k danému konaniu tak, že tieto časové údaje môžu byť navzájom v neskoršej dobe porovnávané. Kvalita týchto dôkazov je založená na postupoch pri vytváraní a správe údajových štruktúr, ktoré reprezentujú danú udalosť, a na kvalite parametrických údajov, ktoré ich pevne spájajú s reálnym svetom. V tomto prípade to budú časové údaje a spôsob, ako budú využité.

Na dôvažok, v prípade overovania elektronického podpisu, môže byť nevyhnutné preukázať, že elektronický podpis podpisovateľa bol zhotovený v čase platnosti certifikátu podpisovateľa. Toto je nevyhnutné v dvoch prípadoch:

- počas doby platnosti certifikátu podpisovateľa môže dôjsť ku kompromitácii súkromného kľúča podpisovateľa a tento certifikát je z uvedeného dôvodu zrušený,
- po ukončení doby platnosti certifikátu podpisovateľa.

Na riešenie uvedeného problému je možné použiť **časovú pečiatku**, ktorá umožňuje preukázať, že elektronický dokument (alebo elektronický podpis) existoval pred určitým konkrétnym časovým momentom uvedeným v časovej pečiatke. Táto technika umožňuje preukázať, že podpis bol vytvorený pred časovým údajom obsiahnutým v časovej pečiatke.

Pravidlá na výkon služby časovej pečiatky certifikačnej autority Ministerstva obrany Slovenskej republiky (ďalej CAMOSR) je dokument, ktorý upresňuje a konkretizuje požiadavky na zriadenie a výkon služby časovej pečiatky. Zaoberá sa pravidlami, ktoré ustanovujú použiteľnosť časovej pečiatky pre definovaný okruh používateľov časových pečiatok a triedy aplikácií so spoločnými bezpečnostnými požiadavkami. Definuje účastníkov procesu vydávania časových pečiatok, ich zodpovednosti, práva a rozsah použitia časových pečiatok.

Tento dokument nastoľuje zásady prevádzkovania a riadenia služby časovej pečiatky, ktoré vytvárajú ich primeranú dôveru k tejto činnosti CAMOSR.

Požiadavky tohto dokumentu sú zamerané na službu časových pečiatok použitú na podporu kvalifikovaných elektronických podpisov alebo na ľubovoľnú aplikáciu vyžadujúcu dôkaz, že informácia existovala pred daným časom.

Požiadavky tohto dokumentu sú založené na použití kryptografie verejných kľúčov, certifikátov verejných kľúčov a spoľahlivom časovom zdroji.

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

Pravidlá na výkon služby 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 služieb časovej pečiatky, na základe ktorých je zriadený a prevádzkovaný poskytovateľ služby časovej pečiatky Ministerstva obrany Slovenskej republiky TSA 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.

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.

TSA CAMOSR v rámci týchto CPS sa rozumie, poskytovateľ dôveryhodných služieb vyhotovovania, overovania a validácie 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

1.2. Identifikácia

Názov:	**Pravidlá na výkon služby poskytovania časovej pečiatky CAMOSR**
Skratka názvu:	**CPS TSA CAMOSR**
Verzia:	**3.4 - Júl 2023**
Tomuto dokumentu je priradený identifikátor objektu (OID):	**1.3.158.30845572.1.7.3.2**

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. 3.158.30845572.1.7.3.2 – CPS TSA 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 autorita časovej pečiatky

Je entita autorizovaná PMA na vytváranie časových pečiatok pomocou súkromného kľúča používaného výhradne na túto činnosť. V tele časovej pečiatky je identifikácia tsa.mil.sk (ďalej len TSA MOSR) ako vydavateľa časovej pečiatky.

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

Služba poskytovania časovej pečiatky vydavateľom časovej pečiatky (ďalej TSA MOSR) pozostáva s dvoch neoddeliteľných zložiek, ktorými sú:

- poskytovanie časovej pečiatky – zložka, ktorá vytvára samotné časové pečiatky,
- riadenie vyhotovovania časovej pečiatky – zložka, ktorá monitoruje a kontroluje priebeh vyhotovovania časovej pečiatky, aby sa zaistilo, že táto služba je poskytovaná v zmysle pravidiel stanovených TSA CAMOSR.

1.3.b. Koncové entity

Používateľ časovej pečiatky

Používateľom časovej pečiatky môže byť individuálna fyzická osoba ako koncový používateľ, prípadne právnická osoba zastupujúca niekoľkých koncových používateľov.

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

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

Služba časovej pečiatky je poskytovaná výhradne iba fyzickým a právnickým osobám organizačne patriacim do rezortu MOSR.

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.

1.3.c. Použiteľnosť

Certifikát vydaný pre TSA, kde súkromný kľúč sa nachádza v HSM a je vydaný výhradne za účelom poskytovania služby časovej pečiatky. Službu časovej pečiatky poskytuje TSA MOSR v rámci dôveryhodných služieb CAMOSR.

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. Ďalej zodpovedá za rozhodovanie o súlade postupov CAMOSR, ktoré sú uvedené v pravidlách na výkon certifikačných činností (CPS).

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 CAMOSR. 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.

1.5. Kontaktné údaje

Zriaďovateľom a prevádzkovateľom CAMOSR je Ministerstvo obrany Slovenskej republiky.

Vydavateľom časovej pečiatky v zmysle týchto pravidiel je:

Adresa:	**VÚ 9066 Trenčín**
	Certifikačná autorita MOSR (CAMOSR)
	Olbrachtova 5
	911 01 Trenčín
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)960 400 400, 40 22 00 (DRKIS)**

fax: **+421 (0)960 40 64 20 (DRKIS)**

2. Všeobecné ustanovenia

2.1. Povinnosti

Interné údaje prevádzkovateľa CA MOSR.

2.1.a. Povinnosti PMA

Interné údaje prevádzkovateľa CA MOSR.

2.1.b. Povinnosti Administrátora TSA

Interné údaje prevádzkovateľa CA MOSR.

2.1.c. Povinnosti Systémového administrátora

Interné údaje prevádzkovateľa CA MOSR.

2.1.d. Povinnosti Bezpečnostného manažéra

Interné údaje prevádzkovateľa CA MOSR.

2.1.e. Povinnosti audítora

Interné údaje prevádzkovateľa CA MOSR.

2.1.f. Povinnosti Operátora TSA

Interné údaje prevádzkovateľa CA MOSR.

2.1.g. Povinnosti žiadateľa o časovú pečiatku

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

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

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

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

2.1.h. Povinnosti strán spoliehajúcich sa na certifikát

Podmienky poskytovania služieb časovej pečiatky, ktoré sú k dispozícii spoliehajúcim sa stranám, musia obsahovať povinnosti, ktoré musí vykonať, keď sa spolieha na časovú pečiatku:

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

2.1.i. Nezlučiteľnosť úrovní (role)

TSA MOSR musí byť zabezpečená proti tomu, aby bola jedna osoba schopná kompromitovať systém (single-handedly) špecifikovaním úrovní (rolí) a zodpovedností medzi viaceré osoby.

Je možné, aby niektoré osoby mali viaceré úrovne (role), ale je potrebné definovať nezlučiteľnosť úrovní (rolí), typicky musia byť oddelené úrovne (role):

- implementujúce politiku,
- vykonávajúce registráciu,
- vykonávajúce audit.

Toto rozdelenie je postačujúce na zabezpečenie systému proti kompromitácii.

2.1.j. Požiadavky na personál pre jednotlivé role

Interné údaje prevádzkovateľa CA MOSR.

2.2. 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) a politikou ETSI 0.4.0.2023.1.1.

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

2.2.a. Záruky a obmedzenia poskytovaných záruk

CAMOSR garantuje jednoznačnosť čísla (Serial Number) každej ňou vydanej časovej pečiatky, tzn. garantuje, že neexistujú a nikdy nebudú existovať žiadne dve časové pečiatky, 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 časových pečiatok použije vlastný privátny kľúč uložený v HSM module patriaci k jej vlastnému certifikátu.

CAMOSR poskytuje záruku, že ňou vydaná časová pečiatka bude koordinovaná s UTC s presnosťou +- 500 milisekúnd, to znamená, ak bude zistená časová odchýlka väčšia ako 500 milisekúnd časová pečiatka nebude vydaná.

2.2.b. Typy krytých škôd

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

2.2.c. Ohraničenie možných strát

Právna zodpovednosť TSA CAMOSR je daná platnou legislatívou Slovenskej republiky.

Finančnú zodpovednosť a z nej vyplývajúce plnenie je možné uznať len za predpokladov, že používateľ neporušil svoje povinnosti (hlavne overiť si, že časová pečiatka je správne podpísaná) a že každý, kto sa v danom prípade spoliehal na časovú pečiatku vydanú TSA CAMOSR, urobil všetko, aby prípadnej škode zabránil.

Neoverenie časovej pečiatky sa kvalifikuje ako hrubé porušenie povinností vyplývajúcich z tohto dokumentu, dôsledkom čoho zanikajú akékoľvek nároky na prípadné uplatňovanie si akejkoľvek náhrady.

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 TSA CAMOSR.

Akákoľvek žiadosť o náhradu škody musí byť podaná písomne.

2.3. 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.

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

2.4. 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:

- TSA,
- 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.

2.5. Poplatky

Nevyberajú sa žiadne poplatky.

2.6. Zverejňovanie informácií

TSA CAMOSR sprístupní všetkým žiadateľom a spoliehajúcim sa stranám podmienky poskytovania služieb časovej pečiatky.

Zverejňované informácie budú obsahovať:

- kontaktné informácie,
- používanú politiku časových pečiatok,
- používaný hash algoritmus
- životnosť kľúčov používaných na vyhotovovanie časovej pečiatky, pričom doba platnosti certifikátu TSA CAMOSR nesmie prekročiť dobu platnosti certifikátu CAMOSR (ktorá vydáva certifikát TSA CAMOSR),

- presnosť času vo vyhotovovaných časových pečiatkach s ohľadom na UTC,
- akékoľvek obmedzenia týkajúce sa používania služby časovej pečiatky,
- povinnosti žiadateľa,
- povinnosti spoliehajúcich sa strán,
- informácie o spôsobe overovania časovej pečiatky tak, aby spoliehajúca sa strana mohla túto považovať za „primerane spoľahlivú“ a akékoľvek obmedzenia trvania platnosti,
- dobu uchovávania záznamov (logov) TSA CAMOSR,
- príslušné právne predpisy,
- obmedzenia zodpovednosti,
- postupy podávania sťažností a urovnávania sporov,
- či bola TSA CAMOSR posudzovaná vzhľadom k svojej politike časových pečiatok, a ak áno, kým.

Hore uvedené informácie budú k dispozícii trvale prostredníctvom webu CAMOSR. Bude ich možné získať v elektronickej podobe stiahnutím z web stránok CAMOSR.

2.7. Audit zhody

2.7.a. 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.

2.7.b. 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.

2.7.c. 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.

2.7.d. 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 2.7.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.

2.7.e. 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.

2.8. Ochrana práv duševného vlastníctva

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

3. Prevádzkové požiadavky

Poskytovateľ časovej pečiatky TSA CAMOSR musí zaviesť systém riadenia spĺňajúci nižšie uvedené požiadavky.

Požiadavky poukazujú na úlohy v oblasti bezpečnosti nasledované viac špecifickými požiadavkami na riadenie, zabezpečujúce splnenie týchto podmienok za účelom preukázania nevyhnutnej dôvery, že tieto úlohy budú splnené.

Poskytovanie služby časovej pečiatky je permanentné pre každého majiteľa KC, ktorý vydala CAMOSR.

3.1. Prehlásenie o výkone služby a zverejňovaných informáciách

3.1.a. Prehlásenie o výkone služby

TSA CAMOSR zabezpečí nevyhnutnú spoľahlivosť pri poskytovaní služby časovej pečiatky nasledovnými opatreniami:

- vypracovaním procedúr resp. pracovných postupov používaných na naplnenie všetkých požiadaviek určených v tejto smernici,
- poskytnutím príslušných častí tohto dokumentu a ďalších náležitých dokumentov všetkým žiadateľom o služby časovej pečiatky ako aj spoliehajúcim sa stranám,

  Poznámka: TSA CAMOSR nemusí sprístupniť všetky detailné informácie o svojej praxi pri výkone TSA.

- zverejnením podmienok týkajúcich sa použitia služieb časovej pečiatky pre všetkých žiadateľov a potenciálne spoliehajúce sa strany ,
- schvaľovaním všetkých dokumentov popisujúcich pravidlá pre výkon činností spojených so službou časovej pečiatky zodpovednými pracovníkmi vedenia CAMOSR,
- zabezpečením prostredníctvom vedenia CAMOSR riadneho sprevádzkovania a používania všetkých postupov a praktík TSA CAMOSR,
- definovaním postupov preskúmania praktík TSA vrátane zodpovedností pri udržiavaní úrovne poskytovaných služieb,
- okamžite po schválení zodpovednými pracovníkmi sprístupnením všetkých zmien týkajúcich sa pravidiel na výkon činností súvisiacich s poskytovaním služieb časovej pečiatky všetkým dotknutým stranám.

3.2. Audit bezpečnosti

Interné údaje prevádzkovateľa CA MOSR.

3.3. 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. o dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zmene a doplnení niektorých zákonov (zákon o dôveryhodných službách).

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

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

Modifikovanie alebo odstraňovanie archivovaných informácií nie je prípustné.

Je zabezpečená utajenosť a integrita archivovaných záznamov a médií.

3.4. Zmena kľúča

Celý proces musí prebehnúť bez negatívneho vplyvu na úroveň zabezpečenia.

K zmene kľúčov TSA CAMOSR môže dôjsť z dôvodu:

- Blíži sa čas ukončenia platnosti (expirácie) aktuálne používaných kľúčov TSA CAMOSR: toto je normálny stav – 1 rok pred uplynutím platnosti doteraz používaného páru kľúčov TSA CAMOSR.
- Je nutné vymeniť aktuálne používané kľúče TSA CAMOSR z dôvodu ich kompromitácie, bezodkladne požiada o zrušenie svojho certifikátu CAMOSR, upozorní prostredníctvom svojho webu spoliehajúce sa strany. Po tom čo sa vygeneruje nový kľúčový pár a CAMOSR vydá nový certifikát TSA CAMOSR, tento nový sa zverejní. Spoliehajúce sa strany budú upovedomené o platnosti nového certifikátu TSA CAMOSR. Každá ďalšia časová pečiatka bude podpísaná novým súkromným kľúčom TSA CAMOSR.

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

3.5. Havarijný plán

V prípade mimoriadnych udalostí resp. havarijných stavov v rámci TSA sa podieľa RA na základe získaných pokynov na informovaní verejnosti.

V prípade zničenia privátneho kľúča TSA CAMOSR, strany spoliehajúce sa na certifikáty môžu na vlastné riziko urobiť rozhodnutie pokračovať v používaní časových pečiatok podpísaných použitím zničeného privátneho kľúča TSA CAMOSR, aby sa splnili ich urgentné operačné požiadavky.

Mimoriadne udalosti a postupy pre zabezpečenie činnosti CAMOSR v prípade mimoriadnych udalostí sú uvedené v havarijných postupoch a plánoch obnovy na výkon certifikačných činností a ochranu osobných údajov držiteľov certifikátov.

3.5.a. Poškodenie výpočtových zdrojov

V prípade havárie, pri ktorej je vybavenie TSA CAMOSR poškodené a neschopné prevádzky, ale nie je zničený jej podpisový kľúč, fungovanie TSA CAMOSR treba obnoviť podľa možnosti čo najrýchlejšie. Detailný postup obnovy výpočtových zdrojov je uvedený v havarijných postupoch a plánoch obnovy na výkon certifikačných činností a ochranu osobných údajov držiteľov certifikátov.

Obnovu pracoviska TSA CAMOSR resp. jeho časti robia oprávnené osoby (predovšetkým Administrátor TSA a Systémový administrátor) v súčinnosti s ostatnými zložkami TSA CAMOSR.

V prípade straty alebo poškodenia QSCD, na ktorom je uložený služobný certifikát osoby zastávajúcej služobnú úroveň (rolu) alebo v prípade zabudnutia hesla na prístup k privátnemu kľúču uloženému na danom zariadení daná osoba obmedzí alebo pozastaví výkon svojej činnosti a udalosť okamžite oznámi PMA.

V prípade straty alebo poškodenia operátorskej alebo administrátorskej karty ku HSM modulu, alebo v prípade zabudnutia hesla na prístup k danej čipovej karte sa udalosť okamžite oznámi PMA.

3.5.b. Zrušenie certifikátu TSA CAMOSR

V prípade havárie, pri ktorej je inštalácia TSA CAMOSR fyzicky poškodená a jej podpisový kľúč je v dôsledku toho zničený a nie je ho možné obnoviť zo zálohy, sa certifikát TSA CAMOSR zruší. Potom sa kompletne zopakuje inštalácia TSA CAMOSR spolu s obnovením jej vybavenia. Ihneď ako sa vygeneruje nový kľúčový pár zverejní sa nový certifikát TSA CAMOSR. Každá ďalšia vydaná (nová) časová pečiatka bude podpísaná novým súkromným kľúčom TSA CAMOSR. Pri obnove sa postupuje v zmysle inštalačných postupov, ktoré sú obsiahnuté v samostatných dokumentoch.

3.5.c. Kompromitácia súkromného kľúča TSA CAMOSR

TSA CAMOSR zabezpečuje, že v prípade udalosti, ktorá ovplyvní jej služby, vrátane kompromitácie privátneho kľúča TSA alebo zistenia odchýlky od kalibrácie, sú príslušné informácie k dispozícii všetkým žiadateľom a spoliehajúcim sa stranám a to:

- plán obnovy TSA CAMOSR sa zaoberá kompromitáciou alebo podozrením na kompromitáciu privátneho podpisového kľúča CAMOSR alebo stratou kalibrácie hodín TSA CAMOSR, ktoré môžu ovplyvniť už vydané časové pečiatky,
- v prípade kompromitácie alebo podozrenia z kompromitácie alebo pri strate kalibrácie dá TSA CAMOSR k dispozícii všetkým žiadateľom a spoliehajúcim sa stranám popis zistenej kompromitácie,
- v prípade kompromitácie činnosti TSA CAMOSR, podozrenia z kompromitácie alebo straty kalibrácie TSA CAMOSR nevydáva časové pečiatky až do času, keď sa prijmú opatrenia na obnovu po kompromitácii,

- v prípade vážnej kompromitácie činnosti TSA CAMOSR alebo straty kalibrácie, sprístupní TSA CAMOSR, pokiaľ je to možné, všetkým žiadateľom a spoliehajúcim sa stranám informáciu, ktorá by im mala napomôcť identifikovať časové pečiatky, ktoré by mohli byť ovplyvnené, s výnimkou, keď by to viedlo k porušeniu súkromia používateľov služby časovej pečiatky alebo bezpečnosti služby TSA CAMOSR.

3.5.d. Prírodná katastrofa

Mimoriadne udalosti a postupy pre zabezpečenie činnosti TSA CAMOSR v prípade mimoriadnych udalostí (prírodná katastrofa) sú uvedené v havarijných plánoch a postupoch pri zisťovaní a riešení bezpečnostných incidentov.

3.6. Ukončenie činnosti TSA CAMOSR

TSA CAMOSR zabezpečuje, že prípadné narušenie služieb žiadateľom a spoliehajúcim sa stranám, v dôsledku zastavenia služby poskytovania časovej pečiatky bude minimalizované a zvlášť zabezpečuje následnú podporu vo forme informácií požadovaných na overenie správnosti časových pečiatok nasledovným spôsobom:

- pred ukončením poskytovania služby časovej pečiatky sa vykoná minimálne nasledovné:
    - TSA CAMOSR poskytne všetkým potenciálnym žiadateľom a spoliehajúcim sa stranám informácie týkajúce sa ukončenia jej činnosti,
    - TSA CAMOSR prenesie na spoľahlivý subjekt svoje záväzky týkajúce sa udržiavania záznamov (logov) a archívu pre audit nevyhnutných pre dokazovanie správnej činnosti TSA CAMOSR po primeranú dobu,
    - TSA CAMOSR prenesie na spoľahlivý subjekt svoje záväzky, aby bol k dispozícii počas primeranej doby jej verejný verifikačný kľúč prostredníctvom certifikátu pre spoliehajúce sa strany,
    - súkromný podpisový kľúč TSA vrátane všetkých jeho kópií je zničený takým spôsobom, že nie je možná jeho obnova,
    - zničenie súkromného kľúča TSA je vykonané pod dohľadom viacerých kvalifikovaných osôb a o zničení súkromného kľúča TSA je spísaný protokol dokladujúci jeho zničenie,
    - TSA CAMOSR prijme všetky kroky na zrušenie svojich certifikátov.

4. Fyzické, procedurálne a personálne bezpečnostné opatrenia

TSA CAMOSR zabezpečuje uplatňovanie takých manažérskych a administratívnych postupov, ktoré sú vhodné a v súlade s najlepšou profesionálnou praxou tak, že:

- TSA CAMOSR preberá plnú zodpovednosť za všetky aspekty poskytovania služby časovej pečiatky popisované vo svojej politike,
- TSA CAMOSR poskytne smernice o informačnej bezpečnosti prostredníctvom svojho vedenia, ktoré je zodpovedné za definovanie informačnej bezpečnosti,
- s týmto dokumentom sú oboznámení všetci pracovníci, ktorých sa týka,
- infraštruktúra informačnej bezpečnosti nevyhnutná pre zabezpečenie bezpečnosti v rámci TSA CAMOSR je udržiavaná počas celej doby činnosti TSA CAMOSR,
- akékoľvek zmeny, ktoré by mohli ovplyvniť úroveň bezpečnosti, sú odsúhlasené vedením CAMOSR,
- bezpečnostné opatrenia a pracovné postupy TSA CAMOSR, systémové a informačné aktíva poskytujúce služby časovej pečiatky sú dokumentované, zavedené a udržiavané.

TSA CAMOSR zabezpečuje, že jej informačné a ďalšie aktíva sú chránené na požadovanej úrovni, a že TSA CAMOSR má zoznam všetkých aktív a ich klasifikáciu z pohľadu požiadaviek na ochranu, ktoré sú v súlade s vykonanou analýzou rizík.

4.1. Fyzické bezpečnostné opatrenia

Interné údaje prevádzkovateľa CA MOSR.

4.2. Procedurálne opatrenia

Interné údaje prevádzkovateľa CA MOSR.

4.2.a. Prevádzkový manažment

TSA CAMOSR zabezpečuje, že systémové komponenty sú bezpečné a pracujú správne, s minimálnym rizikom poruchy nasledovne:

a) integrita systémových komponentov TSA CAMOSR je chránená proti vírusom, škodlivému a neautorizovanému softvéru,

b) zaznamenávanie incidentov a postupy reakcií na incidenty je zavedené takým spôsobom, ktoré minimalizuje škody z bezpečnostných incidentov a zlyhaní,

c) s médiami používanými v rámci dôveryhodného TSA CAMOSR systému sa zaobchádza takým spôsobom, aby sa predišlo ich poškodeniu, odcudzeniu, neautorizovanému prístupu k nim a zastaraniu,

d) médiá obsahujúce citlivé informácie, ktoré nie sú už potrebné, sú vymazané a bezpečným spôsobom likvidované,

e) pre všetky dôveryhodné úrovne (role) sú ustanovené a zavedené postupy, ktoré majú vplyv na poskytovanie služby časovej pečiatky.

4.2.b. Manažment prístupu k systému

Interné údaje prevádzkovateľa CA MOSR.

4.2.c. Nasadenie a údržba dôveryhodných systémov

Interné údaje prevádzkovateľa CA MOSR.

4.3. Personálne bezpečnostné opatrenia

Interné údaje prevádzkovateľa CA MOSR.

4.4. Postup získavania auditných záznamov

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

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

4.4.a. Typy zaznamenávaných udalostí

CAMOSR musí zaznamenávať a vyhodnocovať nasledovné dôležité udalosti:

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

4.4.b. Frekvencia spracovávania auditných záznamov

Interné údaje prevádzkovateľa CA MOSR.

5. Technické bezpečnostné opatrenia

Technická časť infraštruktúry TSA CAMOSR (hardvér a softvér) bude pozostávať len z bezpečných systémov a oficiálneho softvéru. Architektúru infraštruktúry TSA 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 TSA CAMOSR a ktorý patrí k najcitlivejším aktívam. Privátny kľúč TSA 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.

5.1. Generovanie páru kľúčov a inštalácia

Interné údaje prevádzkovateľa CA MOSR.

5.2. Ochrana privátneho kľúča

TSA CAMOSR zabezpečuje, že jej súkromný kľúč zostane tajný a zostane zachovaná jeho integrita nasledovne:

- súkromný podpisový kľúč TSA CAMOSR je generovaný, uchovávaný a používaný v kryptografickom module zariadenia, ktoré spĺňa požiadavky dané štandardom FIPS 140-2 level 3,
- v prípade zálohovania súkromného kľúča je tento kopírovaný, uchovávaný a obnovovaný len dôveryhodnými a kvalifikovanými oprávnenými osobami,
- jednou z osôb, ktorá vykonáva tieto činnosti, je administrátor TSA CAMOSR,
- poverené osoby robia dané výkony v súlade s týmto dokumentom a príslušnou technickou dokumentáciou.
- po ukončení akejkoľvek manipulácie so súkromným kľúčom TSA CAMOSR sa vykoná o danej činnosti (napr. zálohovanie, kopírovanie alebo obnova súkromného kľúča) záznam do „Prevádzkovej knihy CAMOSR“.

5.3. Distribúcia verejného kľúča TSA CAMSOR

TSA CAMOSR zaručuje, že integrita a dôveryhodnosť verejného verifikačného kľúča TSA CAMOSR je zachovaná počas jeho distribúcie k spoliehajúcim sa stranám nasledovne:

- verejný verifikačný kľúč TSA CAMOSR je k dispozícii pre spoliehajúce sa strany prostredníctvom certifikátu verejného kľúča,
- tento certifikát TSA CAMOSR je vydaný CAMOSR ako certifikát na správu a je vydaný certifikačnou autoritou, ktorej certifikačná politika poskytuje rovnakú alebo vyššiu úroveň bezpečnosti ako má tento dokument.

5.4. Obnovovanie kľúča TSA CAMOSR

Interné údaje prevádzkovateľa CA MOSR.

5.5. Ukončenie životnosti kľúčov TSA CAMOSR

Interné údaje prevádzkovateľa CA MOSR.

5.6. Manažment životného cyklu kryptografického modulu používaného na podpisovanie časových pečiatok

TSA CAMOSR zabezpečuje bezpečnosť kryptografického hardvéru (hardvérový modul na podpisovanie časových pečiatok) počas celej jeho životnosti nasledovne:

- garantuje, že do hardvérového modulu na podpisovanie časových pečiatok sa nebude svojvoľne zasahovať, resp. s ním nedovolene manipulovať počas jeho prípadnej prepravy,
- garantuje, že do hardvérového modulu na podpisovanie časových pečiatok sa nebude svojvoľne zasahovať, resp. s ním nedovolene manipulovať v priebehu jeho uschovávania, skladovania a prevádzkového využívania,
- inštalácia, aktivácia a prípadné zálohovanie podpisových kľúčov TSA CAMOSR v kryptografickom module sa vykonáva len dôveryhodnými a kvalifikovanými oprávnenými osobami a vo fyzicky bezpečnom prostredí, pričom jednou z týchto osôb je administrátor TSA CAMOSR,
- garantuje, že hardvérový modul na podpisovanie časových pečiatok funguje korektne,
- v prípade vyradenia hardvérového modulu z prevádzky je z neho vymazaný súkromný kľúč TSA CAMOSR,
- vymazanie súkromného kľúča TSA CAMOSR je vykonané dôveryhodnými a kvalifikovanými oprávnenými osobami za prítomnosti a pod kontrolou minimálne dvoch osôb, a vo fyzicky bezpečnom prostredí, pričom jednou z týchto osôb je administrátor TSA CAMOSR.

5.7. Aktivačné údaje

Interné údaje prevádzkovateľa CA MOSR.

5.8. Synchronizácia času s UTC

TSA CAMOSR zabezpečuje, že čas ňou používaný je synchronizovaný s UTC s deklarovanou presnosťou 500 milisekúnd nasledovne:

- kalibrácia hodín TSA CAMOSR je vykonávaná tak, že očakávaná odchýlka času nebude mimo deklarovanú presnosť,
- hodiny zariadenia TSA CAMOSR sú chránené proti hrozbám, ktoré by mohli viesť k nezistiteľným zásahom do hodín, ktoré by mohli mať za následok ich odchýlku od kalibrácie, pričom pod pojmom hrozba sa myslí napr. neoprávnený zásah (neautorizovanej) osoby alebo elektromagnetické rušenie.
- TSA CAMOSR zabezpečí, že v prípade, že sa čas, ktorý by bol uvedený v časovej pečiatke, odchýli od synchronizácie s UTC, toto sa zistí a o tejto udalosti budú informované spoliehajúce sa strany,

TSA CAMOSR zabezpečí, že bude vykonaná synchronizácia hodín v prípade, že bude notifikovaná oprávneným orgánom o výskyte opravnej sekundy.

5.9. Počítačové bezpečnostné opatrenia

Interné údaje prevádzkovateľa CA MOSR.

5.10. 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.

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.

5.11. Sieťové bezpečnostné opatrenia

Interné údaje prevádzkovateľa CA MOSR.

5.12. Opatrenia pre kryptografické moduly

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

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

6. 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.

6.1. Profil certifikátu

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

6.1.a. Certifikát TSA

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 je maximálne 6 rokov, ak nebola zmluvne dohodnutá iná lehota platnosti.

Tabuľka č. 1: Obsah položiek v certifikáte TSA MOSR

Názov položky	Skratka názvu položky	Popis položky	Príklad hodnoty položky	Typ a max. dĺžka položky
countryName (Štát)	C	Dvojznaková skratka štátu, údaj je povinný	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	6.spojp	UTF8String 64 znakov
commonName (Meno a priezvisko)	CN	Meno OCSP, údaj je povinný	tsa.mil.sk	UTF8String 64 znakov
organizationIdentifier (Identifikátor organizácie)	2.5.4.97	Odkaz na IČO Ministerstva obrany SR.	"NTRSK-30845572".	UTF8String
email (Elektronická adresa)	E	E-mail, údaj je nepovinný	pki@mil.sk	UTF8String 64 znakov

Tabuľka č. 2: Použité rozšírenia v certifikáte TSA MOSR

Názov rozšírenia	Hodnota rozšírenia	Kritičnosť
CertificatePolicies	Policy Identifier= 0.4.0.2023.1.1 Policy Identifier= 1.3.158.30845572.1.7.3.1 CPS= http://pki.mil.sk/CAMOSR/CP2.pdf Policy Identifier= 1.3.158.30845572.1.7.3.2 CPS= http://pki.mil.sk/CAMOSR/CPS_TSA.pdf	nekritické
KeyUsage	Non-Repudiation	nekritické
subjectKeyIdentifier	určí sa výpočtom	nekritické
BasicConstraints	Subject Type=End Entity Path Length Constraint=None	kritické
ExtendedKeyUsage	Time Stamping (1.3.6.1.5.5.7.3.8)	kritické

6.2. Profil OCSP

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

Tabuľka č. 3: 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

6.3. Profil zoznamu zrušených certifikátov

CRL vydávané CAMOSR sú CRL verzie 2.

CRL budú vydávané tou istou CAMOSR ako certifikáty.

Tabuľka č. 4: Použité rozšírenia (CRL extensions) v kvalifikovanom CRL

Názov rozšírenia	Hodnota rozšírenia	Kritickosť
authorityKeyIdentifier	určí sa výpočtom	nekritické

7. Administrácia špecifikácií

7.1. Procedúry na zmenu špecifikácie

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

Zriaďovateľ 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.

7.2. Procedúry pre zverejňovanie a upozornenie

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

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

7.3. Úľavy

PMA má právo rozhodnúť, či je odchýlka v praxi TSA 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 certifikáty a má sa buď iniciovať zmena do tohto dokumentu alebo sa má pre platnosť danej úľavy stanoviť konkrétny časový limit.

7.4. Súlad s právnymi požiadavkami

TSA CAMOSR zabezpečuje súlad svojej činnosti s právnymi požiadavkami. Výkon služby časovej pečiatky sa riadi platnou legislatívou Slovenskej republiky so zreteľom na zákon 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).

TSA CAMOSR zabezpečuje, že:

- sú splnené právne požiadavky legislatívy Európskej únie tak, ako sú premietnuté v legislatíve Slovenskej republiky,
- v rámci TSA CAMOSR sú uplatňované príslušné technické a organizačné opatrenia proti neoprávnenému a nezákonnému spracovávaniu osobných údajov a proti náhodnej strate, poškodeniu alebo zničeniu osobných údajov, ktoré uplatňuje CAMOSR,
- informácie poskytnuté žiadateľmi o služby TSA CAMOSR sú chránené pred ich zverejnením, s výnimkou, že na to dá súhlas žiadateľ, alebo to prikáže súd, alebo iný kompetentný štátny orgán.

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 PRIEZVISKO a Meno		Dátum a čas prevzatia			Podpis oprávnenej osoby na prevzatie	Poznámka
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		