Zmluva o poskytovaní kvalifikovanej dôveryhodnej služby vyhotovovania kvalifikovaných elektronických časových pečiatok

uzatvorená podľa § 51 zákona č. 40/1964 Zb. (Občiansky zákonník) v spojení s § 11 ods. 2 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) (ďalej len „zmluva“)

Názov:	**Národný bezpečnostný úrad**
Sídlo:	Budatínska 30, 851 06 Bratislava
IČO:	36061701
Štatutárny zástupca:	Ing. Jozef Magala, riaditeľ
Zastúpený:	Mgr. Jana Lukáčová, riaditeľka sekcie ekonomiky a prevádzky na základe plnomocenstva riaditeľa Národného bezpečnostného úradu č. 05671/2017/KÚ/OLP-002 zo dňa 04.08.2017

(ďalej len „poskytovateľ“)

a

Názov:	**Ministerstvo školstva, vedy, výskumu a športu Slovenskej republiky**
Sídlo:	Stromová 1, 813 30 Bratislava
IČO:	00164381
Štatutárny zástupca:	JUDr. Mgr. Martina Lubyová, PhD., ministerka

(ďalej len „nadobúdateľ“)
(poskytovateľ a nadobúdateľ ďalej spolu len „zmluvné strany“ alebo jednotlivo „zmluvná strana“)

Čl. I
Predmet zmluvy

1. Predmetom tejto zmluvy je poskytovanie kvalifikovanej dôveryhodnej služby vyhotovovania kvalifikovaných elektronických časových pečiatok[1] (ďalej len „dôveryhodná služba“) v súlade s certifikačnou politikou pre kvalifikovanú dôveryhodnú službu vyhotovovania kvalifikovaných elektronických časových pečiatok[2], zverejnenou na webovom sídle poskytovateľa a za podmienok ustanovených touto zmluvou.

[1] V zmysle Článku 3 ods. 34 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
[2] http://ep.nbu.gov.sk/snca/cp.html

Čl. II
Práva a povinnosti zmluvných strán

1. Poskytovateľ ako prevádzkovateľ Slovenskej národnej certifikačnej autority sa zaväzuje poskytovať nadobúdateľovi dôveryhodnú službu a nadobúdateľ túto službu prijíma.
2. Kontaktnou osobou pre plnenie tejto zmluvy je za poskytovateľa riaditeľ odboru prevádzky sekcie ekonomiky a prevádzky a za nadobúdateľa riaditeľ odboru hospodárskej správy a krízového manažmentu.
3. Zmluvné strany sa zaväzujú bez zbytočného odkladu navzájom si oznamovať všetky skutočnosti, ktoré by mohli mať vplyv na riadne plnenie tejto zmluvy. V prípade zmeny kontaktných osôb podľa tohto článku zmluvy je zmluvná strana povinná túto zmenu bezodkladne písomne oznámiť druhej zmluvnej strane.

Čl. III
Technická špecifikácia

1. Dôveryhodná služba bude poskytovaná v súlade s nariadením Európskeho parlamentu a Rady (EÚ) č. 910/2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES (ďalej len „nariadenie (EÚ) č. 910/2014“), 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), ostatnými všeobecne záväznými právnymi predpismi SR a platnou bezpečnostnou a prevádzkovou dokumentáciou Slovenskej národnej certifikačnej autority.
2. Technickú špecifikáciu dôveryhodnej služby spolu s certifikačnou politikou pre časové pečiatky sprístupní poskytovateľ nadobúdateľovi na jeho žiadosť ešte pred podpisom tejto zmluvy, a to za účelom oboznámenia sa s technickými parametrami a postupnosťou implementácie dôveryhodnej služby do informačno-technologického prostredia nadobúdateľa.
3. Technická špecifikácia dôveryhodnej služby sa písomne vyhotoví a priloží ako Príloha č. 1 k tejto zmluve, ktorá sa stane neoddeliteľnou súčasťou tejto zmluvy.
4. Každú zmenu technickej špecifikácie dôveryhodnej služby oznámi poskytovateľ nadobúdateľovi včas vo forme písomne vyhotoveného Protokolu o zmene technickej špecifikácie.

Čl. IV
Cena

1. Dôveryhodná služba bude nadobúdateľovi poskytovaná bezodplatne.

Čl. V
Doba platnosti a účinnosti zmluvy

1. Táto zmluva nadobúda platnosť a účinnosť dňom podpisu oboma zmluvnými stranami.
2. Táto zmluva sa uzatvára na dobu neurčitú.

Čl. VI
Spoločné ustanovenia

1. Túto zmluvu možno písomne vypovedať ktoroukoľvek zmluvnou stranou bez uvedenia dôvodu. Výpovedná lehota je jeden mesiac a začína plynúť prvým dňom mesiaca nasledujúceho po doručení výpovede druhej zmluvnej strane. Zmluvu možno ukončiť aj písomnou dohodou zmluvných strán.
2. Túto zmluvu možno meniť len po vzájomnej dohode zmluvných strán vo forme očíslovaných písomných dodatkov.
3. Právne vzťahy touto zmluvou neupravené sa riadia príslušnými ustanoveniami zákona č. 40/1964 Zb. (Občiansky zákonník v znení neskorších predpisov) a ostatnými všeobecne záväznými právnymi predpismi Slovenskej republiky.
4. Táto zmluva je vyhotovená v štyroch rovnopisoch, jeden rovnopis pre poskytovateľa, tri rovnopisy pre nadobúdateľa.
5. Zmluvné strany vyhlasujú, že sa s obsahom tejto zmluvy riadne oboznámili a podmienky dohodnuté v tejto zmluve sú prejavom ich slobodnej vôle vyjadrenej zrozumiteľne, určite a vážne, čo potvrdzujú svojimi vlastnoručnými podpismi.

Prílohy zmluvy:

Príloha č. 1: Technická špecifikácia
Príloha č. 2: Certifikačná politika pre kvalifikovanú dôveryhodnú službu vyhotovovania kvalifikovaných elektronických časových pečiatok

V Bratislave dňa 2018

Poskytovateľ

Mgr. Jana Lukáčová
riaditeľka sekcie ekonomiky a prevádzky

V Bratislave dňa 2018

Nadobúdateľ

JUDr. Mgr. Martina Lubyová, PhD.
ministerka

Príloha č. 1

TECHNICKÁ ŠPECIFIKÁCIA KVALIFIKOVANEJ DÔVERYHODNEJ SLUŽBY VYHOTOVOVANIA KVALIFIKOVANÝCH ELEKTRONICKÝCH ČASOVÝCH PEČIATOK

1. Rozhranie pre poskytovanie služby časovej pečiatky: podľa RFC 3161

2. Platnosť certifikátov serverov časovej pečiatky: TSA1 – do 19.4.2020
   TSA2 – do 19.4.2020

3. Protokol pre získanie časovej pečiatky: HTTP

4. Prístupové adresy:

   TSA1 – http://ep.nbusr.sk:8080/tsa1/TSQServer
   TSA2 – http://100.112.90.40:8080/tsa1/TSQServer (z prostredia Govnet)

5. Dostupnosť služby časovej pečiatky:
   Služba časovej pečiatky bude dostupná nepretržite s vopred ohláseným výpadkom v trvaní najviac dve hodiny, mimo vzniku nepredvídateľných mimoriadnych udalostí.

6. Certifikát servera časovej pečiatky je vydaný akreditovanou certifikačnou autoritou SNCA s minimálne jednou certifikačnou politikou, pričom musí obsahovať minimálne certifikačnú politiku s OID: 1 3 158 36061701 0 0 0 1 2 2.

7. V prípade výskytu technických a bezpečnostných incidentov pri poskytovaní služby časovej pečiatky sa budú tieto incidenty riešiť a spravovať opatreniami, postupmi a pokynmi popísanými v dokumente pomenovaného ako *„Certifikačná politika pre kvalifikovanú dôveryhodnú službu vyhotovovania kvalifikovaných elektronických časových pečiatok“* v znení neskorších aktualizovaných verzií, ktorý je sprístupnený na http://ep.nbusr.sk/snca/cp.html.

8. Certifikát obsahuje minimálne tieto odkazy na získanie zoznamov zrušených certifikátov (CRL)

   [1] CRL Distribution Point
   Distribution Point Name:
   Full Name:
   URL=http://ep.nbusr.sk/snca/crls2/snca2.crl

   [2] CRL Distribution Point
   Distribution Point Name:
   Full Name:
   URL=ldap://ep.nbusr.sk/cn=SNCA,ou=SIBEP,o=Narodny bezpecnostny urad,l=Bratislava,c=SK?certificateRevocationList

NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

Verzia 1

Certifikačná politika pre kvalifikovanú dôveryhodnú službu vyhotovovania kvalifikovaných elektronických časových pečiatok

19.6.2017

Odbor prevádzky | Sekcia ekonomiky a prevádzky
Budatínska č. 30 | 851 06 Bratislava | Slovenská republika
tel.: +421 2 6869 1111 | fax: +421 2 6869 1700
e-mail: podatelna@nbu.gov.sk | http://www.nbu.gov.sk/

Obsah

1. Úvod

Tento dokument popisuje politiku poskytovania dôveryhodnej služby vyhotovovania kvalifikovaných elektronických časových pečiatok (v ďalšom aj „CP TSA“) a bezpečnostné požiadavky, ktoré sa týkajú prevádzkovej praxe a postupov pri poskytovaní tejto služby.
Účelom tohto dokumentu je definovať prezentovať metodiku, záväzné postupy a zodpovednosti prevádzkovateľa Slovenskej národnej certifikačnej autority (v ďalšom aj „SNCA“) pri vydávaní časových pečiatok, definovať úlohy, povinnosti a zodpovednosť zúčastnených strán pri používaní časových pečiatok.

Politika je záväzným dokumentom, slúžiacim ako štandard zásad, procedúr a postupov, ktoré musia dodržiavať všetky zúčastnené strany.

Poskytovateľom tejto dôveryhodnej služby je:

Názov poskytovateľa	Národný bezpečnostný úrad SR
Sídlo / poštová adresa	Budatínska 30, 851 06 Bratislava
IČO	36 061 701
Telefón	+421 2 6869 1111
Fax	+421 2 6869 1700
E-mail	podatelna@nbu.gov.sk
Webové sídlo	www.nbu.gov.sk

(ďalej len „SNCA“), prostredníctvom svojho systému autority časovej pečiatky (TSA SNCA).

Táto politika môže byť použitá pre verejnú službu poskytovanie časových pečiatok ako aj na použitie v uzavretých komunitách.

Tento dokument môže byť použitý nezávislými orgánmi ako základ pre potvrdenie, že SNCA je dôveryhodný na vyhotovovanie časových pečiatok.

Služby časovej pečiatky identifikované v tomto dokumente sú využívané v okruhu pôsobnosti SNCA zriadenej a prevádzkovanej Národným bezpečnostným úradom Slovenskej republiky.

1.1 Prehľad

Táto CP TSA sa týka poskytovania dôveryhodnej služby vyhotovovania kvalifikovanej elektronickej časovej pečiatky v zmysle ustanovení Nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014 z 3. 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 vypracovanej podľa normy EN 319411-2 - A best practices policy for time-stamp (BTSP).

Vyhotovované kvalifikované elektronické pečiatky sú podpisované s využitím súkromných kľúčov jednotiek vyhotovujúcich časové pečiatky (ďalej aj „TSU“), ktorých certifikáty môžu byť vydané výhradne týmito certifikačnými autoritami SNCA:

Názov	Sériové číslo certifikátu	Vydavateľ	DigitalID v SK dôveryhodnom zozname
SNCA2	01 26	KCA NBU SR 3	

1.2 Názov dokumentu a jeho identifikácia

Politika časových pečiatok je identifikovaná nasledovným identifikátorom odvodeným od objektového identifikátora NBÚ SR:

1.3.158.36061701.0.1.4

kde jednotlivé zložky OID majú nasledovný význam:

1	ISO
3	ISO Identified Organization
158	Slovakia
36061701	jedinečný identifikátor Národného Bezpečnostného Úradu priradený organizáciou ISO (IČO)
0	KCA (poskytovanie dôveryhodných služieb)
1	Certifikačné politiky
4	Certifikačná politika pre dôveryhodnú službu vyhotovovania kvalifikovaných elektronických časových pečiatok

1.3 Účastníci PKI

V rámci poskytovania dôveryhodných služieb vyhotovovania kvalifikovaných elektronických časových pečiatok sú účastníkmi infraštruktúry verejného kľúča Prevádzkovateľa uvedení v tejto časti.

1.3.1 Jednotka vyhotovovania časových pečiatok

Jednotka vyhotovovania časových pečiatok:

- je entita, ktorá poskytuje kvalifikované dôveryhodné služby vyhotovovania kvalifikovaných elektronických časových pečiatok používateľom (Orgány verejnej moci, Spoliehajúce sa strany),
- má celkovú zodpovednosť za poskytovanie kvalifikovaných dôveryhodných služieb špecifikovaných v odstavci 1.1,
- je uvádzaná vo vydaných časových pečiatkach ako vydavateľ a jej súkromné kľúče sú používané pri vyhotovovaní podpisu týchto časových pečiatok,
- zaručuje, že všetky aspekty jej služieb, operácií a infraštruktúry zviazanej s časovými pečiatkami vydanými podľa tejto politiky sú vykonávané v súlade s jej požiadavkami a ustanoveniami a v súlade s CPS SNCA.

TSU SNCA sú súčasťou hierarchickej PKI:

KCA NBÚ SR 3 -> SNCA 3 -> TSU

SNCAľ môže prevádzkovať v rámci podriadenosti pod certifikačnou autoritou SNCA 3 viaceré TSU poskytujúce dôveryhodné služby vyhotovovania časovej pečiatky.

1.3.2 Registračná autorita

Registračná autorita (ďalej len „RA“) je entita, ktorá koná v mene SNCA, pričom vykonáva niektoré vybrané činnosti pri poskytovaní dôveryhodných služieb SNCA.

RA musí vykonávať svoje aktivity v súlade so schválenou CP TSA a Pravidlami poskytovania dôveryhodnej služby vyhotovovania kvalifikovaných elektronických časových pečiatok (ďalej aj „CPS TSA“) v aktuálnom znení.

SNCA má v súčasnej dobe zriadenú RA pôsobiacu v sídle SNCA.

1.3.3 Klient

O vyhotovenie časovej pečiatky môže žiadať:

1. Orgány verejnej moci,

Žiadatelia o službu časovej pečiatky sú povinní:

- postupovať pri žiadosti o vydanie časovej pečiatky spôsobom predpísaným v tomto dokumente,
- používať predpísaný formát a protokol žiadosti o vydanie časovej pečiatky,
- preveriť platnosť vydanej časovej pečiatky bezprostredne po jej príjme spôsobom definovaným v týchto zásadách,
- riešiť nezrovnalosti pri vydaní časovej pečiatky s kontaktnou osobou SNCA bez zbytočných prieťahov.

1.3.4 Spoliehajúca sa strana

Spoliehajúca sa strana je ľubovoľná právnická alebo fyzická osoba, prípadne technologické zariadenie a to ako so sídlom v SR tak aj v zahraničí, ktorá na základe overovania časovej pečiatky skúma (overuje alebo verifikuje), či údaje ku ktorým existuje časová pečiatka objektívne existovali v určitom (určiteľnom) čase.

Spoliehajúce sa strany sú povinné postupovať pri overovaní časovej pečiatky v zmysle inštrukcií tohto dokumentu o overovaní časových pečiatok.

1.3.5 Iní účastníci

Žiadne ustanovenia

1.4 Použiteľnosť časovej pečiatky

Časové pečiatky vyhotovené v rámci poskytovania dôveryhodnej služby vyhotovovania časových pečiatok popísanej v tejto politike môžu orgány verejnej moci a Spoliehajúce sa strany používať bez obmedzenia všade, kde je vyžadovaná časová pečiatka definovaná v článku 42 Nariadenia eIDAS

1.5 Správa politiky

Táto politika spĺňa požiadavky štandardu ETSI TS 102 023.

1.5.1 Organizácia zodpovedná za správu dokumentu

Tento dokument je spravovaný Sekciou elektronického podpisu Národného bezpečnostného úradu SR.

Kontaktná adresa:

Národný bezpečnostný úrad SR,

Budatínska 30,

851 05 Bratislava,

Slovenská republika,

http://www.nbu.gov.sk

1.5.2 Kontaktná osoba

Bezpečnostný správca SNCA,

Národný bezpečnostný úrad SR,

Budatínska 30,

851 05 Bratislava,

Telefón: 02/6869 21 83

Fax: 02/6869 1700

e-mail: secadmin@nbu.gov.sk

1.5.3 Osoba rozhodujúca o súlade CP s certifikačnou politikou

Vo všetkých záležitostiach a aspektoch týkajúcich sa SNCA a jeho činnosti. s konečnou platnosťou rozhoduje riaditeľka sekcie ekonomiky a prevádzky.

1.5.4 Postupy schvaľovania CP a externej politiky

Ešte pred začiatkom prevádzky má mať SNCA schválený svoj CP a CPS a musí spĺňať všetky jeho požiadavky. Obsah CP a CPS schvaľuje riaditeľka sekcie ekonomiky a prevádzky.

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

1.6 Definície a skratky

1.6.1 Definície

Žiadateľ	Orgány verejnej moci, ktorým sú poskytované služby časových pečiatok na základe vzájomnej dohody.
Spoliehajúca sa strana	Ľubovoľná právnická alebo fyzická osoba, ktorá na základe overovania časovej pečiatky skúma (overuje alebo verifikuje) či údaje ku ktorým existuje časová pečiatka objektívne existovali v určitom (určiteľnom) čase.
Univerzálny koordinovaný čas	Časový údaj v „svetovom čase“ odvodený od slnečného času nultého poludníka.

1.6.2 Skratky

UTC	Univerzálny koordinovaný čas
TST	Telo časovej pečiatky (Time Stamp Token)
TSA	Vydavateľ časových pečiatok (Time Stamp Authority)
NBÚ	Národný bezpečnostný úrad
KCA	Koreňová certifikačná autorita NBÚ
SNCA	Slovenská národná certifikačná autorita NBÚ
RA	Registračná autorita SNCA
TAC	Čas na dokončenie (Time At Completion)
PMA	Autorita pre správu poriadkov (Policy Management Authority)

2. Úložiská

2.1 Zverejňovanie informácií o TSA

Zásady pre poskytovanie služby časovej pečiatky sú zverejnené na internetovej stránke NBÚ SR:

http://ep.nbusr.sk/snca/

V listinnej podobe je dokumentácia k dispozícii aj na pracovisku prevádzkovateľa SNCA.

Verejné kľúče TSA určené na overovanie časových pečiatok sú distribuované vo forme certifikátov vydaných SNCA. Prostriedkami na distribúciu certifikátov verejných kľúčov TSA určených na overovanie časových pečiatok cez

a) adresárové služby dostupné na adrese:

   ldap://ldap.nbusr.sk/cn=snca,ou=SIBEP,o=Narodny bezpecnostny urad,l=Bratislava,c=sk?certificateRevocationList

b) samostatne na webovom sídle:

   http://ep.nbu.gov.sk/snca/ts.html

Miestom zverejňovania certifikátov verejných kľúčov TSA určených na overovanie časových pečiatok je webové sídlo:

http://ep.nbusr.sk/snca/cert_TSA.html

Aktuálny zoznam zrušených certifikátov je publikovaný v súbore na internetovej stránke:

http://ep.nbusr.sk/snca/crls2/snca2.crl

2.2 Frekvencia zverejňovania informácií

Zoznam zrušených certifikátov (CRL) musí byť publikovaný ako je špecifikované v aktuálnom CP pre vyhotovovanie kvalifikovaných certifikátov. Informácie o zrušenom certifikáte TSU musia byť dostupné na webovom sídle SNCA (pozri kapitola 2.1), ktorý slúži ako jeho úložisko.

CP TSA sa musí zverejniť čo najskôr po ich schválení a vydaní.

Všetky ďalšie informácie, ktoré majú byť publikované v úložisku, sa musia publikovať podľa možnosti čo najskôr.

2.3 Kontroly prístupu

V záujme ochrany informácií uložených v úložisku, ktoré nie sú určené na verejné rozšírenie musí SNCAĽ:

- vynaložiť maximálne úsilie na to, aby zaistil integritu, dôvernosť a dostupnosť dát vyplývajúcich s poskytovaných dôveryhodných služieb,
- vykonať logické a bezpečnostné opatrenia, aby zabránil neautorizovanému prístupu k úložisku osobám, ktoré by mohli akýmkoľvek spôsobom zmeniť, poškodiť, pridať resp. vymazať údaje uložené v úložisku.

3. Všeobecné ustanovenia

Služba časových pečiatok poskytuje žiadateľovi časový údaj logicky prepojený s údajmi vo formáte časovej pečiatky, pre ktorý sa časová pečiatka požaduje.

Poskytnutím časovej pečiatky SNCA ako poskytovateľ časových pečiatok osvedčuje, že údaje ku ktorým bola časová pečiatka vyhotovená existovali v čase uvedenom v časovej pečiatke.

3.1 Všeobecné ustanovenia politiky

Právne záruky a obmedzenia záruk v rámci tohto dokumentu vyplývajú zo zákonných predpisov platných v SR.

Spory budú riešené v zmysle platných zákonov a ostatných všeobecne záväzných predpisov SR.

V rámci tohto dokumentu nie je stanovená žiadna finančná zodpovednosť. V prípade jej vzniku bude finančná zodpovednosť jednotlivých strán určená právnymi predpismi platnými v Slovenskej republike.

3.2 Služby súvisiace s časovou pečiatkou

Služby súvisiace s časovou pečiatkou je možné z pohľadu naplnenia požiadaviek rozdeliť na dve samostatné služby, ktorými sú:

- poskytovanie časovej pečiatky – táto služba vytvára samotnú časovú pečiatku,
- manažment časovej pečiatky – táto služba monitoruje a riadi procesy vyhotovovania časovej pečiatky, aby sa zaistilo, že služba je poskytovaná v súlade s touto CP TSA. Súčasťou tohto manažmentu je proces aktivácie resp. de-aktivácie služby vyhotovovania časovej pečiatky. Manažment časovej pečiatky napríklad okrem iného zabezpečuje, aby čas použitý pri vyhotovovaní časových pečiatok bol správne synchronizovaný s UTC.

3.3 Vydavateľ časových pečiatok

Poskytovateľ dôveryhodnej služby vyhotovovania časovej pečiatky pre potreby klientov v zmysle tejto CP TSA je NBÚ SR prostredníctvom SNCA.

SNCA musí niesť celkovú zodpovednosť za poskytovanie služieb súvisiacich s časovou pečiatkou ako sú definované v odstavci 3.2.

Zodpovednosť SNCA za vyhotovovanie časových pečiatok je identifikovateľná (pozri bod 6.7.1)

SNCA môže prevádzkovať niekoľko identifikovateľných nezávislých jednotiek na vyhotovovanie časovej pečiatky (TSU).

3.4 Používateľ časovej pečiatky

Používateľom služby vyhotovovania elektronickej časovej pečiatky sú orgány verejnej moci.

4. Úvod do politiky časovej pečiatky a plnenie všeobecných požiadaviek

4.1 Všeobecne

Tento dokument „Politika časových pečiatok SNCA (zásady pre vydávanie a overovanie časových pečiatok)“ je verejným dokumentom.

Činnosť SNCA pri vydávaní časových pečiatok sa riadi prevádzkovými a bezpečnostnými smernicami SNCA.

4.2 Cieľoví používatelia a použitie

4.2.1 Správna prax uplatňovania politiky vyhotovovania časových pečiatok

Táto politika môže byť použitá pre verejnú službu poskytovanie časových pečiatok ako aj na použitie v uzavretých komunitách.

5. Politiky a pravidlá

5.1 Ohodnotenie rizík

Pravidlá a zásady pre hodnotenie rizík sú definované v Politike poskytovania dôveryhodných služieb, kap. 5. Posúdenie rizík

5.2 Pravidlá pre praktický výkon dôveryhodných služieb

Všeobecné pravidlá pre praktický výkon dôveryhodných služieb sú uvedené v dokumente NBÚ - Politika poskytovania dôveryhodných služieb.

5.3 Všeobecné podmienky

Všeobecné podmienky sú uvedené v dokumente NBÚ - Politika poskytovania dôveryhodných služieb, odstavec 6.2.

5.4 Politika informačnej bezpečnosti

Politika informačnej bezpečnosti je uvedená v dokumente NBÚ - Politika poskytovania dôveryhodných služieb, odstavec 6.3, pričom dôveryhodnosť systému je zaistená:

- zavedenými bezpečnostnými pravidlami a procedúrami,
- spôsobom riadenia bezpečnosti TSA SNCA,
- dohľadom nad bezpečnosťou vykonávanie obslužných činností a prevádzkových rutín,
- pravidelným vnútorným a externým auditom bezpečnosti,
- súladom so štandardami definujúcimi požiadavky na bezpečnosť dôveryhodných systémov.

5.5 Záväzky SNCA

5.5.1 Všeobecne

SNCA ako poskytovateľ služieb časových pečiatok sa zaväzuje:

1. zabezpečiť plnenie požiadaviek v zmysle kapitoly 6 a 7;
2. používať bezpečnostné systémy ktoré zaisťujú primeranú technickú úroveň ochrany, vrátane použitia kryptografických opatrení;
3. vykonávať prijaté postupy bezpečným a spoľahlivým spôsobom,
4. zabezpečiť súlad hodín servera časových pečiatok s časom UTC v proklamovanej presnosti,
5. zabezpečiť sledovateľnosť spracovania žiadostí o vydanie časových pečiatok,
6. zabezpečiť ochranu kľúčov používaných na vydávanie časových pečiatok,
7. zabezpečiť zverejňovanie údajov nutných na overovanie vydaných časových pečiatok v podobe certifikátov verejného kľúča prislúchajúceho súkromnému kľúču používanému pri podpisovaní časových pečiatok,

8. zverejňovať informácie o:
    - spôsobe poskytovania služieb časovej pečiatky,
    - spôsobe prijímania žiadostí o časové pečiatky,
    - spôsobe overovania časových pečiatok.
9. zabezpečiť, aby prax vyhotovovania časovej pečiatky zodpovedala procedúram popísaným v tejto CP TSA a v súlade s CPS TSA.

5.5.2 Záväzky SNCA k orgánom verejnej moci

SNCA ako poskytovateľ služieb časových pečiatok je povinný:

1. zaistiť spracovanie žiadostí o vydanie časovej pečiatky doručených v predpísanom formáte,
2. odpovedať na platnú žiadosť o vydanie časovej pečiatku vydaním časovej pečiatky (pokiaľ tomu nebránia technické problémy),
3. zverejňovať údaje nutné na overovanie vydaných časových pečiatok v podobe certifikátov verejného kľúča prislúchajúceho súkromnému kľúču používanému pri podpisovaní časových pečiatok.

5.6 Informácie pre spoliehajúce sa strany

SNCA ako poskytovateľ služieb časových pečiatok je vo vzťahu k Spoliehajúcim sa stranám povinný zaistiť podmienky na overenie časových pečiatok zverejňovaním údajov nutných na overovanie vydaných časových pečiatok v podobe certifikátov verejného kľúča prislúchajúceho súkromnému kľúču používanému pri podpisovaní časových pečiatok.

SNCA musí sprístupniť pre Spoliehajúce sa strany (kapitola 5.3) nasledovné:

1. povinnosť overenia, že časová pečiatka bola správne podpísaná a že súkromný kľúč použitý na podpis časovej pečiatky nebol do času overovania kompromitovaný,
2. počas platnosti certifikátu vydávajúcej TSU musí byť platnosť jeho podpisového kľúča overená na základe aktuálneho stavu jeho platnosti na základe údajov publikovaných SNCA,
3. všetky obmedzenia pre použitie časovej pečiatky podľa tejto politiky,
4. všetky ďalšie obmedzenia uvedené v dohodách alebo kdekoľvek inde.

6. Riadenie a prevádzka TSA SNCA

6.1 Úvod

Riadenie a prevádzka TSA SNCA musia byť vykonávané tak, aby prijaté bezpečnostné opatrenia a nástroje na kontrolu ich plnenia poskytli nevyhnutnú dôveru, že budú naplnené.

Poskytovanie časovej pečiatky ako odpoveď na požiadavku je na rozhodnutí SNCA a závisí na dohode o úrovni poskytovaných služieb s príslušným orgánom verejnej moci.

6.2 Vnútorná organizácia

SNCA:

- je ústredným orgánom štátnej správy pre dôveryhodné služby,
- sa pri plnení úloh riadi Ústavou Slovenskej republiky, ústavnými zákonmi, právne záväznými aktmi Európskej únie, medzinárodnými zmluvami, ktorými je Slovenská republika viazaná, zákonmi, ďalšími všeobecne záväznými právnymi predpismi, uzneseniami vlády Slovenskej republiky, svojim štatútom a organizačným poriadkom ako aj ostatnými internými predpismi úradu,
- riadi informačnú bezpečnosť primerane pre poskytované služby vyhotovovania časových pečiatok,
- zamestnáva dostatočný počet osôb, ktoré majú nevyhnutné vzdelanie, školenia, technické znalosti a skúsenosti vzhľadom na typ, rozsah a množstvo práce nevyhnutnej na poskytovanie služieb vyhotovovania časovej pečiatky.

Časová pečiatka SNCA je organizačnou súčasťou Sekcie ekonomiky a prevádzky Národného bezpečnostného úradu Slovenskej Republiky.

Organizačná štruktúra NBÚ SR je popísaná v organizačnej schéme zverejnenej na webovom sídle www.nbu.gov.sk.

6.3 Personálna bezpečnosť

Manažment kľúčov môže vykonávať len k tomu poverený pracovník v rámci svojej role. Tieto role pracovníkov sú jednoznačne definované dokumentáciou SNCA. Každý pracovník je preukázateľne poučený o svojich povinnostiach, bezpečnostných a pracovných postupoch požadovaných pri plnení úloh vyplývajúcich z jeho role.

Osoby zabezpečujúce činnosti v prevádzke SNCA sú preverované v zmysle Vyhlášky NBÚ č. 331/2004 Z.z. o personálnej bezpečnosti.

Externé organizácie, ktoré vystupujú ako zmluvní dodávatelia činností pre SNCA, sú preverované v zmysle Vyhlášky NBÚ č. 325/2004 Z.z. o priemyselnej bezpečnosti.

6.4 Správa aktív

Požiadavky pre oblasť správy aktív sú uvedené v dokumente NBÚ - Politika poskytovania dôveryhodných služieb, odstavec 7.3.

6.5 Riadenie prístupu

Požiadavky pre oblasť riadenia prístupu sú uvedené v dokumente NBÚ - Politika poskytovania dôveryhodných služieb, odstavec 7.4.

Navyše:

- na vykonanie kritických činností na kryptografickom module (napr. generovanie, záloha súkromného kľúča SNCA, obnova kľúčov, obnova zariadení) je nutný prístup dvoch určených pracovníkov prevádzkovateľa SNCA (princíp štyroch očí),
- kľúče servera časových pečiatok určené na podpisovanie a overovanie časových pečiatok sú generované v kryptografickom module TSA. Procedúra generovania kľúčov sa vykonáva len pod dozorom komisie na to poverenej.

6.6 Kryptografické opatrenia

6.6.1 Všeobecne

Na správu všetkých kryptografických kľúčov a zariadení sú počas ich životného cyklu použité primerané bezpečnostné prvky a opatrenia.

6.6.2 Generovanie kľúčov pre TSU

Generovanie kľúčov pre jednotlivé TSU spĺňa nasledovné:

a) je vykonané vo fyzicky bezpečnom prostredí (pozri odstavec 6.8) osobami zaradenými v dôveryhodných rolách (pozri odstavec 6.3) za účasti minimálne dvoch oprávnených osôb. Okruh osôb autorizovaných vykonávať túto funkciu je obmedzený len na osoby v rolách vymenované v dokumente CPS TSA.

b) Generovanie TSU podpisového kľúča je vykonávané v bezpečnom kryptografickom zariadení, ktoré je dôveryhodný systém, ktorý spĺňa úroveň EAL 4+ resp. FIPS-140-3.

c) Algoritmus vytvárania TSU kľúča, výsledná dĺžka kľúča a podpisový algoritmus použitý na podpisovanie časových pečiatok je v súlade s požiadavkami normy ETSI TS 119 312.

d) Podpisový kľúč TSU nie je možné importovať do iného kryptografického modulu bez rozhodnutia bezpečnostného správcu a za účasti stanoveného počtu oprávnených osôb.

e) V kryptografických moduloch jednotlivých TSU sú rôzne podpisové kryptografické kľúče.

f) TSU má v danom čase k dispozícii len jeden aktívny kľúč na podpisovanie časovej pečiatky.

6.6.3 Ochrana súkromného kľúča TSU

Súkromné kľúče TSU zostávajú dôverné a ich integrita je udržiavaná minimálne s nasledovnými požiadavkami:

g) Súkromný podpisový kľúč TSU je uložený a používaný v kryptografickom module, ktorý je dôveryhodný systém zabezpečený na úrovni EAL 4+ v zmysle normy ISO/IEC 15408. resp. spĺňa požiadavky FIPS 140-3.

h) Súkromné kľúče TSU sú zálohované, kopírované, ukladané a obnovované len personálom v dôveryhodných rolách, za dodržania podmienky stanoveného počtu oprávnených osôb a vo fyzicky bezpečnom prostredí. Autorizované osoby na vykonávanie týchto činností sú len tie, ktoré podliehajú pravidlám, ktoré sú uvedené v dokumente CPS TSA.

i) Akékoľvek záložné kópie súkromných podpisových kľúčov nachádzajúce sa mimo TSU sú chránené, tak že je zabezpečená ich integrita a dôvernosť.

6.6.4 Certifikát verejného kľúča TSU

SNCA zaručuje integritu a autenticitu verejného kľúča TSU pre overenie podpisu nasledovne:

a) Verejný kľúč TSU, ktorý slúži na overenie podpisu je dostupný spoliehajúcim sa stranám v certifikáte verejného kľúča.

b) Certifikát verejného kľúča TSU pre overenie podpisu je vydaný certifikačnou autoritou poskytujúcou služby v zmysle normy ETSI EN 319 411-1.

c) TSU nevyhotoví časovú pečiatku pred tým ako jej certifikát verejného kľúča pre overenie podpisu je načítaný v kryptografickom zariadení TSU.

Keď SNCA prevezme certifikát verejného kľúča, ktorý slúži na overenie podpisu pre jednotlivé TSU, overí, že tento certifikát bol správne podpísaný, vrátane overenia celej certifikačnej cesty k dôveryhodnej certifikačnej autorite.

6.6.5 Prepísanie kľúča TSU

Životnosť certifikátu TSU nie je dlhšia ako doba, počas ktorej sú zvolený algoritmus a dĺžka kľúča uznané ako vhodné pre tento účel.

6.6.6 Manažment životného cyklu podpisového kryptografického hardvéru

Aplikované sú nasledovné požiadavky:

j) Do kryptografického hardvéru, určeného na podpisovanie časových pečiatok, nesmie byť svojvoľne zasahované počas jeho prepravy.

k) Do kryptografického hardvéru, ktorý podpisuje časové pečiatky, nesmie byť svojvoľne zasahované počas jeho skladovania.

l) Inštalácia, aktivácia a duplikácia podpisových kľúčov TSU v kryptografickom hardware je vykonávaná iba osobami v dôveryhodných roliach, s minimálne dvojitou kontrolou a vo fyzicky bezpečnom prostredí (pozri odstavec 6.8).

m) Súkromné podpisové kľúče TSU uložené v kryptografickom module TSU sú v prípade vyradenia modulu vymazané takým spôsobom, že je prakticky nemožné ich obnovenie.

6.6.7 Ukončenie životného cyklu kľúča TSU

Životný cyklus kľúčov TSA je ukončený:

- vypršaním platnosti certifikátu,
- zrušením platnosti certifikátu v prípade mimoriadnej udalosti.

Zrušenie certifikátu je avizované vydaním CRL a jeho zverejnením publikačnými prostriedkami SNCA.

Neplatné kľúče TSA (kľúče, ktorých životný cyklus bol ukončený) sú nahradené vygenerovaním nového kľúčového páru, certifikáciou verejného kľúča a zverejnením certifikátu na publikačných prostriedkoch.

Zrušené certifikáty zverejnené v CRL je možné používať aj po ich zrušení na overovanie časových pečiatok, ktoré boli vydané pred zrušením certifikátu (čas vydania časovej pečiatky je nižší, ako čas zrušenia certifikátu).

6.7 Vyhotovenie časovej pečiatky

Formát vydávaných časových pečiatok zodpovedá štandardom RFC 3161 a ETSI TS 101 861.

Na vyžiadanie časových pečiatok sa používa proprietárny protokol so zvýšenou ochranou, odvodený od protokolu RFC 3161.

Vyžiadanie časovej značky prebieha v nasledujúcich fázach:

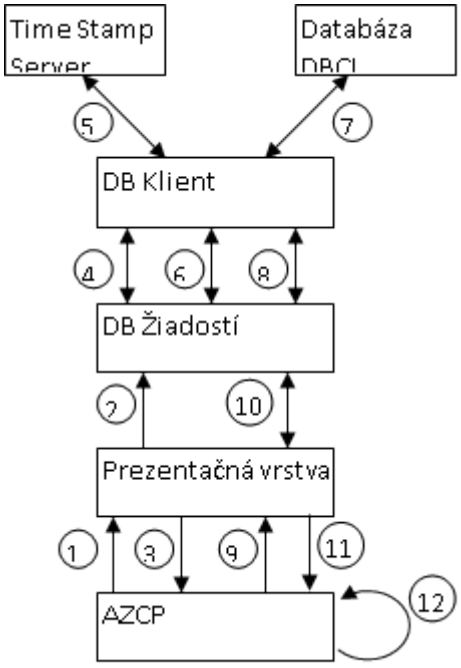
- vygenerovanie žiadosti o pridelenie časovej značky,
- odoslanie žiadosti o pridelenie časovej značky,
- prijatie odpovede na žiadosť o časovú značku (TSR).

Na hašovanie pri vydávaní časových pečiatok je použitý algoritmus SHA1. Na podpisovanie časových pečiatok (šifrovanie produktu hašovania) je použitý algoritmus RSA s dĺžkou kľúča 1024 bitov.

Časový údaj časovej pečiatky je udaný v čase UTC. Časový údaj časovej pečiatky má presnosť 1 sekunda, alebo menej.

6.7.1 Vydanie časovej pečiatky

6.7.1.1 Architektúra časovej pečiatky



Základný popis funkčnosti časovej pečiatky:

1. Pripojenie sa k službe časovej pečiatky, autentifikácia cez Mutual SSL, vytvorenie a poslanie žiadosti.
2. PV vygeneruje jedinečné číslo Req_ID, zapíše žiadosť do DBŽ PV pošle odpoveď klientovi.

3. DB Klient si prečíta žiadosť z DBŽ.
4. DB Klient načíta žiadosť, posunie ju na spracovanie dcérskemu procesu.
5. Dcérsky proces na DB Klientovi skontroluje syntax žiadosti, pošle ju na TimeStamp Server a prijme odpoveď.
6. Dcérsky proces DB Klienta zapíše odpoveď do DBŽ, s príznakom “nedokončené”.
7. DB Klient zapíše odpoveď do archivačnej DB.
8. DB Klient updatuje riadok v DBŽ na príznak=”dokončené”.
9. Klient (AZCP) požiada PV o zaslanie vydanej časovej pečiatky k požiadavke, ktorej ID=Req_ID.
10. PV vyhľadá v DBŽ príslušnú časovú pečiatku.
11. PV pošle časovú pečiatku klientovi.
12. Klient si skontroluje, či získaná pečiatka bola vydaná dôveryhodnou autoritou a či bola vydaná k žiadosti, ktorú poslal.

Pozn.1: Ak nebude odpoveď dostupná okamžite, môže klient (AZCP) opakovať kroky 9-12 aj neskoršie.

Pozn.2: Autentifikácia k službe časovej pečiatky bude realizovaná v 1. etape prostredníctvom HTTPS (SSL). Na autentifikáciu použijú autorizovaní žiadatelia o časovú pečiatku certifikáty, ktoré budú môcť byť použité na SSL autentifikáciu. Pri použití SSL autentifikácie je záznam o použití služby uložený v textovom súbore. V budúcnosti môže vzniknúť požiadavka na zabezpečenie prístupu k službe časovej pečiatky formou elektronického podpisu. Potom by žiadatelia o službu podpisovali žiadosť a vytvárali PKCS7 správu.

6.7.1.2 Podanie žiadosti o vydanie časovej pečiatky

Žiadosť o pridelenie časovej značky vygeneruje klient TS vo formáte TSQ. Žiadosť vo formáte TSQ klient zapuzdri do formátu PKCS #7 (na umožnenie autentizácie).

Klient TS odošle vygenerovanú žiadosť o pridelenie časovej značky (súbor PKCS #7) protokolom HTTP serveru TSA.

Ako potvrdenie prijatia žiadosti o pridelenie časovej značky server TSA odošle klientovi TS identifikátor, pod ktorým klient preberie vygenerovanú časovú značku.

Klient podáva žiadosti o vydanie časovej pečiatky podľa nasledovného postupu:

- žiadosti o vydanie časovej pečiatky sa podávajú na internetovej stránke

TSA1 - http://ep.nbusr.sk:8080/tsa1/TSQServer

TSA2 – http://100.112.90.40:8080/tsa1/TSQServer

- komunikácia je realizovaná protokolom http,
- žiadosti o vydanie časovej pečiatky musia byť vo formáte PKCS #7,
- žiadosť o vyhotgovenie časovej pečiatky musí obsahovať verziu formátu žiadosti, kryptografickú charakteristiku údajov, ku ktorým sa požaduje vydanie časovej pečiatky, vygenerovanú ako produkt hašovej funkcie aplikovanej nad požadovanými údajmi doplnenú o náhodný identifikátor (náhodné celé číslo), ktorý slúži na previazanie žiadosti s odpoveďou,

- na zabezpečenie autentizácie sú žiadosti o časovú pečiatku obalené do správy s formátom PKCS#7,
- za správnosť žiadosti o časovú pečiatku zodpovedá žiadateľ.

6.7.1.3 Generovanie časových pečiatok

Odpoveď na žiadosť o časovú pečiatku TSR je generovaná na základe údajov zo žiadosti. TSR obsahuje status odpovedi a vlastnú časovú pečiatku (TST). Telo časovej pečiatky TST obsahuje informácie zaslané žiadateľom v žiadosti, doplnené o jedinečné sériové číslo, informáciu o dátume a čase vydania časovej pečiatky (UTC čas) a o informačné údaje o časovej pečiatke. Údaje tela TST sú podpísané hašovaním algoritmom SHA1 a zakryptovaním produktu hašovania súkromným kľúčom TSA. Pri prípadnom rozsynchronizovaní hodín TSA je žiadosť odmietnutá. Vygenerované časové pečiatky sú odovzdané žiadateľom na internetovej stránke, na ktorej bola podaná žiadosť o časovú pečiatku.

6.7.1.4 Prijatie odpovede na žiadosť o časovú pečiatku

Proces prevzatia časovej pečiatka je asynchrónny. Klient TS prevezme vygenerovanú časovú pečiatku pri novom HTTP volaní pri ktorom sa identifikuje identifikátorom.

Prevzatá časová pečiatka má štandardný formát podľa RFC 3161.

6.7.1.5 Overovanie časových pečiatok

Overovanie časových pečiatok sa musí vykonať v nasledovných krokoch:

- overenie platnosti certifikátu verejného kľúča TSA proti CRL,
- overenie platnosti certifikátu verejného kľúča TSA preverením podpisu certifikátu,
- overenie platnosti časovej pečiatky na základe overenia elektronického podpisu časovej pečiatky.

Pokiaľ ktorékoľvek z vymenovaných overení nebolo overené s pozitívnym výsledkom, je časová pečiatka pokladaná za neplatnú.

6.7.2 Synchronizácia hodín s UTC

Hodiny TSA používané ako zdroj času pre časové pečiatky sú synchronizované od zdroja presného času služby Sovereign Time.

Synchronizácia času zaručuje presnosť lepšiu ako 1 sekunda.

6.8 Fyzická a objektová bezpečnosť

Pravidlá a zásady pre zaistenie fyzickej a objektovej bezpečnosti sú definované v Politike poskytovania dôveryhodných služieb, kap. 7.6 Fyzická a objektová bezpečnosť.

Navyše platí:

n) Na kryptografický modul musí byť aplikované riadenie prístupu v súlade s odstavcom 6.5.

o) Na správu vyhotovovania časových pečiatok musia byť aplikované nasledovné dodatočné opatrenia:

- Technické prostriedky na vyhotovovanie časových pečiatok musia byť prevádzkované v prostredí, ktoré fyzicky a logicky chráni služby pred kompromitáciou, ktorá môže byť spôsobená neautorizovaným prístupom k systémom alebo údajom.
- Každý vstup do fyzicky bezpečnej oblasti musí podliehať nezávislému dohľadu a neautorizovaná osoba musí byť sprevádzaná autorizovanou osobou pokiaľ je v bezpečnej oblasti. Každý vstup a prítomnosť musí byť zaznamenaná.
- Fyzická ochrana musí byť dosiahnutá vytvorením jasne definovanej bezpečnostnej hranice (perimetrom, fyzickou bariérou) okolo správy vyhotovovania časovej pečiatky. Akékoľvek časti objektu zdieľané s inými organizáciami musia byť mimo tohto perimetra.
- Fyzické a objektové bezpečnostné opatrenia musia chrániť objekty, kde sú umiestnené systémy, samotné systémové zdroje a objekty použité na podporu ich prevádzky. Bezpečnostné opatrenia týkajúce sa fyzickej a objektovej bezpečnosti SNCA musia pokrývať minimálne fyzické riadenie prístupu, ochranu pred prírodnými katastrofami, ochranu pred požiarom, výpadok podporných rozvodov (napr. elektrina, telekomunikácie), zrútenie štruktúry, úniky z potrubí, ochranu proti odcudzeniu, vlámaniu, a obnovu po pohrome.
- Prijaté opatrenia musia chrániť zariadenia, informácie, médiá a softvér týkajúcich sa služieb vyhotovovania časových pečiatok pred vynesením bez autorizácie.

6.9 Prevádzková bezpečnosť

Bezpečnosť prevádzky TSA SNCA je riadená v rámci manažmentu bezpečnosti SNCA.

Na zabezpečovanie akreditovaných certifikačných služieb používa SNCA produkty na elektronický podpis s medzinárodne uznávanou certifikáciou ISO/IEC 15408 a FIPS 140-1. Na dosiahnutie certifikácie ISO/IEC 15408 a FIPS 140-1 museli produkty pre elektronický podpis splniť príslušné požiadavky na zabezpečenie vývoja, ktoré tieto štandardy stanovujú.

Pri vývoji špecializovaného programového vybavenia sa uplatňujú ustanovenia interných bezpečnostných smerníc, ktoré predpisujú zásady bezpečnosti vývoja programového vybavenia a riadenie bezpečnosti pri poskytovaní certifikačných služieb.

Kľúče servera časových pečiatok určené na podpisovanie určené na podpisovanie a overovanie časových pečiatok sú generované v kryptografickom module TSA. Generovanie kľúčov sa vykonáva v bezpečnom prostredí.

Procedúra generovania kľúčov sa vykonáva pod dozorom komisie na to poverenej. Po ukončení platnosti certifikátu pre TSS bude záloha súkromného kľúča zničená.

Súkromné kľúče servera časových pečiatok určené na podpisovanie časových pečiatok sú uchovávané v kryptografickom module servera časových pečiatok a za žiadnych okolností neopúšťajú kryptografický modul.

Kryptografický modul servera časových pečiatok zodpovedá požiadavkám štandardu FIPS 140-1 level 4.

6.10 Sieťová bezpečnosť

Systém a pravidlá na zaistenie sieťovej bezpečnosti sú popísané v Politike poskytovania dôveryhodných služieb, kap. 7.8 Sieťová bezpečnosť.

Ďalej platí, že:

p) SNCA musí udržiavať a chrániť všetky TSU v bezpečnej zóne,

q) všetky systémy TSU musia byť nakonfigurované tak, že budú mať odstránené a/alebo zakázané všetky účty, aplikácie, služby, protokoly a porty, ktoré nie sú používané pre ich prevádzku,

r) do bezpečných zón a vysoko bezpečných zón môžu mať prístup len dôveryhodné roly.

6.11 Riadenie bezpečnostných incidentov

Systém riadenia bezpečnostných incidentov je popísaný v Politike poskytovania dôveryhodných služieb, kap. 7.9 Riadenie bezpečnostných incidentov.

6.12 Zber dôkazov

Všeobecné požiadavky na zber dôkazov sú popísané v Politike poskytovania dôveryhodných služieb, kap. 7.10 Zber dôkazov.

V súvislosti s poskytovaním služby časovej pečiatky je zber dôkazov zabezpečovaný zaznamenávaním a bezpečným uchovávaním informácií súvisiacich s poskytovaním služby časovej pečiatky.

Procesy pri poskytovaní časových pečiatok zaznamenávajú auditové stopy, z ktorých je možné spätne analyzovať priebeh vydania časovej pečiatky.

Auditné záznamy sa uchovávajú po dobu 10 rokov.

Na zaznamenávanie informácií súvisiacich s poskytovaním služby časovej pečiatky slúži databáza DB Klienta, ktorá bude slúžiť na ukladanie:

- zoznamu vydaných časových pečiatok,
- zoznamu vydaných odpovedí,
- informácií o mimoriadnych udalostiach v systéme používanom v manažmente časových pečiatok,
- informácií o dôležitých udalostiach v prostredí vydavateľa časových pečiatok, manažmente kryptografických kľúčov a v synchronizácii zdrojov času vrátane presných časových údajov:
  - riadenie životného cyklu kľúčov TSU;
  - riadenie životného cyklu certifikátov TSU;
  - synchronizácia hodín TSU s UTC. Toto musí zahŕňať aj informácie týkajúce sa normálnej re-kalibrácie alebo synchronizácie hodín použitých pri vyhotovovaní časových pečiatok;
  - zistené straty synchronizácie.

Takýmito záznamami sú:

- všetky časové pečiatky (bez ohľadu na to, ktoré boli vyzdvihnuté a ktoré nie),
- záznamy o štarte a zastavení DB Klienta (aj neúspešnom, napr. ak sa nepodarí pripojiť k DBŽ),
- záznamy o odmietnutí vydať časovú pečiatku (napr. z dôvodu vypršania TAC, nedostupnosti TimeStamp servera, atď.),
- záznamy o prekročení maximálneho počtu vlákien (threadov), ku ktorému môže dôjsť pri nadmernom zaťažení služby časovej pečiatky.

6.13 Riadenie kontinuity činnosti organizácie

Pre prípad vzniku pohromy má SNCA definovaný a udržiavaný plán kontinuity. V prípade pohromy (vrátanie kompromitácie súkromného kľúča alebo iných citlivých údajov SNCA musí byť prevádzka SNCA obnovená v rámci oneskorenia definovaného v pláne kontinuity.

6.14 Ukončenie činnosti SNCA a plány ukončenia činnosti

Postup ukončenia činnosti SNCA je popísaný v Politike poskytovania dôveryhodných služieb, kap. 7.9 Riadenie bezpečnostných incidentov.

Ukončenie činnosti TSA bude oznámené:

- žiadateľom služieb časovej pečiatky,
- verejne ohlásené verejnými oznamovacími prostriedkami.

Okrem toho, v prípade ukončenia služieb TSA, musia byť zrušené všetky certifikáty vydané pre jednotlivé TSU.

6.15 Zhoda

Poskytovanie služby vyhotovovania kvalifikovaných elektronických časových pečiatok sa riadia:

- Nariadením 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,
- Zákonom č. 272/2016 Z.z. o dôveryhodných službách,
- ostatnými všeobecne platnými nariadeniami platnými v SR, vzťahujúcimi sa k výkonu tejto činnosti.

7. Plnenie požiadaviek pre kvalifikované elektronické časové pečiatky podľa Nariadenia eIDAS

7.1 Certifikát verejného kľúča TSU

Pre kvalifikované elektronické časové pečiatky (v zmysle eIDAS) musí byť certifikát verejného kľúča TSU, ktorý slúži na overenie podpisu kvalifikovanej elektronickej časovej pečiatky, vydaný certifikačnou autoritou prevádzkovanou v zmysle politiky, ktorá vychádza z normy ETSI EN 319 411-2.

7.2 Vyhotovovanie nekvalifikovaných a kvalifikovaných elektronických časových pečiatok podľa Nariadenia eIDAS

Ak TSU zahrnutá v systéme SNCA vyhotovuje časové pečiatky, ktoré sú vyhlasované ako kvalifikované elektronické pečiatky podľa eIDAS, táto TSU nesmie vyhotovovať nekvalifikované elektronické časové pečiatky.

V prípade vyhotovovania nekvalifikovaných elektronických časových pečiatok musí SNCA používať rôzne inú TSU s rozdielnym názvom subjektu certifikátu verejného kľúča. Služba takejto TSU musí byť prístupná cez iný samostatný prístupový bod.