Č. p.:

DKDS5 Certifikačná politika pre kvalifikovanú dôveryhodnú službu vyhotovovania kvalifikovaných elektronických časových pečiatok

Názov dokumentu:	DKDS5 Certifikačná politika pre kvalifikovanú dôveryhodnú službu vyhotovovania kvalifikovaných elektronických časových pečiatok		
Označenie dokumentu:	DKDS5 Certifikačná politika TSAP SNCA.pdf		
Verzia:	0.9	Status:	*Návrh*
Dátum vytvorenia:	18.11.2020	Platný do:	31.12.2021

História dokumentu

História revízií dokumentu

Verzia	Dátum	Popis zmeny	Autor / Autor zmien
0.9	18.11.2020	Úvodná verzia	Ing. Marián Štefánek

Schválenia

Verzia	Funkcia	V zastúpení	Schválil dňa	Podpis

Distribúcia

Verzia	Spoločnosť	Meno	Počet výtlačkov

Referencie na legislatívne a normatívne dokumenty

[1] ETSI EN 319 421 v.1.1.1 - Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps.
ETSI EN 319 421 v.1.1.1

[2] Nariadenie Európskeho parlamentu a Rady (EÚ) č. 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES.
Nariadenie eIDAS

[3] ETSI EN 319 401 v.2.2.1 - Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.
ETSI EN 319 401 v.2.2.1

[4] Politika poskytovania dôveryhodných služieb NASES, OID: 1.3.158.42156424.0.1.1.

[5] ETSI TS 119 312 v.1.3.1 - Electronic Signatures and Infrastructures (ESI); Cryptographic Suites.
ETSI TS 119 312 v.1.3.1

[6] ISO/IEC 15408-1:2009 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model.

[7] Pravidlá na praktický výkon dôveryhodnej služby časovej pečiatky.

[8] ETSI EN 319 411-1 v.1.2.2 - Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.
ETSI EN 319 411-1 v.1.2.2

[9] ETSI EN 319 422 v.1.1.1 - Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles.
ETSI EN 319 422 v.1.1.1

[10] ETSI EN 319 411-2 v.2.2.2 - Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates.
ETSI EN 319 411-2 v.2.2.2

[11] ITU-R TF.460-6 Standard-frequency and time-signal emissions
ITU-R TF.460-6

[12] RFC 3647 - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.
RFC 3647

[13] Certifikačná politika pre Kvalifikovanú dôveryhodnú službu vyhotovovania a overovania kvalifikovaných certifikátov pre elektronický podpis, ktorej kvalifikovaný štatút udelil NBÚ SR, OID: 1.3.158.42156424.0.1.2.

[14] Zákon č. 272/2016 Z. z. o dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zmene a doplnení niektorých zákonov (ďalej aj „zákon o dôveryhodných službách“).
Zákon č. 272/2016 Z. z. o dôveryhodných službách

[15] 05968/2019/ORD-001 - Schéma dohľadu kvalifikovaných dôveryhodných služieb definovaná orgánom dohľadu, Verzia 1.4, NBÚ SR (ďalej aj „schéma dohľadu“).
Schéma dohľadu KDS definovaná orgánom dohľadu

[16] IETF RFC 3161 - Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP).
RFC 3161

Zoznam tabuliek

Použité definície a skratky

Tabuľka 1 Použité definície

Definícia	Vysvetlenie definície
Univerzálny koordinovaný čas	Časová škála, založená na sekunde podľa definície v Recommendation ITU-R TF.460-6, „svetový čas“.
Elektronická časová pečiatka	Údaje v elektronickej forme, ktoré viažu iné údaje v elektronickej forme s konkrétnym časom, čím tvoria dôkaz o existencii týchto iných údajov v danom čase.
Kvalifikovaná elektronická časová pečiatka	Elektronická časová pečiatka, ktorá spĺňa požiadavky stanovené v článku 42 Nariadenia eIDAS.
Politika časovej pečiatky (Time-stamp policy)	Definovaný súbor pravidiel, ktorý svedčí o použiteľnosti časovej pečiatky pre konkrétnu skupinu a/alebo triedu aplikácií so spoločnými bezpečnostnými požiadavkami.
Autorita časovej pečiatky	TSP poskytujúci služby vyhotovovania časovej pečiatky použitím jednej alebo viacerých TSU.
Služba vyhotovovania časových pečiatok (Time-stamping service)	Dôveryhodná služba vyhotovovania časových pečiatok.
Jednotka vyhotovovania časových pečiatok	Sústava technických a programových prostriedkov, ktorá je spravovaná ako jednotka a má v danom čase aktívny jeden kľúč na podpisovanie časových pečiatok.
Poskytovateľ dôveryhodnej služby	Entita, ktorá poskytuje jednu alebo viac dôveryhodných služieb.
Pravidlá na vykonávanie TSA činností (TSA practice statement)	Prehlásenie o postupoch, ktoré TSA používa pri vyhotovovaní časových pečiatok, je to špecifický typ prehlásenia o postupoch dôveryhodnej služby ako je definovaný v norme ETSI EN 319 401 (Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers).
Systém TSA (TSA system)	Zostava IT produktov a komponentov, zorganizovaných na podporu poskytovania služieb vyhotovovania časovej pečiatky.

Tabuľka 2 Použité skratky

Skratka	Vysvetlenie skratky
BTSP	Osvedčené postupy politiky časových pečiatok (Best practices Time-Stamp Policy).
CA	Certifikačná autorita.
IT	Informačné technológie.
Nariadenie eIDAS	Nariadenie Európskeho parlamentu a Rady (EÚ) č. 910/2014 [2].
NASES	Národná agentúra pre sieťové a elektronické služby.
NBÚ	Národný bezpečnostný úrad.
PKI	Infraštruktúra verejného kľúča (Public Key Infrastructure).
PMA	Autorita pre riadenie politík (Policy Management Authority)
RA	Registračná autorita.
SNCA	Slovenská národná certifikačná autorita.
TSA	Autorita časovej pečiatky, vydavateľ časovej pečiatky (Time-Stamping Authority).
TSP	Poskytovateľ dôveryhodnej služby (Trust Service Provider).
TSU	Samostatná jednotka vyhotovovania časových pečiatok (Time-Stamping Unit).
UTC	Univerzálny koordinovaný čas (Coordinated Universal Time).

Pre potreby tohto dokumentu sú použité definície prevzaté z Nariadenia eIDAS [6] resp. normy ETSI EN 319 401[3].

Obsah

1 Úvod

Tento dokument definuje politiku poskytovania kvalifikovanej dôveryhodnej služby vyhotovovania kvalifikovaných elektronických časových pečiatok (ďalej aj „TSAP“) a bezpečnostné požiadavky, ktoré sa týkajú postupov riadenia a prevádzkovej praxe pri poskytovaní tejto služby.

Poskytovateľom tejto dôveryhodnej služby je Národná agentúra pre sieťové a elektronické služby so sídlom Kollárova 8, 917 02 Trnava, Detašované pracovisko: BC Omnipolis, Trnavská cesta 100/II, 821 01 Bratislava, IČO: 42 156 424 (ďalej aj „Poskytovateľ“ alebo „NASES“), prostredníctvom svojho systému autority časovej pečiatky (ďalej aj „TSA SNCA“).

Táto certifikačná politika (ďalej aj „CP“) je záväzným dokumentom, ktorého ustanovenia musia dodržiavať všetky zúčastnené strany.

Táto certifikačná politika môže byť použitá pre poskytovanie verejnej služby vyhotovovania elektronických časových pečiatok ako aj pre poskytovanie tejto služby v uzavretých komunitách.

Tento dokument môže byť použitý nezávislými orgánmi ako základ pre potvrdenie, že Poskytovateľ s prevádzkovaným systémom TSA SNCA je dôveryhodný na poskytovanie služby vyhotovovanie kvalifikovaných elektronických časových pečiatok.

Služba vyhotovovania elektronických časových pečiatok, identifikovaná v tomto dokumente, je využívaná v okruhu pôsobnosti SNCA, zriadenej a prevádzkovanej agentúrou NASES.

2 Prehľad

Táto certifikačná politika sa týka poskytovania dôveryhodnej služby:

- vyhotovovanie 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 aj „Nariadenie eIDAS“) [2] a bola vypracovaná podľa normy ETSI EN 319 421 - A best practices policy for time-stamp (ďalej aj „BTSP“) [1].

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

Názov	Sériové číslo certifikátu	Vydavateľ	DigitalID v SK dôveryhodnom
SNCA3	**07 8e**	**KCA NBU SR 3**	**82**

2.1 Názov dokumentu a jeho identifikácia

Politika poskytovania kvalifikovanej dôveryhodnej služby vyhotovovania kvalifikovaných elektronických časových pečiatok je identifikovaná nasledovným identifikátorom, odvodeným od objektového identifikátora NASES:

1.3.158.42156424.0.1.4

kde jednotlivé zložky OID majú nasledovný význam:

1	ISO
3	ISO Identified Organization
158	Slovakia
42156424	jedinečný identifikátor Národnej agentúry pre sieťové a elektronické služby priradený organizáciou ISO (IČO)
0	KCA (poskytovanie dôveryhodných služieb)
1	Certifikačné politiky
4	Certifikačná politika poskytovania kvalifikovanej dôveryhodnej služby vyhotovovania kvalifikovaných elektronických časových pečiatok

2.2 Účastníci PKI

V rámci poskytovania dôveryhodných služieb vyhotovovania kvalifikovaných elektronických časových pečiatok, sú účastníkmi infraštruktúry verejného kľúča entity, uvedené tejto časti.

2.2.1 Jednotka vyhotovovania časových pečiatok

Jednotka vyhotovovania časových pečiatok:

- je entita, ktorá poskytuje kvalifikované dôveryhodné služby vyhotovovania kvalifikovaných elektronických časových pečiatok pre používateľov (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 pravidlami na výkon certifikačných činností SNCA (ďalej aj „CPS SNCA“).

TSU Poskytovateľa je súčasťou hierarchickej PKI:

KCA NBÚ SR 3 -> SNCA 3 -> TSA

KCA NBÚ SR 3 -> SNCA 3 -> TSU

Poskytovateľ môže prevádzkovať, v rámci podriadenosti pod certifikačnou autoritou SNCA3, viaceré TSU, poskytujúce dôveryhodné služby vyhotovovania časovej pečiatky.

Služba vyhotovovania časovej pečiatky, akceptuje žiadosti o vydanie časovej pečiatky, bez uvedenia OID politiky časovej pečiatky v žiadosti *TimeStampReq*.

2.2.2 Registračná autorita

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

RA musí vykonávať svoje aktivity v súlade so schválenou Politikou a Pravidlami na výkon certifikačných činností CPS SNCA v aktuálnom znení.

Poskytovateľ má v súčasnej dobe zriadené RA, pôsobiace na týchto adresách:

- sídla registračných autorít SNCA / registračné miesta:
  - interná registračná autorita SNCA:

Národná agentúra pre sieťové a elektronické služby
BC Omnipolis,
Trnavská cesta 100/II,
821 01 Bratislava
Slovenská republika

- externá OVM registračná autorita SNCA:

Národný bezpečnostný úrad
Budatínska 30
851 06 Bratislava
Slovenská republika

2.2.3 Odberateľ

O vyhotovenie časovej pečiatky môžu žiadať:

- Fyzické osoby.
- Právnické osoby.
- Orgány verejnej moci.

Žiadatelia o službu vyhotovovania časových pečiatok 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 rámci týchto povinností,
- riešiť nezrovnalosti, pri vydaní časovej pečiatky, s kontaktnou osobou Poskytovateľa bez zbytočných prieťahov.

2.2.4 Spoliehajúca sa strana

Spoliehajúca sa strana, je ľubovoľná právnická alebo fyzická osoba, prípadne technologické zariadenie, so sídlom v SR alebo 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 tejto TSAP o overovaní časových pečiatok.

2.2.5 Iní účastníci

PMA je zložka Poskytovateľa, ustanovená za účelom:

- dohľadu nad vytváraním a aktualizáciou TSAP, vrátane vyhodnocovania zmien a plánov na implementovanie ľubovoľných prijatých zmien,
- revízie CPS, aby sa zaručilo, že prax Poskytovateľa vyhovuje príslušnej TSAP,
- revízie výsledkov auditov, aby sa určilo, či Poskytovateľ zodpovedne dodržiava ustanovenia vydaných CPS,
- vydávania odporúčaní pre Poskytovateľa, týkajúcich sa nápravných a iných vhodných opatrení,
- riadenia a usmerňovania činností Poskytovateľa a RA,
- výkladu ustanovení vydaných CPS a svojich pokynov pre Poskytovateľa a RA,
- výkonu funkcie interného audítora, pričom touto činnosťou poverí samostatného zamestnanca.

PMA predstavuje vrcholovú zložku, ktorá rozhoduje s konečnou platnosťou vo všetkých záležitostiach a aspektoch týkajúcich sa Poskytovateľa a jeho činnosti.

2.3 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. [2]

2.4 Správa politiky

Táto politika spĺňa požiadavky štandardu ETSI EN 319 421 a požiadavky, definované v dokumente „Schéma dohľadu kvalifikovaných dôveryhodných služieb definovaná orgánom dohľadu“ [15].

2.4.1 Organizácia zodpovedná za správu dokumentu

Tento dokument je spravovaný sekciou Slovenskej národnej certifikačnej autority Národnej agentúry pre sieťové a elektronické služby.

Kontaktná adresa:

Národná agentúra pre sieťové a elektronické služby

Detašované pracovisko:

BC Omnipolis,

Trnavská cesta 100/II,

821 01 Bratislava,

Slovenská republika,

http://www.nases.gov.sk

2.4.2 Kontaktná osoba

Bezpečnostný správca SNCA.

Národná agentúra pre sieťové a elektronické služby

Detašované pracovisko:

BC Omnipolis,

Trnavská cesta 100/II,

821 01 Bratislava,

Slovenská republika,

Telefón: +421 2 3278 0700

e-mail: info@nases.gov.sk

2.4.3 Osoba rozhodujúca o súlade CPS s TSA politikou

Osobou, ktorá je zodpovedná za súlad postupov Poskytovateľa s ustanoveniami, ktoré sú uvedené v tejto TSAP je osoba, menovaná do roly PMA.

Vo všetkých záležitostiach a aspektoch, týkajúcich sa Poskytovateľa a jeho činnosti, s konečnou platnosťou rozhoduje riaditeľ sekcie Slovenskej národnej certifikačnej autority NASES.

2.4.4 Postupy schvaľovania TSAP a externej politiky

Je nevyhnutné, aby pred uvedením do prevádzky, mal Poskytovateľ schválenú požadovanú dokumentáciu, svoje TSAP a CPS a zároveň, aby spĺňal všetky požiadavky, definované v týchto dokumentoch. Obsah TSAP a CPS schvaľuje riaditeľ sekcie Slovenskej národnej certifikačnej autority NASES.

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

3 Zverejňovanie informácií a úložiská

SNCA spravuje repozitáre (úložiská dokumentácie a informácií) podľa Nariadenia eIDAS a zákona č. 272/2016 Z. z..

Úložiská musia byť umiestnené tak, aby boli prístupné Odberateľom a Spoliehajúcim sa stranám a boli v súlade s celkovými bezpečnostnými požiadavkami.

Funkciu úložiska Poskytovateľa, bude zastávať webové sídlo SNCA, ktoré je zverejnené a dostupné na internetovej adrese:

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

Webové sídlo SNCA, je prostredníctvom internetu verejne prístupné všetkým Odberateľom, Spoliehajúcim sa stranám a verejnosti vôbec.

Verejne dostupné informácie, uvedené na webovom sídle SNCA, majú charakter riadeného prístupu.

3.1 Zverejňovanie informácií o TSA

Zásady pre poskytovanie služby vyhotovovania časových pečiatok, sú zverejnené na internetovej stránke SNCA:

http://ep.nbu.gov.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. Prostriedkom na distribúciu certifikátov verejných kľúčov TSA, určených na overovanie časových pečiatok, je internetová stránka SNCA.

Konštitutívny charakter pre stav služby, má dôveryhodný zoznam:

http://www.nbu.gov.sk/doveryhodne-sluzby/doveryhodne-zoznamy/

podľa ktorého sa určuje aj jej platnosť.

Miestom zverejňovania certifikátov verejných kľúčov TSA, určených na overovanie časových pečiatok, je internetová stránka SNCA:

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

Aktuálny zoznam zrušených certifikátov, je publikovaný v súboroch, na internetovej stránke:

http://ep.nbu.gov.sk/snca/crls2/snca2.crl

http://ep.nbu.gov.sk/snca/crls3/snca3.crl

3.2 Frekvencia zverejňovania informácií

Zoznam zrušených certifikátov (CRL) musí byť publikovaný, ako je špecifikované v časti 4.9.7 aktuálnej CP pre vyhotovovanie kvalifikovaných certifikátov [13]0. Informácie o zrušenom certifikáte TSU musia byť dostupné na internetovej stránke SNCA (pozri kapitola 3.1), ktorý slúži ako jeho úložisko.

TSAP sa musí zverejniť čo najskôr po ich schválení a vydaní.

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

3.3 Kontroly prístupu

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

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

4 Všeobecné ustanovenia

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

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

4.1 Všeobecné ustanovenia politiky

Táto certifikačná politika nadväzuje na dokument „Politika poskytovania dôveryhodných služieb NASES“ [4], kde sú popísané všeobecné požiadavky a pravidlá poskytovania dôveryhodných služieb, ktoré musí NASES ako poskytovateľ dôveryhodných služieb rešpektovať.

Právne záruky a obmedzenia záruk v rámci tejto politiky, 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.

4.2 Služby súvisiace s časovou pečiatkou

Služby, súvisiace s vyhotovovaním časových pečiatok, 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 politikou. Súčasťou tohto manažmentu je proces aktivácie, resp. de-aktivácie služby vyhotovovania časovej pečiatky. Manažment časovej pečiatky, okrem iného zabezpečuje, aby čas, použitý pri vyhotovovaní časových pečiatok, bol správne synchronizovaný s UTC.

4.3 Vydavateľ časových pečiatok

Poskytovateľ dôveryhodnej služby vyhotovovania časovej pečiatky, pre potreby Odberateľov v zmysle tejto politiky, je NASES prostredníctvom SNCA.

Za poskytovanie služieb, súvisiacich s časovou pečiatkou podľa bodu 4.2, zodpovedá Poskytovateľ.

Zodpovednosť Poskytovateľa za vyhotovovanie časových pečiatok je identifikovateľná (pozri bod 7.7.1)

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

4.4 Používateľ časovej pečiatky

Používateľom služby vyhotovovania elektronickej časovej pečiatky sú fyzické osoby, právnické osoby, orgány verejnej moci.

5 Úvod do politiky časovej pečiatky a plnenie všeobecných požiadaviek

5.1 Všeobecne

Táto TSAP je verejným dokumentom.

Pri vydávaní časových pečiatok, sa činnosť TSA SNCA, riadi prevádzkovými a bezpečnostnými smernicami Poskytovateľa a SNCA.

5.2 Cieľoví používatelia a použitie

5.2.1 Správne prax uplatňovania politiky vyhotovovania časových pečiatok

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

6 Politiky a pravidlá

6.1 Ohodnotenie rizík

Pravidlá a zásady pre hodnotenie rizík, sú definované v „Politike poskytovania dôveryhodných služieb NASES“ [4], kap. 5.

6.2 Pravidlá pre praktický výkon dôveryhodných služieb

Všeobecné pravidlá pre praktický výkon dôveryhodných služieb, sú uvedené v „Politike poskytovania dôveryhodných služieb NASES“ [4].

6.3 Všeobecné podmienky

Platia všeobecné podmienky, popísané v „Politike poskytovania dôveryhodných služieb NASES“ [4], odstavec 4.2.

6.4 Politika informačnej bezpečnosti

Politika informačnej bezpečnosti je uvedená a popísaná v dokumente „Politika poskytovania dôveryhodných služieb NASES“, bod 4.3, pričom dôveryhodnosť systému je zabezpečená:

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

6.5 Záväzky Poskytovateľa

6.5.1 Všeobecne

NASES, ako prevádzkovateľ SNCA a poskytovateľ služieb vyhotovovania časových pečiatok sa zaväzuje:

- zabezpečiť plnenie požiadaviek v zmysle kapitoly 6 a 7 tejto TSAP;
- používať bezpečnostné systémy, ktoré zaisťujú primeranú technickú úroveň ochrany, vrátane použitia kryptografických opatrení;
- vykonávať prijaté postupy bezpečným a spoľahlivým spôsobom,
- zabezpečiť súlad hodín servera časových pečiatok s časom UTC v proklamovanej presnosti,
- zabezpečiť sledovateľnosť spracovania žiadostí o vydanie časových pečiatok,
- zabezpečiť ochranu kľúčov, používaných na vydávanie časových pečiatok,
- zabezpečiť zverejňovanie údajov, nutných na overovanie vydaných časových pečiatok v podobe certifikátov verejného kľúča, prislúchajúceho súkromnému kľúču, používanému pri podpisovaní časových pečiatok,
- zverejňovať informácie o:
  - spôsobe poskytovania služieb časovej pečiatky,
  - spôsobe prijímania žiadostí o časové pečiatky,
  - spôsobe overovania časových pečiatok.
- zabezpečiť, aby prax vyhotovovania časovej pečiatky zodpovedala procedúram, popísaným v tejto TSAP a bola v súlade s CPS SNCA.

6.5.2 Záväzky Poskytovateľa k orgánom verejnej moci

NASES, ako prevádzkovateľ SNCA a poskytovateľ služieb vyhotovovania časových pečiatok, je povinný:

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

6.6 Informácie pre spoliehajúce sa strany

NASES, ako prevádzkovateľ SNCA a poskytovateľ služby vyhotovovania 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 k súkromnému kľúču, používanému pri podpisovaní časových pečiatok.

Poskytovateľ musí sprístupniť pre Spoliehajúce sa strany (bod 6.3) nasledovné:

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

7 Manažment a prevádzka TSA Poskytovateľa

7.1 Úvod

Manažment a prevádzka TSA Poskytovateľa sú 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 Poskytovateľa a závisí na dohode o úrovni poskytovaných služieb s Odberateľom.

7.2 Vnútorná organizácia

NASES, ako prevádzkovateľ SNCA a poskytovateľ dôveryhodných služieb:

- 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 agentúry,
- 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.

TSA SNCA je organizačnou súčasťou Odboru Slovenskej národnej certifikačnej autority Národnej agentúry pre sieťové a elektronické služby.

Organizačná štruktúra agentúry NASES je popísaná v organizačnej schéme, zverejnenej na webovom sídle www.nases.gov.sk.

7.3 Personálna bezpečnosť

Manažment kľúčov, môže vykonávať len k tomu poverený pracovník, v rámci svojej role. Tieto role pracovníkov sú jednoznačne definované dokumentáciou ku kvalifikovaným dôveryhodným službám SNCA. Každý pracovník, je preukázateľne poučený o svojich povinnostiach, bezpečnostných a pracovných postupoch, požadovaných pri plnení úloh a 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 Poskytovateľa, sú preverované v zmysle Vyhlášky NBÚ č. 325/2004 Z. z. o priemyselnej bezpečnosti.

7.4 Správa aktív

Požiadavky pre oblasť správy aktív, sú uvedené a popísané v dokumente „Politika poskytovania dôveryhodných služieb NASES“, bod 5.3.

7.5 Riadenie prístupu

Požiadavky pre oblasť riadenia prístupu, sú uvedené a popísané v dokumente „Politika poskytovania dôveryhodných služieb NASES“, bod 5.4.

NASES, ako prevádzkovateľ SNCA a poskytovateľ služby TSA, garantuje bezpečnú prevádzku systému TSA SNCA a dostupnosť uvedenej služby naviac nasledovnými činnosťami:

- 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.

7.6 Kryptografické opatrenia

7.6.1 Všeobecne

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

7.6.2 Generovanie kľúčov pre TSU

Generovanie kľúčov pre jednotlivé TSU spĺňa nasledovné atribúty:

- je vykonané vo fyzicky bezpečnom prostredí (podľa bodu 7.8 tohto dokumentu) osobami, zaradenými v dôveryhodných rolách (podľa bodu 7.3 tohto dokumentu) za účasti minimálne dvoch oprávnených osôb. Okruh osôb, autorizovaných vykonávať túto funkciu, je obmedzený len na osoby v rolách, vymenovaných v dokumente CPS TSA [7].
- Generovanie TSU podpisového kľúča, je vykonávané v bezpečnom kryptografickom zariadení, ktoré je dôveryhodným systémom, spĺňajúcim úroveň EAL 4+ resp. FIPS-140-3.

- 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.
- Podpisový kľúč TSU nie je možné importovať do iného kryptografického modulu bez rozhodnutia bezpečnostného správcu a za účasti stanoveného počtu oprávnených osôb.
- V kryptografických moduloch jednotlivých TSU sú rôzne podpisové kryptografické kľúče.
- TSU má v danom čase k dispozícii len jeden aktívny kľúč na podpisovanie časovej pečiatky.

7.6.3 Ochrana súkromného kľúča TSU

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

- 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 0, resp. spĺňa požiadavky FIPS 140-3.
- 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 [7].
- Akékoľvek záložné kópie súkromných podpisových kľúčov, nachádzajúce sa mimo TSU, sú chránené tak, že je zabezpečená ich integrita a dôvernosť.

7.6.4 Certifikát verejného kľúča TSU

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

- Verejný kľúč TSU, ktorý slúži na overenie podpisu, je dostupný Spoliehajúcim sa stranám v certifikáte verejného kľúča.
- Certifikát verejného kľúča TSU pre overenie podpisu je vydaný certifikačnou autoritou, poskytujúcou služby v zmysle normy ETSI EN 319 411-1 0.
- 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.

7.6.5 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.

7.6.6 Manažment životného cyklu podpisového kryptografického hardvéru

Aplikované sú nasledovné požiadavky:

- Do kryptografického hardvéru, určeného na podpisovanie časových pečiatok, nesmie byť svojvoľne zasahované počas jeho prepravy.
- Do kryptografického hardvéru, ktorý podpisuje časové pečiatky, nesmie byť svojvoľne zasahované počas jeho skladovania.
- Inštalácia, aktivácia a duplikácia podpisových kľúčov TSU v kryptografickom hardware je vykonávaná iba osobami v dôveryhodných rolách, s minimálne dvojitou kontrolou a vo fyzicky bezpečnom prostredí (podľa bodu 7.8 tohto dokumentu).
- Súkromné podpisové kľúče TSU, uložené v kryptografickom module TSU, sú v prípade vyradenia modulu vymazané takým spôsobom, že je prakticky nemožné ich obnovenie.

7.6.7 Ukončenie životného cyklu kľúča TSU

Životný cyklus kľúčov TSA je ukončený:

- vypršaním platnosti certifikátu,
- zrušením platnosti služby TSA v dôveryhodnom zozname a rovnako 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).

7.7 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 kvalifikovanej elektronickej časovej pečiatky prebieha v nasledujúcich fázach:

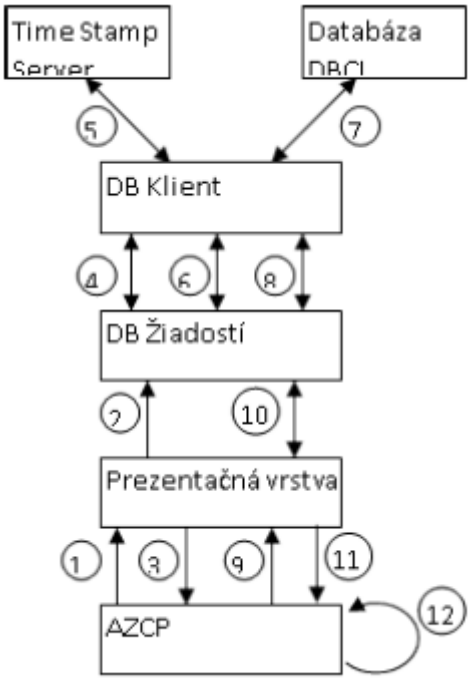
- vygenerovanie žiadosti o pridelenie kvalifikovanej elektronickej časovej pečiatky,
- odoslanie žiadosti o pridelenie kvalifikovanej elektronickej časovej pečiatky,
- prijatie odpovede na žiadosť o kvalifikovanú elektronickú časovú pečiatku (TSR).

Na hašovanie pri vydávaní časových pečiatok je použitý algoritmus, podľa zoznamu povolených algoritmov, uverejnených v podpisovej politike podľa §11 ods. 1 pism. m) zákona 272/2016 Z. z.. Na podpisovanie časových pečiatok (šifrovanie produktu hašovania) je použitý algoritmus RSA s dĺžkou kľúča 3072 bitov a viac.

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

7.7.1 Vydanie časovej pečiatky

7.7.1.1 Architektúra časovej pečiatky



Základný popis funkčnosti časovej pečiatky:

1. Pripojenie sa k službe vyhotovovania časovej pečiatky, vytvorenie a poslanie žiadosti.
2. Prezenčná vrstva (PV) vygeneruje jedinečné číslo Req_ID, zapíše žiadosť do databázy žiadostí (DBŽ) a 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 neskôr.

7.7.1.2 Podanie žiadosti o vydanie časovej pečiatky

Žiadosť o pridelenie kvalifikovanej elektronickej časovej pečiatky, vygeneruje klient TS vo formáte TSQ.

Klient TS odošle vygenerovanú žiadosť o pridelenie kvalifikovanej elektronickej časovej pečiatky protokolom HTTP serveru TSA.

Klient podáva žiadosť o vydanie časovej pečiatky podľa nasledovného postupu:

- žiadosť o vydanie časovej pečiatky sa podáva prostredníctvom internetových stránok:

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

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

  TSU (6,7,8) – http://tsa.nbu.gov.sk/tsa
- komunikácia je realizovaná protokolom http,
- žiadosť o vydanie časovej pečiatky, musí byť vo formáte *TimeStampReq* podľa IETF RFC 3161, kde sa nemusí uvádzať OID politiky časovej pečiatky,
- žiadosť o vyhotovenie 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,
- za správnosť žiadosti o časovú pečiatku zodpovedá žiadateľ.

7.7.1.3 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 informačné údaje o časovej pečiatke. Údaje tela TST sú podpísané hašovacím algoritmom podľa zoznamu povolených algoritmov, uverejnených v podpisovej politike podľa §11 ods. 1 pism. m) zákona 272/2016 Z. z. a kryptovaním 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.

7.7.1.4 Prijatie odpovede na žiadosť o časovú pečiatku

Proces prevzatia časovej pečiatky je synchrónny. Klient TS prevezme vygenerovanú časovú pečiatku pri HTTP volaní, pri ktorom zasiela žiadosť.

Prevzatá časová pečiatka má štandardný formát podľa RFC 3161.

7.7.1.5 Overovanie časových pečiatok

Overovanie časových pečiatok sa musí vykonať v nasledovných krokoch:

- overenie platnosti certifikátu verejného kľúča TSA podľa stavu v dôveryhodnom zozname, zverejnenom na internetovej adrese:

  http://www.nbu.gov.sk/doveryhodne-sluzby/doveryhodne-zoznamy/

  a informatívne, pomocou 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.

7.7.2 Synchronizácia hodín s UTC

Hodiny TSA, používané ako zdroj času pre časové pečiatky, sú synchronizované od zdroja presného času GPS.

Synchronizácia času zaručuje presnosť lepšiu ako 1 sekunda.

7.8 Fyzická a objektová bezpečnosť

Pravidlá a zásady pre zaistenie fyzickej a objektovej bezpečnosti sú popísané a definované v dokumente „Politika poskytovania dôveryhodných služieb NASES“ [2], bod 5.6.

NASES, ako prevádzkovateľ SNCA a poskytovateľ služby vyhotovovania časových pečiatok, garantuje bezpečnú prevádzku systému TSA SNCA a dostupnosť uvedenej služby, aplikovaním dodatočných opatrení, v rozsahu:

- Na kryptografický modul musí byť aplikované riadenie prístupu v súlade s bodom 6.5 tejto TSAP.
- Na správu služby vyhotovovania časových pečiatok, musia byť aplikované nasledovné dodatočné opatrenia:
  - Technické prostriedky služby vyhotovovania 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 sa nachádza v bezpečnej oblasti. Každý vstup a prítomnosť musia byť zaznamenané.
  - Fyzická ochrana musí byť dosiahnutá vytvorením jasne definovanej bezpečnostnej hranice (perimetrom, fyzickou bariérou) okolo správy služby 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 prevádzkované softvérové prostriedky, súvisiace so službou vyhotovovania časových pečiatok, pred vynesením bez autorizácie.

7.9 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 (TSS), určené na podpisovanie a overovanie vyhotovovaných 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 server TSS, bude záloha súkromného kľúča zničená.

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

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

7.10 Sieťová bezpečnosť

Systém a pravidlá na zaistenie sieťovej bezpečnosti, sú popísané a definované v dokumente „Politika poskytovania dôveryhodných služieb NASES“ [4], bod 5.8.

NASES, ako prevádzkovateľ SNCA a poskytovateľ služby vyhotovovania časových pečiatok, garantuje bezpečnú prevádzku systému TSA SNCA a dostupnosť uvedenej služby, aplikovaním dodatočných opatrení, v rozsahu:

- SNCA udržiava a chráni všetky TSU v bezpečnej zóne,
- všetky systémy TSU sú nakonfigurované tak, že majú odstránené a/alebo zakázané všetky účty, aplikácie, služby, protokoly a porty, ktoré nie sú používané pre ich prevádzku,
- do bezpečných zón a vysoko bezpečných zón majú prístup iba dôveryhodné roly.

7.11 Riadenie bezpečnostných incidentov

Systém riadenia bezpečnostných incidentov je popísaný a definovaný v dokumente „Politika poskytovania dôveryhodných služieb NASES“ [4], bod 5.9.

7.12 Zber dôkazov

Všeobecné požiadavky na zber dôkazov sú popísané a definované v dokumente „Politika poskytovania dôveryhodných služieb NASES“[4], bod 5.10.

V súvislosti s poskytovaním služby vyhotovovania časových elektronických pečiatok, je zber dôkazov zabezpečovaný zaznamenávaním a bezpečným uchovávaním informácií, súvisiacich s poskytovaním služby vyhotovovania časových elektronických pečiatok.

Procesy, pri poskytovaní služby vyhotovovania časových pečiatok, zaznamenávajú auditné 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 vyhotovovania elektronických časových pečiatok, slúži databáza DB Klienta, v ktorej sa kontinuálne ukladajú informácie v nasledovnom rozsahu:

- zoznam vydaných časových pečiatok,
- zoznam vydaných odpovedí,
- informácie o mimoriadnych udalostiach v systéme, používanom na manažment časových pečiatok,
- informácie o dôležitých udalostiach v prostredí vydavateľa časových pečiatok, manažmente kryptografických kľúčov a v synchronizácii zdrojov času, vrátane presných časových údajov, s dôrazom na:
  - riadenie životného cyklu kľúčov TSU;
  - riadenie životného cyklu certifikátov TSU;
  - synchronizáciu hodín TSU s UTC, vrátane informácií, týkajúcich sa pravidelnej, 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 servera časovej pečiatky (TSS), a pod.),
- záznamy o prekročení maximálneho počtu vlákien (threadov), ku ktorému môže dôjsť pri nadmernom zaťažení služby vyhotovovania časovej pečiatky.

Riadenie kontinuity činnosti organizácie

Pre riadenie kontinuity činnosti poskytovateľa platia ustanovenia, popísané a definované v dokumente „Politika poskytovania dôveryhodných služieb NASES“ [4]0, bod 5.11.

NASES, ako prevádzkovateľ SNCA a poskytovateľ služby vyhotovovania časových pečiatok, garantuje bezpečnú prevádzku systému TSA SNCA a dostupnosť uvedenej služby, aplikovaním dodatočných opatrení, v rozsahu:

- Plán obnovy po pohrome musí definovať postupy pre obnovu služby, pokrývajúce možnú kompromitáciu, prípadne podozrenie z kompromitácie súkromného kľúča TSU alebo stratu kalibrácie hodín TSU, čo mohlo mať vplyv na vydané časové pečiatky.
- V prípade kompromitácie alebo podozrenia z kompromitácie alebo straty kalibrácie pri vyhotovovaní časovej pečiatky, musí Poskytovateľ sprístupniť všetkým odberateľom a Spoliehajúcim sa stranám popis kompromitácie, ktorá nastala.
- V prípade kompromitácie prevádzky TSU (napr. kompromitácia kľúča TSU), podozrenia z kompromitácie alebo straty TSU kalibrácie, nesmie Poskytovateľ vyhotovovať časové

pečiatky do doby, pokiaľ nebudú vykonané kroky na obnovu po kompromitácii.

- V prípade významnej kompromitácie prevádzky Poskytovateľa alebo straty kalibrácie, je Poskytovateľ povinný sprístupniť všetkým odberateľom a Spoliehajúcim sa stranám informáciu, ktorá môže byť použitá na identifikáciu časových pečiatok, ktoré mohli byť ovplyvnené, pokiaľ tým neporuší súkromie používateľov Poskytovateľa alebo bezpečnosť služieb Poskytovateľa.

7.13 Ukončenie činnosti Poskytovateľa a plány ukončenia činnosti

Pre ukončenie činnosti Poskytovateľa platia ustanovenia, popísané a definované v dokumente „Politika poskytovania dôveryhodných služieb NASES“ [4], bod 5.12.

NASES, ako prevádzkovateľ SNCA a poskytovateľ služby vyhotovovania časových pečiatok, garantuje bezpečnú prevádzku systému TSA SNCA a dostupnosť uvedenej služby, aplikovaním dodatočných opatrení, v rozsahu:

- V prípade ukončenia služieb Poskytovateľa, musia byť zrušené všetky certifikáty, vydané pre jednotlivé TSU.
- Ukončenie činnosti TSA bude oznámené žiadateľom služby vyhotovovania časovej pečiatky a verejne ohlásené verejnými oznamovacími prostriedkami.

7.14 Zhoda

NASES, ako prevádzkovateľ SNCA a poskytovateľ služby vyhotovovania kvalifikovaných elektronických časových pečiatok, sa pri zabezpečení prevádzky uvedenej služby riadi:

- Nariadením eIDAS, [2]
- Zákonom č. 272/2016 Z. z. o dôveryhodných službách, [14]
- Ostatnými, všeobecne platnými nariadeniami, platnými v SR, vzťahujúcimi sa k výkonu tejto činnosti.

8 Plnenie požiadaviek pre kvalifikované elektronické časové pečiatky podľa Nariadenia eIDAS

8.1 Certifikát verejného kľúča TSU

V zmysle Nariadenia eIDAS [2], pre kvalifikované elektronické časové pečiatky, 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 [10].

8.2 Vyhotovovanie nekvalifikovaných a kvalifikovaných elektronických časových pečiatok podľa Nariadenia eIDAS

Ak TSU, zahrnutá v systéme Poskytovateľa, vyhotovuje časové pečiatky, ktoré sú vyhlasované ako kvalifikované elektronické pečiatky podľa Nariadenia eIDAS [2], táto TSU nesmie vyhotovovať nekvalifikované elektronické časové pečiatky.

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