VOJENSKÝ ÚTVAR 8116
TRENČÍN
ZaSKIS-56/204

Trenčín, 31 marca 2014
Výtlačok jediný.
Počet listov: 13

Schvaľujem:
plk. PaedDr. Marián PEŤOVSKÝ, PhD.
riaditeľ
Bezpečnostný úrad MO SR

CAMOSR
Politika časovej pečiatky

Oblasť: Administratívna bezpečnosť PKI / ZEP
Spracovateľ: Odbor informačnej bezpečnosti / SkBTP
Verzia: 2.8
Dátum platnosti: 01. APR. 2014

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

História zmien

Verzia	Dátum	Opis revízie
0.1.	10.10.2005	prvý návrh - pripomienkovanie
1.0.	26.10.2005	na schválenie
1.1.	14.11.2005	schválený
2.0.	26.7.2006	zrevidovaný
2.1.	17.10.2006	po jazykovej korektúre
2.2.	15.12.2008	aktualizácia údajov
2.3.	30.11.2009	zrevidovaný, úprava VÚ
2.4.	1.3.2011	formálna revízia, zmena OID
2.5.	19.8.2011	zrevidovaný
2.6.	6.7.2012	zmena OID CP CAMOSR
2.7.	1.3.2013	zrevidovaný
2.8.	25.3.2014	zrevidovaný

Obsah

1. Zoznam obrázkov a tabuliek

Obrázky

Tento dokument neobsahuje obrázky.

Tabuľky

2. Úvod

Služba časovej pečiatky vydáva časovú pečiatku, ktorá priraďuje dátum a čas k dokumentu v elektronickej podobe v prísnom kryptografickom režime.

Časovú pečiatku je možné neskôr použiť na preukázanie skutočnosti, že elektronický dokument (alebo elektronický podpis) existoval pred určitým konkrétnym časovým momentom uvedeným v časovej pečiatke. Elektronický dokument a časová pečiatka spolu tvoria nezvratný dôkaz v prípade akejkoľvek snahy o spochybnenie existencie duševného vlastníctva uvedeného v dokumente v danom čase.

Politika časovej pečiatky (ďalej len politika) certifikačnej autority Ministerstva obrany Slovenskej republiky (ďalej len CAMOSR) je súhrn pravidiel, ktoré stanovujú použiteľnosť časovej pečiatky pre definovaný okruh užívateľov a triedy aplikácií so spoločnými bezpečnostnými požiadavkami.

Politika presne určuje účastníkov procesu vydávania časovej pečiatky, ich zodpovednosť, práva a rozsah použitia časovej pečiatky.

Opísaná politika určuje žiadateľovi a spoliehajúcej sa strane zásady prevádzkovania a riadenia služby časovej pečiatky, ktoré vytvárajú ich primeranú dôveru k činnosti CAMOSR v tejto oblasti.

Požiadavky tejto politiky sú zamerané na službu časovej pečiatky použitú na podporu kvalifikovaných elektronických podpisov alebo na ľubovoľnú aplikáciu vyžadujúcu dôkaz, že informácia existovala pred daným časom, pričom sú tieto založené na použití kryptografie verejných kľúčov, certifikátov verejných kľúčov a na spoľahlivom časovom zdroji.

3. Pojmy a skratky

3.1. Pojmy

Časová pečiatka – informácia pripojená alebo inak logicky spojená s elektronickým dokumentom vyhovujúca požiadavkám § 9 zákona č. 215/2002 Z. z. o elektronickom podpise, 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, sa označuje skratkou TSA (Time Stamp Authority). Podľa zákona č. 215/2002 o elektronickom podpise ju môže vyhotoviť iba akreditovaná certifikačná autorita s 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 pomocou hašovacej funkcie z dokumentu resp. súboru.

Žiadateľ – právnická osoba 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 hašovacej funkcie.

3.2. Skratky

CA – Certifikačná autorita

MOSR – Ministerstvo obrany Slovenskej republiky

NBÚ – Národný bezpečnostný úrad

TSA – Vydavateľ časovej pečiatky (Time Stamp Authority)

UTC – Univerzálny svetový čas (Coordinated Universal Time)

4. Všeobecné ustanovenia

4.1. Služba poskytovania časovej pečiatky

Služba poskytovania časovej pečiatky vydavateľom časovej pečiatky (ďalej TSAMOSR) sa skladá z dvoch neoddeliteľných zložiek, ktorými sú:

- poskytovanie časovej pečiatky – zložka, ktorá vytvára samotnú časovú pečiatku,
- riadenie vyhotovovania časovej pečiatky – zložka, ktorá monitoruje a kontroluje priebeh vyhotovovania časovej pečiatky, aby sa zabezpečilo, že táto služba je poskytovaná podľa pravidiel stanovených TSAMOSR.

Druhá zložka služby je zároveň zodpovedná za inštaláciu a odinštalovanie služby poskytovania časovej pečiatky.

4.2. Vydavateľ časovej pečiatky

Vydavateľom časovej pečiatky podľa tejto politiky je:

Adresa:	**VÚ 8116 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)960 406 400, 406 351-5**
fax:	**+421 (0)960 406 420**
Mimopracovný čas	
telefón:	**+421 (0)960 406 400, 40 22 00 (DRKIS)**
fax:	**+421 (0)960 406 420 (DRKIS)**

Všetky otázky, sťažnosti a reklamácie týkajúce sa poskytovania služby časovej pečiatky je potrebné zasielať písomne na uvedenú adresu, pričom certifikačná autorita podporuje elektronickú výmenu takýchto informácií.

CAMOSR preberá celú zodpovednosť za poskytovanie služby časovej pečiatky tak, ako je stanovená v ods. 4.1.

Na vytvorenie časovej pečiatky je použitý privátny kľúč TSAMOSR a v tele časovej pečiatky je identifikácia TSAMOSR ako vydavateľa časovej pečiatky.

TSAMOSR nevyužíva žiadnu ďalšiu stranu pri poskytovaní služieb časovej pečiatky.

Na poskytovanie časovej pečiatky využíva TSAMOSR zariadenie certifikované podľa štandardu FIPS 140-2 level 3.

Všetky zmeny týkajúce sa kontaktných údajov budú ihneď zverejnené na webovej stránke CAMOSR.

4.3. Užívateľ časovej pečiatky

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

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

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

5. Politika časovej pečiatky

5.1. Prehľad

Politika časovej pečiatky je súhrn pravidiel, ktoré stanovujú použiteľnosť časovej pečiatky pre definovaný okruh užívateľov a/alebo triedy aplikácií so spoločnými bezpečnostnými požiadavkami.

Tento dokument určuje politiku TSAMOSR a prostredníctvom nej požiadavky na TSAMOSR, ktorá vydáva časové pečiatky používajúce kvalifikované certifikáty vydané CAMOSR.

5.2. Identifikácia

Politika časovej pečiatky CAMOSR je identifikovaná týmto identifikátorom (OID):

Názov:	**Politika časovej pečiatky CAMOSR**
Skratka názvu:	**TSA CP CAMOSR**
Verzia:	**Marec 2013**
Tomuto dokumentu je priradený identifikátor objektu (OID):	**1.3.158.30845572.1.7.1.17**

5.3. Užívatelia a platnosť politiky časovej pečiatky

Táto politika má za cieľ vyhovieť požiadavkám na službu časovej pečiatky pre zaručený elektronický podpis v súlade s požiadavkami zákona č. 215/2002 Z. z. o elektronickom podpise a jeho vykonávacích vyhlášok (pozri ods. 3).

Táto politika je použiteľná pre službu časovej pečiatky pre uzatvorenú skupinu.

Službu časovej pečiatky poskytuje TSAMOSR v rámci CAMOSR bezplatne.

5.4. Zhoda

TSAMOSR používa vo vyhotovovaných časových pečiatkach identifikáciu politiky časových pečiatok podľa ods. 5.2 a je schopná preukázať, že si plní povinnosti podľa ods. 6.1 a má zavedené kontroly podľa ods. 7.

6. Povinnosti a zodpovednosť pri poskytovaní a používaní služby časovej pečiatky

6.1. Povinnosti poskytovateľa služby časovej pečiatky

6.1.1. Všeobecne

TSAMOSR, ako poskytovateľ služby časovej pečiatky, sa zaväzuje:

- uskutočňovať všetky príslušné požiadavky kladené na TSA uvedené v ods. 7,
- zabezpečiť súlad praxe TSA s procedúrami predpísanými touto politikou a ďalšími súvisiacimi dokumentmi,
- poskytovať služby časovej pečiatky v súlade s prevádzkovou smernicou TSA a ďalšími súvisiacimi dokumentmi.

6.1.2. Povinnosti poskytovateľa služby časovej pečiatky voči žiadateľovi

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

6.2. Povinnosti žiadateľa

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

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

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

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.

6.3. Povinnosti spoliehajúcich sa strán

Spoliehajúce sa strany majú tieto povinnosti, ktoré musia vykonať, ak sa chcú spoliehať na časovú pečiatku:

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

6.4. Zodpovednosť

Právna zodpovednosť TSAMOSR je daná platnou legislatívou Slovenskej republiky.

7. Požiadavky kladené na výkon služby časovej pečiatky (TSA)

Poskytovateľ časovej pečiatky TSAMOSR má zavedený systém poskytovania služby vyhovujúci požiadavke zákona č. 215/2002 Z.z. a jeho vykonávacích predpisov.

7.1. Vyhlásenie o výkone služby a o zverejňovaných informáciách

7.1.1. Vyhlásenie o výkone služby

TSAMOSR zabezpečuje nevyhnutnú spoľahlivosť pri poskytovaní služby časovej pečiatky týmito opatreniami:

- má vypracované pravidlá na výkon služby časovej pečiatky a procedúry, resp. pracovné postupy, používané na naplnenie všetkých požiadaviek určených v tejto politike,
- poskytovať príslušné časti svojich pravidiel na výkon služby časovej pečiatky a ďalšie potrebné dokumenty všetkým žiadateľom o službu časovej pečiatky ako aj spoliehajúcim sa stranám,

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

- zverejňovať podmienky týkajúce sa použitia služieb časovej pečiatky podľa časti 7.1.2 pre všetkých žiadateľov a potenciálne spoliehajúce sa strany,
- schvaľovať všetky dokumenty opisujúcich pravidiel na výkon činností spojených so službou časovej pečiatky zodpovednými pracovníkmi vedenia CAMOSR,
- zabezpečiť prostredníctvom vedenia CAMOSR riadneho zavedenia a používania všetkých postupov a praktík TSAMOSR,
- definovať postupy preskúmania praktík TSAMOSR vrátane zodpovedností pri udržiavaní úrovne poskytovaných služieb,
- sprístupniť všetky zmeny týkajúce sa pravidiel na výkon činností súvisiacich s poskytovaním služieb časovej pečiatky, okamžite po schválení zodpovednými pracovníkmi, všetkým dotknutým stranám.

7.1.2. Zverejňované informácie

TSAMOSR sprístupňuje všetkým žiadateľom a spoliehajúcim sa stranám podmienky poskytovania služieb časovej pečiatky.

Zverejňované informácie obsahujú:

a) kontaktné informácie,
b) používanú politiku časovej pečiatky,

c) používaný algoritmus hašovacej funkcie,
d) životnosť kľúčov používaných na vyhotovovanie časovej pečiatky,
e) presnosť času vo vyhotovovanej časovej pečiatke s ohľadom na UTC,
f) akékoľvek obmedzenia týkajúce sa používania služby časovej pečiatky,
g) povinnosti žiadateľa,
h) povinnosti spoliehajúcich sa strán,
i) informácie o spôsobe overovania časovej pečiatky tak, aby spoliehajúca sa strana ju mohla považovať za „primerane spoľahlivú“ a akékoľvek obmedzenia trvania platnosti,
j) lehotu uchovávania záznamov TSAMOSR,
k) príslušné právne predpisy,
l) obmedzenia zodpovednosti,
m) postupy podávania sťažností a urovnávania sporov,
n) či bola TSAMOSR posudzovaná vzhľadom na svoju politiku časových pečiatok.

Uvedené informácie sú k dispozícii trvale prostredníctvom webu CAMOSR.

Je ich možné získať v elektronickej podobe stiahnutím z web stránok CAMOSR.

Za ich základný zdroj sa považuje tento dokument.

7.2. Manažment životného cyklu kľúčov

7.2.1. Generovanie kľúčov

TSAMOSR zabezpečuje, že všetky kryptografické kľúče používané počas výkonu služby časovej pečiatky sú generované za kontrolovaných okolností v bezpečnom zariadení a vo fyzicky bezpečnom prostredí (pozri ods. 7.4.4) dôveryhodnými a kvalifikovanými osobami (pozri ods. 7.4.3) za prítomnosti a pod kontrolou stanoveného počtu osôb.

7.2.2. Ochrana súkromného kľúča TSAMOSR

TSAMOSR zabezpečuje, že jej súkromný kľúč zostane tajný a zostane zachovaná jeho integrita.

Súkromný podpisový kľúč TSAMOSR je generovaný, uchovávaný a používaný v kryptografickom module, ktorý vyhovuje požiadavkám daným štandardom FIPS 140-2 level 3 a je certifikovaný na NBÚ SR ako produkt pre poskytovateľov certifikačných služieb.

7.2.3. Distribúcia verejného kľúča TSAMOSR

TSAMOSR zaručí, že integrita a dôveryhodnosť verejného verifikačného kľúča TSA MOSR bude zachovaná počas jeho distribúcie k spoliehajúcim sa stranám a to najmä:

- verejný verifikačný kľúč TSAMOSR je k dispozícii pre spoliehajúce sa strany prostredníctvom certifikátu verejného kľúča,
- certifikát TSAMOSR je vydaný CAMOSR ako kvalifikovaný certifikát,
- certifikát je vydaný certifikačnou autoritou, ktorej certifikačná politika poskytuje rovnakú alebo vyššiu úroveň bezpečnosti, ako má táto politika časovej pečiatky.

7.2.4. Obnovovanie kľúča TSAMOSR

Životnosť certifikátu TSAMOSR nie je dlhšia ako časový interval, počas ktorého zvolený algoritmus a dĺžka kľúča sú vhodné na daný účel.

7.2.5. Skončenie životnosti kľúčov TSAMOSR

TSAMOSR sa zaručuje, že súkromný podpisový kľúč TSA sa nebude používať po skončení jeho životnosti.

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

TSAMOSR zabezpečuje bezpečnosť kryptografického hardvéru (hardvérový modul na podpisovanie časovej pečiatky) počas celej jeho životnosti.

7.3. Vytváranie časovej pečiatky

7.3.1. Časová pečiatka

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

Predovšetkým:

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

g) časová pečiatka sa podpisuje kľúčom TSAMOSR, ktorý je používaný len na tento účel,
h) certifikát časovej pečiatky obsahuje:
    - identifikáciu Slovenskej republiky ako krajiny, v ktorej pôsobí TSA CAMOSR,
    - identifikáciu TSA CAMOSR.

7.3.2. Vyhotovenie a overenie časovej pečiatky

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

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

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

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

Časová pečiatka je platná, ak:

- zaručený elektronický podpis časovej pečiatky je platný,
- časová pečiatka je v súlade s použitou politikou časových pečiatok.

7.3.3. Synchronizácia času s UTC

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

a) kalibrácia hodín TSAMOSR sa vykonáva tak, že očakávaná odchýlka času nie je mimo deklarovanej presnosti,
b) hodiny zariadenia TSAMOSR sú chránené proti hrozbám, ktoré by mohli viesť k nezistiteľným zásahom do hodín, ktoré by mohli mať za následok ich odchýlku od kalibrácie,
c) TSAMOSR zabezpečuje, že v prípade, ak sa čas, ktorý by bol uvedený v časovej pečiatke, odchýli od synchronizácie s UTC, táto skutočnosť sa zistí a časová pečiatka nebude vydaná,
d) TSAMOSR zabezpečí, aby bola vykonaná synchronizácia hodín v prípade, ak bude notifikovaná oprávneným orgánom o výskyte opravnej sekundy.

7.3.4. Profil certifikátu časovej pečiatky

Tabuľka č. 1: Použité rozšírenia (certificate extensions) certifikátu časovej pečiatky CAMOSR

Názov rozšírenia	Hodnota rozšírenia	Kritičnosť
AuthorityInfoAccess	URL=http://pki.mil.sk/camosr2.cer	nekritické
AuthorityKeyIdentifier	KeyID = určí sa výpočtom Certificate Issuer= Directory Address vydavateľa certifikátu CA Certificate SerialNumber= SerialNumber vydavateľa certifikátu CA	nekritické
CertificatePolicies	Policy Identifier=1.3.158.36061701.0.0.0.1.2.2 Policy Identifier= 1.3.158.30845572.1.7.1.17 CPS= http://pki.mil.sk/TSA_CP.pdf Policy Identifier= 1.3.158.30845572.1.7.1.19 CPS= http://pki.mil.sk/ACA2/CP2.pdf	nekritické
crlDistributionPoints	URI: http://pki.mil.sk/ACA2/camosr2.crl URI: http://crl.mil.sk/ACA2/camosr2.crl	nekritické
KeyUsage	Non-Repudiation	nekritické
subjectKeyIdentifier	určí sa výpočtom	nekritické
BasicConstraints	Subject Type=End Entity Path Length Constraint=None	kritické
ExtendedKeyUsage	Time Stamping (1.3.6.1.5.5.7.3.8)	kritické

7.4. Manažment a prevádzka TSAMOSR

7.4.1. Manažment bezpečnosti

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

a) TSAMOSR preberá celú zodpovednosť za všetky aspekty poskytovania služby týkajúce sa časovej pečiatky opisované v tejto politike,
b) TSAMOSR poskytuje smernice o informačnej bezpečnosti prostredníctvom svojho vedenia, ktoré je zodpovedné za definovanie informačnej bezpečnosti.
c) s touto politikou sú oboznámení všetci pracovníci, ktorých sa uvedená politika týka,
d) infraštruktúra informačnej bezpečnosti nevyhnutná na zabezpečenie bezpečnosti v rámci TSAMOSR sa udržiava počas celej činnosti TSAMOSR,
e) akékoľvek zmeny, ktoré by mohli ovplyvniť úroveň bezpečnosti, sú odsúhlasené vedením CAMOSR,

f) bezpečnostné opatrenia a pracovné postupy TSAMOSR, systémové a informačné aktíva poskytujúce služby časovej pečiatky sú dokumentované, zavedené a udržiavané.

7.4.2. Klasifikácia a manažment aktív

TSAMOSR zabezpečuje, že jej informačné a ďalšie aktíva sú chránené na požadovanej úrovni, a to predovšetkým:

a) TSAMOSR má zoznam všetkých aktív a ich klasifikáciu z pohľadu požiadaviek na ochranu, ktoré sú v súlade s vykonanou analýzou rizík.

7.4.3. Personálna bezpečnosť

TSAMOSR zabezpečuje, že postupy personálnej práce podporujú jej dôveryhodnosť.

Predovšetkým:

a) prevádzkou TSAMOSR sú poverení pracovníci, ktorí majú zodpovedajúce znalosti, skúsenosti a nevyhnutnú kvalifikáciu pre poskytované služby, a ktorí sú vhodní na danú pracovnú pozíciu,
b) TSAMOSR z organizačného hľadiska pozostáva z úrovní (role), kde pod pojmom rola (úroveň) sa rozumie skupina osôb, ktoré vykonávajú buď tie isté činnosti, alebo činnosti z nejakého aspektu príbuzné, pričom pri niektorých osobitne dôležitých činnostiach sa vyžaduje, aby pri ich vykonávaní bolo prítomných viacero osôb zastávajúcich danú rolu (tzv. princíp “k” z “n”),
c) dôveryhodné úrovne (role) a ich zodpovednosť sú opísané v prevádzkových smerniciach a prípadne v ďalších dokumentoch a tie úrovne (role), na ktorých je závislá bezpečnosť TSAMOSR, sú jasne identifikované,
d) jednotlivé dôveryhodné roly v rámci TSAMOSR majú opisy práce definované z hľadiska rozdelenia povinností a minimálnych privilégií, stanovenia citlivosti pozície z hľadiska zodpovednosti a úrovne prístupových práv, ich predchádzajúcej praxe a úrovne zaškolenia a povedomia,
e) pracovníci uplatňujú administratívne a manažérske postupy a procedúry, ktoré sú v súlade s procedúrami manažmentu informačnej bezpečnosti (pozri ods. 7.4.1).

7.4.4. Fyzická a priestorová bezpečnosť

TSAMOSR zabezpečuje, že fyzický prístup k jej kritickým aktívam je kontrolovaný a riziko neoprávneného fyzického prístupu je minimalizované.

Predovšetkým:

a) na poskytovanie aj na manažovanie časovej pečiatky:
   - fyzický prístup do priestorov týkajúcich sa služby časovej pečiatky je umožnený len autorizovaným osobám,
   - je zavedená kontrola, ktorá zabráni stratám, poškodeniu alebo kompromitácii aktív a prerušeniu obchodných aktivít,
   - je zavedená kontrola, ktorá zabráni prezradeniu alebo odcudzeniu informácií alebo zariadení spracúvajúcich alebo obsahujúcich informácie,
b) je implementovaná kontrola prístupu ku kryptografickému modulu, aby sa zaručili požiadavky kladené na bezpečnosť kryptografického modulu podľa ods. 7.2.1 a 7.2.2.,
c) všetko vybavenie používané na poskytovanie služby týkajúcej sa časovej pečiatky je prevádzkované v prostredí, ktoré fyzicky chráni toto vybavenie pred kompromitáciou prostredníctvom neautorizovaného prístupu k systémom alebo k dátam,
d) je implementované riadenie fyzickej a priestorovej bezpečnosti, aby sa ochránilo vybavenie, kde sú lokalizované systémové zdroje, samotné systémové zdroje a podporné vybavenie.

7.4.5. Prevádzkový manažment

TSAMOSR zabezpečuje, že systémové komponenty sú bezpečné a pracujú správne, s minimálnym rizikom poruchy.

Predovšetkým:

a) integrita systémových komponentov TSAMOSR je chránená proti vírusom, škodlivému a neautorizovanému softvéru,
b) zaznamenávanie incidentov a postupy reakcií na incidenty sú zavedené takým spôsobom, aby sa minimalizovali škody z bezpečnostných incidentov a zlyhaní,
c) s médiami používanými v rámci dôveryhodného TSAMOSR systému sa zaobchádza takým spôsobom, aby sa predišlo ich poškodeniu, odcudzeniu, neautorizovanému prístupu k nim a ich zastaraniu.

7.4.6. Manažment prístupu k systému

TSAMOSR zaisťuje, že prístup k systému je vyhradený len autorizovaným osobám.

Predovšetkým:

a) je implementovaná ochrana, ktorá zabráni neautorizovanému prístupu cez sieť,
b) TSAMOSR zaisťuje efektívnu administráciu prístupu používateľov (vrátane používateľov v dôveryhodných rolách) na udržiavanie bezpečnosti systému,
c) nepretržite je používané monitorovacie a poplašné vybavenie, aby bolo možné detegovať a registrovať neautorizované pokusy o prístup k systémom TSA a vhodným spôsobom na ne reagovať.

7.4.7. Nasadenie a údržba dôveryhodných systémov

TSAMOSR používa dôveryhodné systémy a produkty, ktoré sú chránené pred modifikáciou.

Na vykonávanie zmien (napr. aktualizácie, patche, fixy a pod.) používaného softvéru sa používajú ustálené procedúry alebo postupy odporúčané výrobcom softvéru.

7.4.8. Kompromitácia služieb TSA MOSR

TSAMOSR 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.

7.4.9. Skončenie činnosti TSA MOSR

TSAMOSR zabezpečuje, že prípadné narušenie služieb žiadateľom a spoliehajúcim sa stranám v dôsledku zastavenia služby poskytovania časovej pečiatky je minimalizované a najmä zabezpečí následnú podporu vo forme informácií požadovaných na overenie platnosti časových pečiatok.

7.4.10. Súlad s právnymi požiadavkami

TSAMOSR zabezpečuje súlad svojej činnosti s právnymi požiadavkami. Výkon služby časovej pečiatky sa riadi platnou legislatívou Slovenskej republiky so zreteľom na zákon č. 215/2002 Z. z. o elektronickom podpise a súvisiace vyhlášky (vyhlášky NBÚ č. 131/2009 Z. z., 132/2009 Z. z., 133/2009 Z. z., 134/2009 Z. z., 135/2009 Z. z., 136/2009 Z. z., 32/2010 Z. z.)

Popri tom:

a) sú splnené právne požiadavky legislatívy Európskej únie tak, ako sú premietnuté v slovenskej legislatíve,
b) v rámci TSAMOSR 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,
c) informácie poskytnuté žiadateľmi o služby TSAMOSR sú chránené pred zverejnením, ak na to nedá súhlas žiadateľ alebo to neprikáže súd alebo iný kompetentný štátny orgán.

7.4.11. Zaznamenávanie údajov týkajúcich sa výkonu služby časovej pečiatky

TSAMOSR zabezpečuje, že všetky dôležité informácie týkajúce sa výkonu služby časovej pečiatky sú zaznamenávané a uchovávané počas stanovenej lehoty, najmä s cieľom poskytnúť dôkazy na účely prípadných právnych konaní.

Predovšetkým:

a) TSAMOSR dokumentuje, ktoré konkrétne prípady a údaje sa majú zaznamenávať,
b) je udržiavaná dôvernosť a celistvosť súčasných a archivovaných záznamov týkajúcich sa činnosti služby časovej pečiatky,
c) záznamy týkajúce sa činnosti služby časovej pečiatky sú bezpečne a kompletne archivované v súlade so zverejnenými praktikami,
d) záznamy týkajúce sa činnosti služby časovej pečiatky sú k dispozícii v prípade požiadavky kladenej na poskytnutie dôkazov správnosti výkonu činnosti služby časovej pečiatky v prípade právnych úkonov,
e) je zaznamenávaný presný čas významných udalostí týkajúcich sa prostredia TSAMOSR, manažmentu kľúčov a synchronizácie času,
f) záznamy týkajúce sa činnosti služby časovej pečiatky sú uchovávané počas primeranej lehoty po vypršaní platnosti podpisového kľúča TSAMOSR, aby bolo možné poskytnúť právny dôkaz a ako je to uvedené vo vyhlásení o zverejňovaní informácií (pozri ods. 7.1),
g) udalosti sa zaznamenávajú takým spôsobom, aby tieto záznamy nemohli byť ľahko zmazané alebo zničené a sú uchovávané počas lehoty, ktorá je na ich uchovávanie požadovaná,
h) akékoľvek informácie o žiadateľovi sa uchovávajú ako dôverné okrem prípadov, keď existuje súhlas žiadateľa s ich publikovaním alebo okrem prípadov uvedených v ods. 7.4.10,
i) sú zaznamenávané všetky záznamy týkajúce sa všetkých udalostí majúcich vzťah k životnému cyklu kľúčov TSAMOSR,
j) sú zaznamenávané všetky záznamy týkajúce sa všetkých udalostí majúcich vzťah k životnému cyklu certifikátov TSAMOSR,
k) sú zaznamenávané všetky záznamy týkajúce sa všetkých udalostí majúcich vzťah k synchronizácii hodín TSAMOSR,
l) sú zaznamenávané všetky záznamy týkajúce sa všetkých udalostí majúcich vzťah k detegovaniu straty synchronizácie hodín.

7.5. Organizačné aspekty

TSAMOSR zaisťuje, že jej organizácia je spoľahlivá, pričom kladie dôraz na zaistenie, že:

a) politika a postupy používané TSAMOSR nie sú diskriminačné,
b) umožní prístup k svojim službám žiadateľom, ktorých aktivity patria do oblasti jej pôsobnosti, a ktorí súhlasia s dodržiavaním svojich povinností tak, ako sú špecifikované v tomto dokumente,
c) má systém pre manažment kvality a informačnej bezpečnosti vhodný na poskytovanie služieb týkajúcich sa časovej pečiatky,
d) má primerané prostriedky na pokrytie svojej zodpovednosti vyplývajúcej z výkonu svojich činností,

e) je finančne stabilná a má zdroje požadované na výkon činností v súlade s touto politikou,

f) zamestnáva dostatočný počet pracovníkov, ktorí majú nevyhnutné vzdelanie, zácvik, technické znalosti a skúsenosti týkajúce sa poskytovania služby súvisiacej s časovou pečiatkou,

g) má postup riešenia sťažností a podnetov od žiadateľov alebo iných strán týkajúceho sa poskytovania služby časovej pečiatky alebo iných súvisiacich služieb.

8. Odkazy

Táto politika vychádza z:

- ETSI TS 102 023 V1.2.2 (2008-10) „Policy requirements for time-stamping authorities“
- RFC 3628, November 2003 „Policy requirements for time-stamping authorities (TSAs)“
- RFC 3161, August 2001 „Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)“
- Zákon č. 215/2002 Z. z. o elektronickom podpise a súvisiace vyhlášky (vyhlášky NBÚ č. 131/2009 Z. z., 132/2009 Z. z., 133/2009 Z. z., 134/2009 Z. z., 135/2009 Z. z. a 136/2009 Z. z.)