NÁRODNÁ AGENTÚRA PRE SIEŤOVÉ A ELEKTRONICKÉ SLUŽBY

Národná agentúra pre sieťové a elektronické služby

Politika poskytovania kvalifikovaných dôveryhodných služieb uchovávania kvalifikovaných elektronických podpisov a uchovávania kvalifikovaných elektronických pečatí

Verzia dokumentu	1.2
Dátum vydania	03.12.2024
Názov dokumentu	Politika poskytovania kvalifikovaných dôveryhodných služieb uchovávania kvalifikovaných elektronických podpisov a uchovávania kvalifikovaných elektronických pečatí
Gestor	Riaditeľ sekcie prevádzky informačných systémov
Vlastník	NASES

Denník zmien:

Dátum	Verzia	Predmet	Spracoval
20.12.2017	1.0	Prvá verzia dokumentu	Ing. Dana Gáliková
15.06.2018	1.1	Úprava dokumentu – aktualizácia	Ing. Dana Gáliková
03.12.2024	1.2	Úprava dokumentu – aktualizácia	Marek Žáčik, Štefan Szilva

Skontroloval:

Funkcia	Meno	Verzia	Dátum	Podpis
Riaditeľ SB NASES	Mgr. Peter Frolo	1.0	21.12.2017	
PMA	Štefan Szilva	1.2	11.11.2024	

Schválil:

Funkcia	Meno	Verzia	Dátum	Podpis
Generálny riaditeľ NASES	Ing. Ľubomír Mindek	1.2	12.11.2024	

OBSAH:

1 ÚVOD

Tento dokument (ďalej aj „CP LTA“) definuje politiku a plnenie bezpečnostných požiadaviek, ktoré sa týkajú prevádzkovej praxe a postupov riadenia poskytovania kvalifikovaných dôveryhodných služieb uchovávania kvalifikovaných elektronických podpisov a uchovávania kvalifikovaných elektronických pečatí (ďalej len „dôveryhodná služba“).
Poskytovateľom tejto služby je príspevková organizácia Národná agentúra pre sieťové a elektronické služby so sídlom Kollárova 8, 917 02 Trnava, IČO: 42156424 (ďalej len „NASES“), prostredníctvom svojho vlastného informačného systému pre poskytovanie dôveryhodnej služby.

1.1 Prehľad

Táto politika sa týka poskytovania kvalifikovaných dôveryhodných služieb:

- Služba uchovávania kvalifikovaných elektronických podpisov
- Služba uchovávania kvalifikovaných elektronických pečatí

v zmysle čl. 34 a čl. 40 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, v znení Nariadenia Európskeho parlamentu a Rady (EÚ) 2024/1183 z 11. apríla 2024. (ďalej len „Nariadenie eIDAS“) [1] . Služby sú poskytované v súlade s ETSI EN 319 401[4] a ETSI TS 119 511[6] .

Služby sú prevádzkované v rámci totožnej infraštruktúry a rovnakým spôsobom, preto sa pre obe služby publikujú pravidlá v rámci jedinej CP.

Táto politika bude použitá pre službu poskytovania služieb uchovávania kvalifikovaných elektronických podpisov a pečatí v prostredí Ústredného portálu verejnej správy - www.slovensko.sk (ďalej „ÚPVS“) v správe NASES.

Nakoľko nariadenie eIDAS nešpecifikuje presné požiadavky na „postupy a technológie“, nie je možné určiť presnú záväznú referenčnú normu / smernicu, ktorá by sa kvalifikovaných dôveryhodných služieb týkala a voči ktorej by mala byť táto CP a súvisiace CPS posudzované. Tento dokument teda vychádza zo štruktúry CP, ktorá je definovaná v rámci RFC 3647, s výnimkou kapitol 3 (Identifikácia a autentifikácia), 4 (Požiadavky na životný cyklus certifikátu) a 7 (Profily KC, CRL a OCSP), nakoľko pri poskytovaní služieb uchovávania KEP/KEPe sú bezpredmetné.

Dokument má za cieľ poskytnúť dostatočnú mieru záruky, že navrhnutý systém pre poskytovanie dôveryhodnej služby je dostatočne robustný a dokáže dôveryhodne zabezpečiť predĺženie dôveryhodnosti kvalifikovaného elektronického podpisu, resp. kvalifikovanej elektronickej pečate, aj na obdobie po uplynutí technologickej platnosti.

1.2 Názov dokumentu a jeho identifikácia

Názov:	Politika poskytovania kvalifikovaných dôveryhodných služieb uchovávania kvalifikovaných elektronických podpisov a uchovávania kvalifikovaných elektronických pečatí
Skratka názvu:	CP LTA NASES
Verzia:	1.2
Schválené dňa:	12.11.2024
Platnosť od:	03.12.2024
Identifikátor objektu (OID):	1.3.158. 42156424.0.0.2.0.1

Popis použitého identifikátora objektu (OID):

1.	ISO

1.3.	Identified Organization
1.3.158.	IČO
1.3.158.42156424.	NASES
1.3.158. 42156424.0.	Vyhradené pre NASES
1.3.158. 42156424.0.0.	Vyhradené pre NASES
1.3.158. 42156424.0.0.2.	Služby uchovávania kvalifikovaných elektronických podpisov a uchovávania kvalifikovaných elektronických pečatí
1.3.158. 42156424.0.0.2.0.	Vyhradené pre NASES
1.3.158. 42156424. 0.0.2.0.1	CP LTA

1.3 Účastníci PKI

V rámci poskytovania dôveryhodnej služby sú účastníkmi infraštruktúry verejného kľúča NASES:

1.3.1 Jednotka dôveryhodnej služby (TSU)

Jednotkou dôveryhodnej služby je súbor komponentov a modulov ÚPVS, ktorý slúži na poskytovanie dôveryhodných služieb. Ide predovšetkým o modul dlhodobého uchovávania registratúrnych záznamov (ďalej „MDURZ“).
Samotný modul poskytuje rozhranie na prevádzku všetkých základných funkcií, ktoré koncepčne odpovedajú OAIS modelu (ISO 14721) pre elektronický archív, zároveň zabezpečuje funkcionalitu dlhodobého ukladania a overovania kvalifikovaných elektronických podpisov a kvalifikovaných elektronických pečatí, pričom na kryptografické operácie využíva komponent ÚPVS – Centrálnu elektronickú podateľňu (ďalej „CEP“), v rámci ktorej je prevádzkovaný systém na vyhotovovanie a overovanie kvalifikovaného elektronického podpisu a kvalifikovanej elektronickej pečate, ako aj sústava kvalifikovaných zariadení pre elektronický podpis a pečať s platnou certifikáciou.
Samotný princíp dlhodobej overiteľnosti KEP/KEPe je založený na vytváraní integritných elektronických podpisov (pečatí) pre zoznam digitálnych odtlačkov vytvorený z dokumentov podpísaných KEP/KEPe a z údajov potrebných pre ich overenie a na vytváraní archívnej formy integritných podpisov pred koncom ich platnosti. Pre tento účel sa využívajú služby modulu CEP – podpísanie (pečatenie) dokumentov, overenie podpisov, prevod el. podpisu na archívnu formu a časové pečiatky vydávané kvalifikovaným poskytovateľom dôveryhodných služieb.
Poskytovateľom dôveryhodných služieb je NASES. Viď aj kap. 1.5.1.

1.3.2 Klienti

Klientmi dôveryhodných služieb sú používatelia s aktivovanou elektronickou schránkou v rámci modulu eDesk na ÚPVS, ktorí žiadajú o ukladanie záznamov opatrených kvalifikovaným elektronickým podpisom alebo kvalifikovanou elektronickou pečaťou do MDURZ v rámci ÚPVS. Jedná sa predovšetkým o orgány verejnej moci („OVM“), štatutárov právnických osôb, živnostníkov a fyzické osoby.

1.3.3 Spoliehajúca sa strana

Spoliehajúca sa strana je tretia strana, ktorá sa pri svojom konaní spolieha na dôveryhodné služby NASES.
Spoliehajúce sa strany nemusia byť nevyhnutne zmluvní partneri NASES.

1.3.4 Iní účastníci

Autorita pre správu politík

Autorita pre správu politík (ďalej len „PMA“) je zložka NASES ustanovená za účelom:

- dohľadu nad vytváraním a aktualizáciou CP a CPS, vrátane vyhodnocovania zmien a plánov na implementovanie ľubovoľných prijatých zmien,
- revízie výsledkov auditov, aby sa určilo, či NASES zodpovedne dodržiava ustanovenia vydanej CP,
- vydávanie odporúčaní pre NASES týkajúce sa nápravných a iných vhodných opatrení,
- riadenia a usmerňovania činnosti NASES ako poskytovateľa dôveryhodnej služby..

PMA predstavuje zložku pre dohľad a vypracovanie rozhodnutí v prípade sporných udalostí a aspektov týkajúcich sa NASES ako poskytovateľa dôveryhodnej služby.

1.4 Použiteľnosť uchovávaných KEP/KEPe

Kvalifikované elektronické podpisy a kvalifikované elektronické pečate, ktoré sú uchovávané v rámci poskytovania dôveryhodných služieb môžu byť použité výlučne v súlade s požiadavkami nariadenia eIDAS.

1.5 Správa politiky

1.5.1 Organizácia zodpovedná za správu dokumentu

Nasledujúca tabuľka obsahuje údaje poskytovateľa (NASES), ktorý je zodpovedný za prípravu, vytvorenie a udržiavanie tohto dokumentu.

Tabuľka 1 Kontaktné údaje poskytovateľa

Organizácia	Národná agentúra pre sieťové a elektronické služby
Adresa	Kollárova 8 917 02 Trnava
Adresa detašovaného pracoviska	Tower 115 Pribinova 25 811 09 Bratislava
IČO	42156424
Telefón	+421 2 3278 0700
E-mail	info@nases.gov.sk
Webové sídlo	https://www.nases.gov.sk/

1.5.2 Kontaktná osoba

Na účel tvorby politík a pravidiel má NASES vytvorenú autoritu pre správu politík (PMA), ktorá plne zodpovedá za ich obsah a ktorá je pripravená odpovedať na všetky otázky týkajúce sa politík a pravidiel NASES ako poskytovateľa dôveryhodnej služby.

Tabuľka 2 Kontaktné údaje na zložku zodpovednú za prevádzku dôveryhodnej služby

Zodpovedný:	Riaditeľ sekcie prevádzky informačných systémov
Organizácia	Národná agentúra pre sieťové a elektronické služby
Adresa:	Kollárova 8, 917 02 Trnava
Telefón	+421 2 3278 0700
E-mail	info@nases.gov.sk
Fax:	
Webové sídlo:	https://www.nases.gov.sk/

1.5.3 Pravidlá schvaľovania CP

- Poskytovateľ musí mať schválenú svoju CP ešte pred začiatkom prevádzky dôveryhodnej služby.
- Obsah certifikačnej politiky schvaľuje generálny riaditeľ NASES na základe návrhu PMA.
- Po schválení musí byť príslušný dokument publikovaný v súlade s publikačnou a oznamovacou politikou.
- Poskytovateľ musí spĺňať všetky požiadavky schválenej CP.

1.6 Definície a skratky

1.6.1 Definície

Jednotka dôveryhodnej služby: sústava technických a programových prostriedkov, ktorá je spravovaná s účelom poskytovať kvalifikované dôveryhodné služby prevádzkovateľa

Dôveryhodná služba: kvalifikovaná dôveryhodná služba v zmysle nariadenia eIDAS. V zmysle tejto CP sa za dôveryhodné služby považujú služby uchovávania kvalifikovaných elektronických podpisov a kvalifikovaných elektronických pečatí.
Poskytovateľ dôveryhodnej služby: entita, ktorá poskytuje jednu alebo viac dôveryhodných služieb
Kvalifikovaná elektronická pečať: pečať vyhotovená pomocou kvalifikovaného zariadenia na vyhotovenie elektronickej pečate a založená na kvalifikovanom certifikáte pre elektronickú pečať
Elektronická pečať: údaje v elektronickej forme, ktoré sú pripojené alebo logicky pridružené k iným údajom v elektronickej forme s cieľom zabezpečiť pôvod a integritu týchto pridružených údajov.

1.6.2 Skratky

CA — Certifikačná autorita, autorita vyhotovujúca certifikáty verejného kľúča (Certification Authority)
CP — Certifikačná politika
CPS — Pravidlá poskytovania dôveryhodnej služby
CEP — Centrálna elektronická podateľňa
FOB — Fyzická a objektová bezpečnosť
GDPR — Všeobecná nariadenie o ochrane osobných údajov (General Data Protection Regulation)
HSM — Hardvérový bezpečnostný modul (Hardware security module)
IS — Informačný systém
IT — Informačná technológia (Information Technology)
KEP — Kvalifikovaný elektronický podpis
KEPe — Kvalifikovaná elektronická pečať
MDURZ — Modul dlhodobého uchovávania registratúrnych záznamov
NASES — Národná agentúra pre sieťové a elektronické služby
NBÚ SR — Národný bezpečnostný úrad Slovenskej republiky
OID — Object identifier
OVM — Orgán verejnej moci
PMA — Autorita pre správu politík (Policy Management Authority)
PKI — Infraštruktúra verejného kľúča (Public Key Infrastructure)
RA — Registračná autorita
TS — Dôveryhodná služby (Trust Service)
TSP — Poskytovateľ dôveryhodnej služby (Trust Service Provider)
TSU — Jednotka dôveryhodnej služby (Trust Service Unit)
ÚPVS — Ústredný portál verejnej správy

2 ZODPOVEDNOSTI ZA PUBLIKÁCIU A ÚLOŽISKO

2.1 Úložiská informácií

- Úložiská informácií musia byť umiestnené tak, aby boli prístupné klientom a Spoliehajúcim sa stranám a v súlade s celkovými bezpečnostnými požiadavkami NASES.
- Funkciu úložiska informácií zastáva webové sídlo NASES. Presná URL adresa je uvedené v kapitole 1. Webové sídlo NASES je prostredníctvom internetu verejne prístupné Klientom, Spoliehajúcim sa stranám a verejnosti vôbec.
- Verejne dostupné informácie uvedené na webovom sídle NASES majú charakter riadeného prístupu.

2.2 Zverejňovanie informácií o dôveryhodnej službe

NASES zverejní, v on-line režime:

- úložisko, ktoré je prístupné Klientom a Spoliehajúcim sa stranám,

- prostredníctvom svojho webového sídla túto CP ako aj ďalšie dokumenty súvisiace s poskytovaním dôveryhodných služieb v zmysle tejto CP.

2.3 Frekvencia zverejňovania informácií

- CP prípadne jej revízie sa musia zverejniť čo najskôr po ich schválení a vydaní.
- Všetky ďalšie informácie, ktoré majú byť publikované v úložisku, sa musia publikovať podľa možnosti čo najskôr.

2.4 Kontrola prístupu k repozitárom

- NASES musí zabezpečiť riadenie prístupu k uloženým dokumentom s KEP / KEPe na základe prístupových práv vyplývajúcich z informácií o pôvodcovi KEP / KEPe.
- NASES musí chrániť ľubovoľnú informáciu uloženú v úložisku, ktorá nie je určená na verejné rozšírenie.
- NASES musí vynaložiť maximálne úsilie na to, aby zaistil integritu, dôvernosť a dostupnosť dát vyplývajúcich s poskytovanej dôveryhodnej služby.
- NASES musí 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

3.1 Všeobecné ustanovenia politiky

- Tento dokument nadväzuje na dokument „Politika poskytovania dôveryhodných služieb“ [2] , kde sú popísané všeobecné pravidlá poskytovania dôveryhodných služieb.
- Klienti, Spoliehajúce sa strany a tretie strany poskytujúce podporné služby musia konzultovať podrobnosti spôsobu poskytovania dôveryhodnej služby priamo s poskytujúcou TSU NASES.

3.2 Služby súvisiace s dôveryhodnou službou

NASES prostredníctvom TSU v rámci ÚPVS poskytuje orgánom verejnej správy, ďalším modulom ÚPVS a používateľom ÚPVS službu dlhodobého uchovávania elektronických dokumentov podpísaných kvalifikovaným elektronickým podpisom alebo opatrených kvalifikovanou elektronickou pečaťou. Základná funkcionalita TSU je najmä:

- trvalá čitateľnosť a jednoznačnosť obsahu uložených záznamov
- udržiavanie dôveryhodnosti elektronických podpisov, pečatí a pečiatok
- príjem registratúrnych záznamov vo forme spisu
- správa spisov a ich položiek (vyhľadávanie, výpožičky, sledovanie histórie)
- vyraďovanie záznamov

Podrobný popis kvalifikovanej služby a súvisiacich služieb je uvedený v CPS LTA [5] .

3.3 Poskytovateľ dôveryhodnej služby

- Poskytovateľ dôveryhodnej služby pre potreby Klientov v zmysle tejto CP je NASES (pozri kapitola 1).
- NASES musí niesť celkovú zodpovednosť za poskytovanie služieb súvisiacich s dôveryhodnou službou, ako sú definované v odstavci 3.2.
- NASES môže prevádzkovať niekoľko identifikovateľných nezávislých jednotiek na poskytovanie dôveryhodnej služby (TSU).

4 FYZICKÉ, PROCEDURÁLNE A PERSONÁLNE BEZPEČNOSTNÉ OPATRENIA

NASES musí mať bezpečnosť založenú na súhrne bezpečnostných opatrení v oblasti fyzickej, objektovej, personálnej a prevádzkovej bezpečnosti. Bezpečnostné opatrenia musia byť navrhnuté, dokumentované a aplikované na základe bezpečnostných pravidiel a schválené vedením NASES.
Bezpečnostné opatrenia musia byť k dispozícii všetkým pracovníkom, ktorých sa týkajú.
NASES musí:

- niesť plnú zodpovednosť za súlad svojej činnosti s postupmi definovanými vo svojej bezpečnostnej politike.
- mať zoznam všetkých svojich aktív s vyznačením ich klasifikácie v zmysle vykonaného posúdenia rizika.

Bezpečnostná politika NASES a súhrn aktív týkajúci sa bezpečnosti musia byť preskúmavané v pravidelných intervaloch, prípade pri významných zmenách na zaistenie ich kontinuity, vhodnosti, dostatočnosti a účinnosti.
Všetky zmeny, ktoré môžu ovplyvniť úroveň poskytovanej bezpečnosti musia byť schválené vedením NASES.
Nastavenie systémov NASES musí byť pravidelne preskúmavané na zmeny, ktoré ohrozujú jeho bezpečnostnú politiku.

4.1 Opatrenia fyzickej bezpečnosti

Proces FOB musí byť riadený a musia byť definované pravidlá pre fyzickú a objektovú bezpečnosť a ďalej :

- Na kryptografický modul je aplikované riadenie prístupu.
- Technické prostriedky na uchovávanie KEP/KEPe sú 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 podlieha nezávislému dohľadu a neautorizovaná osoba musí byť sprevádzaná autorizovanou osobou pokiaľ je v bezpečnej oblasti. Každý vstup a prítomnosť je zaznamenaná.
- Fyzická ochrana je dosiahnutá vytvorením jasne definovanej bezpečnostnej hranice (perimetrom, fyzickou bariérou) okolo správy dôveryhodných služieb. Akékoľvek časti objektu zdieľané s inými organizáciami sú mimo tohto perimetra.
- Fyzické a objektové bezpečnostné opatrenia chránia objekty, kde sú umiestnené systémy, samotné systémové zdroje a objekty použité na podporu ich prevádzky. Bezpečnostné opatrenia týkajúce sa fyzickej a objektovej bezpečnosti NASES pokrývajú 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 chránia zariadenia, informácie, médiá a softvér týkajúcich sa dôveryhodných služieb pred vynesením bez autorizácie.

4.1.1 Lokalizácia a konštrukcia prevádzkových priestorov

Všetky systémy a zariadenia NASES musia byť umiestnené v bezpečných priestoroch chránených pred neautorizovaným prístupom nepovolaných osôb, pred živelnými pohromami a haváriami v inžinierskych sieťach.

4.1.2 Fyzický prístup

Prístup do priestorov umiestnenia infraštruktúry poskytujúcej dôveryhodné služby musí byť riadený. NASES má pripravené spôsoby a postupy na ochranu svojich počítačových systémov, údajov a archívov proti neoprávnenej manipulácii, krádeži a prezradeniu. Vstup cudzích osôb môže byť povolený len v sprievode oprávnenej osoby a každý takýto vstup musí byť zaznamenaný.

4.1.3 Napájanie a vzduchotechnika
Komponenty systému musia byť chránené viacerými zdrojmi elektrického napájania. Priestory, v ktorých sa nachádza infraštruktúra poskytujúca dôveryhodné služby, musia byť vybavené klimatizáciou.

4.1.4 Možné vystavenia vode
Priestory musia byť chránené proti nebezpečenstvu pôsobenia vody.

4.1.5 Predchádzanie požiarom a ochrana pred požiarmi
Priestory musia byť chránené dymovými a požiarnymi detektormi.

4.1.6 Uchovávanie médií
NASES musí uchovávať všetky médiá, ako sú pásky a dokumenty, v bezpečnom prostredí.

Médiá majú byť uchovávané tak, aby boli chránené pred poškodením (voda, oheň, elektromagnetické poškodenie). Médiá obsahujúce záznamy pre audit, archívne alebo zálohované informácie majú byť uchovávané v priestoroch, ktoré nie sú fyzicky spojené s prevádzkovými priestormi NASES v súlade s príslušnými internými smernicami NASES a právnymi predpismi SR.

4.1.7 Odpadové hospodárstvo
Nosiče informácií, obsahujúce citlivé informácie, musia byť likvidované v zmysle postupov, stanovených záväznými vnútornými predpismi, kde je uvedená klasifikačná schéma citlivosti informácií.

4.1.8 Záložné prevádzkové priestory
Okrem prevádzkových priestorov umiestnenia NASES musí prevádzkovateľ zabezpečiť záložné prevádzkové priestory určené na ukladanie pravidelných záložných kópií a archívnych dát.

4.2 Procedurálne opatrenia

4.2.1 Dôveryhodné roly
NASES musí mať definované dôveryhodné roly zodpovedné za jednotlivé aspekty poskytovaných dôveryhodných služieb ako PMA, administrátor, bezpečnostný manažér, interný audítor a pod.. Zároveň musia byť definované zodpovednosti jednotlivých rolí.

Osoby vybrané na zastávanie rolí, ktoré si vyžadujú dôveryhodnosť, musia byť zodpovedné a dôveryhodné.

Spôsob a bezpečnosť vykonávania činností vyplývajúcich pre jednotlivé roly musí byť pravidelne kontrolovaná.

Definícia roly musí pokrývať: rozsah činností ktoré môže pracovník vykonávať, rozsah zodpovednosti pracovníka za vykonávané činnosti, pravidlá na obmedzenie fyzického prístupu do priestorov umiestnenia TSU, spôsob autentifikácie pracovníka pri vykonávaní činností, požiadavky na znalosti a skúsenosti a zlučiteľnosť príslušnej roly s ďalšími rolami.

4.2.2 Počet pracovníkov vyžadovaných na vykonávanie činností
Pre každú úlohu musí byť identifikovaný počet jednotlivcov, ktorí sú určení na vykonávanie jednotlivých úloh (pravidlo K z N).

4.2.3 Identifikácia a autentizácia pre každú rolu
Každá rola musí mať definovaný spôsob identifikácie a autentifikácie pri prístupe k IS NASES.

4.2.4 Nezlučiteľnosť rolí
Každá rola musí mať stanovené kritériá, ktoré zohľadňujú potrebu oddelenia funkcií z hľadiska samotnej roly t. j. musia byť uvedené roly, ktoré nemôžu byť vykonávané rovnakými jednotlivcami.

4.3 Personálne opatrenia

Každý pracovník musí byť preukázateľne poučený o svojich povinnostiach, bezpečnostných a pracovných postupoch požadovaných pri plnení úloh vyplývajúcich z jeho roly.

4.3.1 Požiadavky na kvalifikácie, skúsenosti a oprávnenia

Zamestnanci Poskytovateľa musia byť schopní spĺňať požiadavky odborných vedomostí, skúseností a kvalifikácie prostredníctvom formálneho vzdelávania, školení a certifikátov, prípadne prostredníctvom reálnych skúseností alebo kombináciou oboch.

4.3.2 Procedúry preverovania osôb

Všetci zamestnanci NASES musia byť pred prijatím do zamestnania primerane preverení v zmysle bezpečnostnej politiky NASES a národnej legislatívy.

4.3.3 Požiadavky na školenia personálu

Osoby zabezpečujúce činnosti v prevádzke ÚPVS a TSU musia byť pravidelne preškoľované z tém špecifických pre oblasť informačnej bezpečnosti. Rozsah školení pre jednotlivých pracovníkov je definovaný ich rolami.

4.3.4 Požiadavky na preškoľovanie personálu a jeho frekvencia

Pre roly, kde sú stanovené požiadavky na absolvovanie predpísaných školení je možné stanoviť potrebu ich opakovania po absolvovaní primárneho školenia..

4.3.5 Frekvencia a postupnosť rotácie rolí

Bez ustanovení.

4.3.6 Sankcie za neoprávnené činnosti

Udeľovanie sankcií za neoprávnené činnosti sa musí riadiť bezpečnostnou politikou NASES a právnymi predpismi SR.

4.3.7 Požiadavky na nezávislých dodávateľov

Externé organizácie, ktoré vystupujú ako zmluvní dodávatelia činností pre ÚPVS musia spĺňať pravidlá stanovené prevádzkovateľom.

Každý pracovník, zabezpečujúci zmluvné činnosti, musí mať vo svojej pracovnej náplni pridelenú rolu na zabezpečení činností a s tým súvisiacu bezpečnostnú rolu. Každý pracovník, zabezpečujúci zmluvné činnosti, musí byť preukázateľne poučený o svojich povinnostiach, bezpečnostných a pracovných postupoch požadovaných pri plnení úloh vyplývajúcich z jeho roly.

4.3.8 Dokumentácia poskytovaná pracovníkom

Na definovanie povinností a procedúr pre každú rolu musí byť poskytnutá pracovníkom vykonávajúcim túto rolu dokumentácia v potrebnom rozsahu.

Pracovníci obsluhy NASES sa musia riadiť dokumentmi, ktoré obdržali, len na účely, na ktoré sú určené. Každý pracovník musí byť preukázateľne oboznámený s bezpečnostnou politikou NASES.

4.4 Procedúry spojené s auditnými záznamami

Poskytovateľ musí zaznamenávať a v primeranej dobe udržiavať dostupné všetky relevantné informácie, týkajúce sa údajov vydaných a prijatých Poskytovateľom (aj v prípade, že Poskytovateľ už neposkytuje dôveryhodné služby). Doba uchovávania informácii o životnom cykle kľúčov je 10 rokov. Tieto úkony musí Poskytovateľ vykonávať pre prípad potreby poskytnutia dôkazov v súdnom konaní a zabezpečenia kontinuity služieb.

Prevádzkové záznamy a dokumenty môžu byť uchovávané v papierovej alebo elektronickej forme, podľa toho v akej podobe vznikli.

Prevádzkové záznamy vedené v elektronickej forme musia byť zálohované tak, aby nemohlo dôjsť k ich porušeniu alebo strate.

Prevádzkové záznamy vedené listinnou formou musia byť spravované v režime, ktorý zabezpečí, aby nemohlo dôjsť k ich porušeniu alebo strate.

4.4.1 Typy zaznamenávaných udalostí

V prevádzke NASES sa musia zaznamenávať:

- udalosti (záznamy) súvisiace so základnými funkciami TSU:
  a) vloženie záznamu (ingescia).

b) poskytnutie záznamu (diseminácia).
c) kontrola záznamu.
d) yyradenie záznamu.
e) predĺženie doby uloženia záznamu.
f) obnova integritného elektronického podpisu.

- Procesy týkajúce sa správy certifikátu MDURZ a všetky procesy na HSM module
- Systémové logy komponentov ÚPVS, ktoré zabezpečujú poskytovanie služby.

4.4.2 Frekvencia spracovania záznamov

Záznamy sa musia získavať priebežne a spracovávať v pravidelných intervaloch. Na vyhodnocovanie prevádzkových záznamov TSU musí byť vypracovaný systém pravidelného ako aj náhodného auditu v súlade s internými smernicami NASES.

4.4.3 Doba uchovávania auditných záznamov

Záznamy priebežného dokumentovania kľúčových aktivít musia byť uchovávané minimálne 14 dní. Ostatné prevádzkové záznamy sa musia uchovávať ako aktívne záznamy po dobu min. 14 dní od ich vzniku. Po uplynutí definovanej doby aktívneho života musia byť významné záznamy preradené do archívu.

4.4.4 Ochrana auditných záznamov

Prevádzkové záznamy vedené v elektronickej forme musia byť zálohované tak, aby nemohlo dôjsť k ich porušeniu alebo strate.

Prevádzkové záznamy vedené listinnou formou musia byť spravované v režime, ktorý zabezpečí, aby nemohlo dôjsť k ich porušeniu, znehodnoteniu, alebo strate.

4.4.5 Procedúry zálohovania auditných záznamov

ÚPVS musí zabezpečiť zálohovanie prevádzkových záznamov v súlade s bezpečnostnou politikou, odpovedajúcou smernicou a platnými právnymi predpismi SR.

4.4.6 Systém zberu auditných záznamov

Proces zberu elektronických prevádzkových záznamov musí byť aktivovaný už pri štarte modulov ÚPVS a uzavrie sa len pri vypnutí celého informačného systému.

V prípade prerušenia činnosti automatizovaného systému zberu prevádzkových záznamov musia byť vykonané príslušné kroky na obnovu jeho činnosti alebo využité náhradné možnosti, ktoré boli vopred odsúhlasené ako náhradné riešenie.

4.4.7 Notifikácia subjektu, ktorý spôsobil udalosť

Musia byť popísané pravidlá informovania administrátorov o chybách, vrátane chýb, ktoré vzniknú pri výkone administratívnych činností v rámci TSU.

4.4.8 Posudzovania zraniteľností

Poskytovateľ musí pravidelne vykonávať posúdenie rizík s cieľom identifikovať, analyzovať a vyhodnotiť riziká súvisiace s poskytovaním dôveryhodných služieb.
Poskytovateľ musí zvoliť vhodné opatrenia na riadenie rizík, pričom zohľadňuje výsledky posúdenia rizík. Opatrenia na riadenie rizík majú za cieľ zabezpečiť, že úroveň zabezpečenia je primeraná a úmerná stupňu rizika.
Poskytovateľ určuje bezpečnostné požiadavky a prevádzkové postupy, ktoré sú nevyhnutné pre implementáciu opatrení na riadenie rizík. Opatrenia na riadenie rizík musia byť zdokumentované a dostupné všetkým relevantným roliam.
Manažment NASES schvaľuje posúdenie rizík a akceptuje zvyškové riziká.

4.5 Archivácia záznamov

NASES musí spracovať pravidlá pre zálohovanie a archiváciu TSU, vrátane komplexných postupov zálohovania databáz, úložiska obsahu, ako aj konfiguračné a aplikačné zálohy.

Prevádzkové záznamy a dokumenty môžu byť uchovávané v papierovej alebo elektronickej forme, podľa toho v akej podobe vznikli.

Prevádzkové záznamy vedené v elektronickej forme musia byť zálohované tak, aby nemohlo dôjsť k ich porušeniu alebo strate.

Prevádzkové záznamy vedené listinnou formou musia byť spravované v režime, ktorý zabezpečí, aby nemohlo dôjsť k ich porušeniu alebo strate.

4.5.1 Typy archivovaných záznamov

Minimálne musia byť archivované nasledovné informácie MDURZ:

1) katalóg (databáza) záznamov;
2) úložisko obsahu;
3) pracovné úložisko;
4) aplikačné komponenty a konfigurácia;

Každý archívny záznam musí byť opatrený časovým údajom o dátume jeho vytvorenia.

4.5.2 Doba archivácie

Doba uchovávania archivovaných údajov sa stanovuje na min. 3 roky.

Po vymazaní záznamu musia ostať uchovávané informácie o zázname ako názov a vlastník, ale samotný záznam a súvisiace KEP/KEPe sa nebude uchovávať.

4.5.3 Ochrana archívu

Archívne záznamy musia byť chránené kombináciou fyzickej bezpečnosti, kryptografickej ochrany a režimových opatrení. Archivačné médiá musia byť chránené pred vplyvmi prostredia ako je teplota, vlhkosť a magnetizmus.

4.5.4 Procedúry zálohovania archívu

Procedúry zálohovania archívu musia byť navrhnuté tak, aby zaisťovali kompletné obnovenie služieb.

4.5.5 Požiadavky na pridávanie časových pečiatok k záznamom

Požiadavka sa overuje pri prvom prijatí dokumentu do TSU. Pokiaľ nie je opatrený časovou pečiatkou, je odoslaný do modulu CEP, kde je časová pečiatka pridaná a až následne je dokument uchovaný v rámci MDURZ.

4.5.6 Zberný systém archívu

Systém archívu je implementovaný ako samostatný modul v rámci ÚPVS a postavený na internom riešení modulu MDURZ.

4.5.7 Procedúry na získanie a overenie archívnych informácií

Postupy musia byť podrobne popísané a publikované v rámci manuálov pre používateľov MDURZ.

4.6 Zmena kľúčov

Neuplatňuje sa.

4.7 Kompromitácia a havarijný plán

4.7.1 Procedúry pre riešenie incidentov a havárií

Na zabezpečenie integrity služieb ÚPVS musí NASES zaviesť postupy zálohovania údajov a ich obnovy. NASES musí mať vypracované havarijné postupy a plány obnovy pre poskytovanie dôveryhodných služieb. Postupy v prípade havárie a obnovy musia byť pravidelne preskúmavané a testované (minimálne na ročnej báze) a mali by byť revidované a aktualizované podľa potreby.

4.7.2 IT zdroje, softvér a/alebo postup v prípade poškodenia

ÚPVS musí mať spracované komplexné postupy obnovy v prípade poškodenia časti infraštruktúry.

4.7.3 Procedúry pre prípad kompromitácie súkromného kľúča

Riadi sa pravidlami TSP, ktorý vydáva certifikát na kľúčový pár modulu MDURZ pre vytvorenie integritného podpisu a pravidlami TSP, ktorý poskytuje časové pečiatky.

4.7.4 Schopnosť business kontinuity po havárii

Ako 4.7.2

4.8 Ukončenie poskytovania služieb

NASES pred ukončením poskytovania svojich služieb aplikuje minimálne nasledovné postupy:

a) Informuje o ukončení poskytovania služieb všetkých Odberateľov a iné entity, s ktorými má NASES uzatvorené zmluvy alebo iné formy vzťahov. O ukončení poskytovania služieb informuje aj Spoliehajúce sa strany.
b) Prenesie všetky záväzky týkajúce sa uchovávania informácií potrebných na poskytovanie dôkazov o prevádzke NASES počas primerane stanovenej doby na spoľahlivú stranu.
c) Zničí (vrátane kópií) alebo stiahne z používania primárne kľúče takým spôsobom, že ich nebude možné znovu obnoviť a používať.
d) Vytvorí dohodu (ak je to možné) o prevode poskytovania dôveryhodných služieb pre svojich súčasných Odberateľov na iného poskytovateľa dôveryhodných služieb.
e) Informuje súčasných Odberateľov o možnosti prevzatia uložených záznamov z modulu MDURZ. O formátoch a konkrétnom technickom spôsobe realizácie prevzatia rozhodne NASES najneskôr 3 mesiace pred plánovaným ukončením poskytovania služby po schválení navrhovaného postupu Orgánom dohľadu.

NASES je príspevková organizácia, z toho dôvodu je krytie nákladov na splnenie týchto minimálnych požiadaviek v prípade, že NASES zanikne alebo z iných dôvodov nie je schopný pokryť náklady sám, zabezpečené štátnym rozpočtom.
NASES vo svojich postupoch uvedie ustanovenia o ukončení poskytovania dôveryhodných služieb čo zahŕňa:

a) informovanie všetkých dotknutých entít,
b) prevod záväzkov Poskytovateľa na tretie strany.

NASES bude dodržiavať svoje záväzky o sprístupnení svojho verejného kľúča alebo dôkazov o dôveryhodných službách Spoliehajúcim sa stranám počas primeranej doby, resp. prevedie tieto záväzky na inú dôveryhodnú osobu.

5 TECHNICKÉ BEZPEČNOSTNÉ OPATRENIA

Technické bezpečnostné opatrenia zahrňujú opatrenia na ochranu kryptografických kľúčov a aktivačných údajov, počítačové bezpečnostné opatrenia (riadenie prístupu, audit, testovanie), bezpečnostné opatrenia na vývoj a riadenie bezpečnosti, sieťové bezpečnostné opatrenia a opatrenia pre kryptografické moduly.

Technická časť infraštruktúry ÚPVS (hardvér a softvér) musí pozostávať len z bezpečných systémov a oficiálneho softvéru. Architektúru infraštruktúry ÚPVS musí byť navrhnutá s použitím komponentov, ktoré vyhovujú bezpečnostným štandardom na úrovni súčasných poznatkov.

Súčasťou systému NASES musia byť zariadenia na nepretržitú detekciu, monitorovanie a signalizáciu neautorizovaných a neobvyklých pokusov o prístup k jej prostriedkom.

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

5.1 Generovanie kľúčového páru a inštalácia

Poskytované kvalifikované dôveryhodné služby spracúvajú už vyhotovené kvalifikované elektronické podpisy a kvalifikované elektronické pečate. Pre zaistenie dlhodobej overiteľnosti ich integrity sa vytvárajú integritné elektronické podpisy (pečate) pre zoznam digitálnych odtlačkov vytvorený z KEP/KEPe a údajov potrebných pre ich overenie a následne archívna forma integritných podpisov pred koncom ich platnosti. Pre pečatenie sa používa certifikát kvalifikovanej elektronickej pečate zmluvného TSP a kvalifikované časové pečiatky zmluvného TSP. Generovanie kľúčového páru a inštalácia preto prebieha v zmysle požiadaviek zmluvného TSP.

5.1.1 Generovanie kľúčového páru
Neuplatňuje sa – pozri 5.1.

5.1.2 Doručenie súkromného kľúča žiadateľovi
Neuplatňuje sa – pozri 5.1.

5.1.3 Doručenie verejného kľúča vydavateľovi certifikátu
Neuplatňuje sa – pozri 5.1.

5.1.4 Doručenie verejného kľúča CA spoliehajúcim sa stranám
Neuplatňuje sa – pozri 5.1.

5.1.5 Dĺžky kľúčov
Neuplatňuje sa – pozri 5.1.

5.1.6 Parametre generovania verejného kľúča a kontrola kvality
Neuplatňuje sa – pozri 5.1.

5.1.7 Účely použitia kľúča
Neuplatňuje sa – pozri 5.1.

5.2 Ochrana súkromného kľúča a opatrenia inžinierstva kryptografického modulu

5.2.1 Štandardy a opatrenia pre kryptografický modul
Vybavenie NASES musí byť chránené pred neautorizovaným prístupom a to aj pred neautorizovaným fyzickým prístupom. Pozri aj 5.1.

5.2.2 Rozdelenie kontroly nad prístupom k súkromnému kľúču
Na vykonanie kritických činností na kryptografickom module je nutná súčasná autorizácia dvoch určených pracovníkov NASES. Pozri aj 5.1.

5.2.3 Obnova súkromného kľúča
Neuplatňuje sa.

5.2.4 Zálohovanie súkromného kľúča
Súkromné kľúče NASES musia byť zálohované v zašifrovanej forme, na ich obnovu musí byť nevyhnutná kontrola min. 2 určených pracovníkov. Po ukončení platnosti certifikátu, ktorý je zviazaný s verejným kľúčom prislúchajúcim k zálohovanému súkromnému kľúču, bude záloha súkromného kľúča zničená. Pozri aj 5.1.

5.2.5 Archivácia súkromného kľúča
Nearchivuje sa.

5.2.6 Presun súkromného kľúča do alebo z kryptografického modulu
Presun sa riadi rovnakými podmienkami na bezpečnosť, aké poskytuje kryptografický modul. Export kľúčov je možný výlučne v šifrovanej podobe, oprávneným administrátorom a tak, aby obnova nebola možná. Pozri aj 5.1.

5.2.7 Uloženie súkromného kľúča v kryptografickom module
Súkromný kľúč sa musí generovať priamo v kryptografickom module. Na vygenerovanie súkromného kľúča musí byť potrebná súčasná autorizácia viacerých pracovníkov. Súkromný kľúč musí byť uložený v zašifrovanom tvare. Funkčné, technické a bezpečnostné vlastnosti kryptografického modulu, na ktorom bude uložený súkromný kľúč, spĺňajú požiadavky Nariadenia eIDAS a Zákona o dôveryhodných službách. Pozri aj 5.1.

5.2.8 Metóda aktivácie súkromného kľúča
Súkromné kľúče môžu aktivovať len oprávnené osoby NASES.

Pri aktivácií musí každá oprávnená osoba z potrebného počtu oprávnených osôb vložiť do HSM modulu svoju čipovú kartu a zadať k nej heslo. Po aktivácii sú kľúče v HSM module aktívne až do doby, kým nedôjde k ich deaktivácii oprávnenou osobou (administrátor CEP) alebo výpadkom elektrického napájania HSM modulu. Pozri aj 5.1.

5.2.9 Metóda deaktivácie súkromného kľúča
Deaktiváciu súkromného kľúča v HSM module môže vykonať len oprávnená osoba (administrátor CEP) alebo sú kľúče deaktivované automaticky pri výpadku relácie alebo výpadkom elektrického napájania HSM modulu. Pozri aj 5.1.

5.2.10 Metóda zničenia súkromného kľúča
NASES zabezpečí dôveryhodné a bezpečné zničenie súkromné kľúča po vypršaní jeho platnosti, alebo v prípade zistenia porušenia jeho dôvernosti. Pozri aj 5.1.

5.2.11 Hodnotenie kryptografického modulu
Kryptografické moduly v správe NASES musia spĺňať požiadavky medzinárodného štandardu FIPS 140-2 úroveň 3. Bezpečnosť kryptografických modulov musí byť pravidelne monitorovaná a testovaná. Všetky činnosti súvisiace s prevádzkou kryptografických modulov musia byť zaznamenávané a vyhodnocované. Pozri aj 5.1.

5.3 Ostatné aspekty manažmentu kľúčových párov

5.3.1 Archivácia verejného kľúča
Archivácia verejných kľúčov sa zabezpečuje prostredníctvom archivovania certifikátov, v ktorých sa verejné kľúče nachádzajú. Archiváciu zabezpečuje TSP, ktorý certifikát vydal.

5.3.2 Prevádzková doba certifikátu a doba použitia kľúčového páru
Doba použitia kľúčových párov musí byť totožná s prevádzkovou dobou platnosti príslušných vydaných certifikátov. Dobu používania musí určiť TSP, ktorý vydáva certifikát. Pozri aj 5.1.

5.4 Aktivačné údaje

5.4.1 Generovanie a inštalácia aktivačných údajov
Pozri 5.1

5.4.2 Ochrana aktivačných údajov
Aktivačné údaje nesmú byť zaznamenané na žiadnom nekontrolovane prístupnom médiu. Pozri aj 5.1.

5.4.3 Ostatné aspekty aktivačných údajov
Musí byť zabezpečené, že sa súkromné kľúče nikdy nedostali v nezašifrovanej forme mimo modul, kde sú uložené.
Nikto nesmie získať prístup k súkromnému podpisovému kľúču.
Pozri aj 5.1.

5.5 Opatrenia počítačovej bezpečnosti

Všetky počítačové komponenty TSU musia spĺňať požiadavky na spoľahlivé a bezpečné prevádzkovanie dôveryhodných služieb.

Moduly ÚPVS musia používať produkty na elektronický podpis s medzinárodnou certifikáciou (Common Criteria, ITSEC, NIST).

Musia byť implementované min. nasledovné bezpečnostné opatrenia systému:

- prístup ku komponentom systému na úrovni logickej bezpečnosti vyžaduje identifikáciu a autentifikáciu používateľov;
- diferenciácia prístupu ku komponentom systému ÚPVS na základe separácie rolí a rôznych funkcií obslužného personálu;
- využitie monitorovania a signalizačného zariadenia na včasnú detekciu, zaznamenanie a zastavenie pokusov o neautorizovaný prístup k prostrediu ÚPVS;
- ďalšie bezpečnostné opatrenia popísané v interných dokumentoch NASES.

5.6 Technické opatrenia životného cyklu

5.6.1 Opatrenia pre vývoj

Na zabezpečovanie kvalifikovaných dôveryhodných služieb používa NASES produkty s platnou certifikáciou NBÚ SR.

Pri vývoji špecializovaného programového vybavenia sa musia uplatniť NASES ustanovenia interných bezpečnostných smerníc, ktoré predpisujú zásady bezpečnosti vývoja programového vybavenia a riadenie bezpečnosti pri poskytovaní dôveryhodných služieb.

5.6.2 Opatrenia pre riadenie bezpečnosti

Musia sa vykonávať pravidelné kontroly a aktualizácie komponentov IS ÚPVS.

5.6.3 Bezpečnostné opatrenia životného cyklu

Neuplatňuje sa.

5.7 Sieťové bezpečnostné opatrenia

Moduly ÚPVS, zabezpečujúce funkcie poskytovania kvalifikovaných dôveryhodných služieb, musia byť oddelené od ďalších komponentov ÚPVS riadením sieťových pravidiel prístupu a nesmú byť priamo dostupné z verejnej siete Internet.

5.8 Časová pečiatka

V zmysle 4.5.5.

6 AUDIT ZHODY A INÉ POSUDZOVANIA

Na zaistenie stabilného dohľadu nad bezpečnosťou prevádzky ÚPVS sa musí vykonávať audit posúdenia zhody s požiadavkami Nariadenia eIDAS.

6.1 Frekvencia alebo okolnosti posudzovania

NASES ako TSP poskytujúci kvalifikované dôveryhodné služby uchovávania kvalifikovaných elektronických podpisov a uchovávania kvalifikovaných elektronických pečatí, sa musí, v súlade s nariadením eIDAS, podrobiť posudzovaniu zhody (auditu) aspoň jeden krát za 24 mesiacov.

Orgán dohľadu (NBÚ) môže kedykoľvek vykonať audit prevádzkovateľa - NASES alebo požiadať orgán posudzovania zhody, aby vykonal posúdenie zhody týkajúce sa prevádzkovateľa, a to na náklady NASES, s cieľom potvrdiť, že NASES a kvalifikované dôveryhodné služby, ktoré poskytuje, spĺňa požiadavky stanovené v Nariadení eIDAS.

6.2 Identita/kvalifikácie posudzovateľa

Požiadavky na orgán posudzovania zhody sú stanovené v nariadení eIDAS a v medzinárodnej norme ISO/IEC 17065:2012 a európskej norme ETSI EN 319 403.

6.3 Vzťah posudzovateľa voči posudzovanej entite

Osoba vykonávajúca audit NASES musí spĺňať kód správania sa audítora v zmysle Prílohy A ETSI EN 319 403 minimálne vo verzii 2.2.2.

6.4 Témy pokrývané posudzovaním

Účelom auditu je potvrdiť, že NASES ako kvalifikovaný poskytovateľ dôveryhodných služieb a kvalifikované dôveryhodné služby, ktoré poskytuje, spĺňajú požiadavky stanovené v Nariadení eIDAS.

6.5 Opatrenia na odstránenie nedostatkov

V prípade, že počas auditu zo stranu orgánu posudzovania zhody dôjde k zisteniu nedostatkov, k týmto musí NASES pripraviť a realizovať nápravné opatrenia na ich odstránenie a s týmito oboznámiť orgán posudzovania zhody.

6.6 Komunikácia výsledkov

Výsledky auditu interného, aj externého auditu bezpečnosti musia byť predkladané formou správy audítora o vykonaní bezpečnostného auditu.

Správa interného auditu podlieha pravidlám interných smerníc NASES.

Záverečná správa externého auditu musí obsahovať minimálne:

a) výrok audítora a zhodnotenie celkového stavu bezpečnosti TSP v čase výkonu auditu;

b) popis zistení o nedostatkoch bezpečnostného charakteru;

c) odporúčania na odstránenie zistených nedostatkov.

NASES musí predložiť výslednú správu o posúdení zhody orgánu dohľadu v lehote troch pracovných dní od jej doručenia.

7 OSTATNÉ USTANOVENIA A PRÁVNE USTANOVENIA

7.1 Poplatky

7.1.1 Poplatky za vydanie alebo obnovu certifikátu
Neuplatňuje sa.

7.1.2 Poplatky za prístup k certifikátu
Neuplatňuje sa.

7.1.3 Poplatky za prístup k informáciám o zrušení alebo stave certifikátu
Neuplatňuje sa.

7.1.4 Poplatky za ostatné služby
NASES poskytuje služby uchovávania KEP/KEPe bezodplatne.

7.1.5 Politika refundácie
Neuplatňuje sa.

7.2 Finančná zodpovednosť

7.2.1 Finančná zodpovednosť jednotlivých strán je určená platnými právnymi predpismi SR. NASES ako príspevková rozpočtová organizácia zabezpečuje povinné finančné krytie zdrojmi štátneho rozpočtu Poistenie
Pozri 7.2.

7.2.2 Iné aktíva
Bez ustanovení.

7.2.3 Poistenie alebo záručné krytie voči koncovým entitám
Neuplatňuje sa.

7.3 Dôvernosť obchodných informácií

7.3.1 Rozsah informácií považovaných za dôverné

Typy informácií, ktoré sú klasifikované ako utajované skutočnosti

- Počas prevádzky kvalifikovaných dôveryhodných služieb nevznikajú žiadne utajované skutočnosti v zmysle zákona č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

Typy informácií považovaných za citlivé

Citlivými informáciami TSP sú:

- všetky osobné údaje klientov podliehajúce ochrane v zmysle zákona č. 122/2013 o ochrane osobných údajov a o zmene a doplnení niektorých zákonov (ďalej len „zákon o ochrane osobných údajov“),
- výsledky posúdenia zhody (auditu).

7.3.2 Informácie nepovažované za dôverné

Za verejné informácie sa považujú informácie, ktoré je NASES povinná poskytovať ako TSP, prípadne ktoré publikuje pre zabezpečenie informovanosti verejnosti v súvislosti s prevádzkou ÚPVS. Verejne dostupné informácie musia byť zverejnené na webovom sídle NASES dostupnom na adrese https://www.nases.gov.sk .

7.3.3 Zodpovednosť za ochranu dôverných informácií

NASES, v prípade získania dôverných informácií alebo prístupu k nim, musí ich chrániť pred ich prezradením tretej strane.

NASES môže za určitých okolností poskytnúť určité dôverné informácie tretej strane, najmä v prípade:

- povinného poskytnutia informácii orgánu dohľadu,
- povinného poskytnutia informácii v trestnom konaní, občianskom súdnom konaní alebo správnom konaní,
- poskytnutia informácii na požiadanie dotknutej osoby.

7.4 Dôvernosť osobných údajov

7.4.1 Politika ochrany osobných údajov

NASES musí spracovávať osobné údaje v zmysle zákona č. 122/2013 Z.z. V primeranej lehote zabezpečí NASES zosúladenie spracúvania osobných údajov s požiadavkami Nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 (Nariadenie GDPR).

7.4.2 Informácie považované za osobné údaje

Viď. bod 7.4.1.

7.4.3 Informácie nepovažované za osobné údaje

Neuplatňuje sa

7.4.4 Zodpovednosť chrániť osobné údaje

Viď. bod 7.4.1.

7.4.5 Oznámenie o používaní osobných údajov súhlas so spracovaním osobných údajov

Viď. bod 7.4.1.

7.4.6 Poskytnutie získaných osobných údajov pre účely súdneho alebo správneho konania

Viď. bod 7.4.1.

7.4.7 Iné okolnosti sprístupnenia osobných údajov

Neuplatňuje sa.

7.5 Práva intelektuálneho vlastníctva

Prevádzkovateľ NASES zaručuje, že na všetok použitý softvér a hardvér má licenciu alebo je vo vlastníctve NASES. Autorské právo na Pravidlá na výkon certifikačných činností (CPS) a Certifikačnú politiku (CP) má NASES.

7.6 Zastupovanie a záruky

7.6.1 Zastupovanie a záruky CA

Zodpovednosť NASES za škodu je podľa nariadenia eIDAS a zákona o dôveryhodných službách nasledovná:

- NASES nie je zodpovedná za akékoľvek neoprávnené použitie ňou poskytovaných služieb klientmi a taktiež nenesie akékoľvek následky trestných činov, priestupkov alebo porušení zmluvy vyplývajúcich z tohto neoprávneného použitia.
- Za škodu spôsobenú porušením povinností zodpovedá NASES podľa všeobecne platných právnych predpisov SR a EÚ.
- NASES zodpovedá za ochranu osobných údajov klientov podľa platných právnych predpisov SR a EÚ (nariadenie GDPR a zákon o ochrane osobných údajov).
- Zodpovednosť NASES podľa odseku 7.6.2 nemožno vopred vylúčiť.

7.6.2 Zastupovanie a záruky RA

Viď relevantné časti bodu 7.6.1.

7.6.3 Zastupovanie a záruky držiteľa certifikátu

Neuplatňuje sa

7.6.4 Zastupovanie a záruky spoliehajúcich sa strán

Neuplatňuje sa

7.6.5 Zastupovanie a záruky ostatných strán

Neuplatňuje sa.

7.7 Zrieknutia sa záruk

NASES sa riadi najmä ustanoveniami nariadenia eIDAS a zákona o dôveryhodných službách a nemôže sa zrieknuť záruk vyplývajúcich z uvedených právnych úprav.

7.8 Obmedzenia záväzkov

NASES nezodpovedá sa škody spôsobené spoliehajúcim sa stranám v prípadoch, keď nedodržali ustanovenia týchto CPS a príslušnej CP.

NASES nezodpovedá za škodu, ktorá vznikla klientom dôveryhodných služieb, Spoliehajúcej sa strane príp. akýmkoľvek tretím stranám z dôvodu:

a) porušenia povinností klientom alebo Spoliehajúcou sa stranou uvedených v právnych predpisoch, zmluve alebo v politikách NASES;
b) neposkytnutia potrebnej súčinnosti zo strany klienta dôveryhodných služieb;
c) technickými vlastnosťami, konfiguráciou, nekompatibilitou, nevhodnosťou alebo inými vadami nimi použitých softvérových alebo hardvérových prostriedkov;
d) neposkytnutia niektorej z dôveryhodných služieb alebo jej nedostupnosti v priebehu plánovanej údržby alebo reorganizácie oznámenej na webovom sídle NASES alebo ÚPVS;
e) pôsobenia vyššej moci;

7.9 Zodpovednosť za škodu

Kto poruší svoju povinnosť alebo akýkoľvek záväzok, vyplývajúci z tejto CP, je povinný nahradiť škodu tým spôsobenú druhej strane, okrem prípadov kde je vylúčená zodpovednosť daného subjektu za škody. Za škodu sa považuje skutočná škoda, ušlý zisk a náklady vzniknuté poškodenej strane v súvislosti so škodovou udalosťou.

Kto poruší svoju povinnosť alebo akýkoľvek záväzok, vyplývajúci z tejto CP sa môže zbaviť zodpovednosti na náhradu škody, jedine ak preukáže, že k porušeniu povinnosti alebo akéhokoľvek záväzku, došlo v dôsledku okolností vylučujúcich zodpovednosť – vyššej moci.

7.10 Doba platnosti a ukončenie platnosti

7.10.1 Doba platnosti
Tato verzia CP platí odo dňa nadobudnutia jej platnosti, až do jej nahradenia novou verziou. Podrobnosti o histórii zmien týchto CP sú uvedené na začiatku dokumentu v časti „Denník zmien“.

7.10.2 Ukončenie platnosti
Platnosť tejto verzie CP skončí dňom publikovania novej verzie s vyšším číslom (podľa Denníka zmien)

7.10.3 Dôsledok ukončenia platnosti a pokračovanie záväzkov
V prípade, že tento dokument nebude nahradený novou verziou a v čase jeho platnosti dôjde k ukončeniu poskytovania kvalifikovaných dôveryhodných služieb zo strany NASES, musia byť dodržané všetky ustanovenia tejto CP, týkajúce sa poskytovania kvalifikovaných dôveryhodných služieb, ktoré je povinný NASES dodržať po ukončení svojej činnosti.

7.11 Individuálne oznámenia a komunikácia so zúčastnenými účastníkmi

Neuplatňuje sa.

7.12 Dodatky

7.12.1 Procedúra platná pre dodatky
Neuplatňuje sa.

7.12.2 Mechanizmus a doby oznamovania zmien
NASES zmeny oznamuje na svojom webovom sídle.

7.12.3 Okolnosti pre zmenu OID
OID sa riadi pravidlami uvedenými v kap. 1.2. v prípade zmeny formátu OID musí o zmenách informovať NASES dotknuté strany aspoň oznámením na svojom webovom sídle.

7.13 Opatrenia pre riešenie sporov

Klient má právo zaslať NASES sťažnosť, podnet alebo reklamáciu na poskytnutú kvalifikovanú dôveryhodnú službu. NASES vybaví reklamáciu najneskôr do 30 dní od jej prijatia, pokiaľ sa strany nedohodnú inak. Vybavenie reklamácie sa vzťahuje len k popisu vady uvedenej Klientom.

Súdy Slovenskej republiky majú výlučnú právomoc na rozhodovanie akýchkoľvek sporov medzi NASES a klientom.

7.14 Riadiace právo

Poskytovanie dôveryhodných služieb sa riadi platnými právnymi predpismi SR a EÚ.

7.15 Zhoda s právnymi predpismi

Všetky strany, na ktoré sa vzťahuje táto politika konajú v zhode s týmito platnými právnymi predpismi:

- Nariadenie eIDAS,
- Zákon o dôveryhodných službách.

7.16 Rôzne ustanovenia

7.16.1 Rámcová dohoda
Neuplatňuje sa.

7.16.2 Postúpenie práv
Klient nesmie svoje práva, povinnosti ako aj pohľadávky z tejto CP postúpiť alebo previesť (ani s nimi akokoľvek inak obchodovať) tretej osobe bez písomného súhlasu zo strany NASES.

7.16.3 Oddeliteľnosť ustanovení
Neuplatňuje sa.

7.16.4 Presadzovanie práva
Neuplatňuje sa.

7.16.5 Vyššia moc
NASES ani klienti nie sú zodpovední za omeškanie so splnením svojich záväzkov spôsobené okolnosťami vylučujúcimi zodpovednosť (vyššou mocou).

Okolnosťou vylučujúcou zodpovednosť je prekážka, ktorá nastala nezávisle na vôli povinnej strany a bráni jej v splnení jej povinnosti, ak je nemožné rozumne predpokladať, že by povinná strana túto prekážku alebo jej následky odvrátila alebo prekonala a ďalej, že by v čase vzniku prekážku predvídala, či mohla alebo mala predvídať.

Ak okolnosti vylučujúce zodpovednosť nastanú, potom je strana, u ktorej táto skutočnosť nastane, povinná bezodkladne informovať druhú stranu o povahe, začiatku a konci trvania takejto prekážky, ktorá bráni splneniu jej povinností. NASES a Klient sa zaväzujú vyvinúť maximálne úsilie na odvrátenie a prekonanie okolností vylučujúcich zodpovednosť.

Zodpovednosť však nie je vylúčená v prípade, keď takáto okolnosť vznikla až v čase, keď povinná strana bola v omeškaní s plnením svojej povinnosti, alebo ak predmetná strana nesplní svoju povinnosť bezodkladne informovať druhú stranu o povahe a začiatku trvania prekážky, alebo ak vznikla z jej hospodárskych pomerov. Účinky vylučujúce zodpovednosť sú obmedzené len na obdobie, kým trvá prekážka, s ktorou sú tieto účinky spojené.

7.17 Iné ustanovenia

Poskytovanie kvalifikovaných dôveryhodných služieb je s ohľadom na online formu prístupu k službe dostupné aj osobám so zdravotným postihnutím.

8 ODKAZY

[1] 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, v znení Nariadenia Európskeho parlamentu a Rady (EÚ) 2024/1183 z 11. apríla 2024. .

[2] NASES: Politika poskytovania dôveryhodných služieb

[3] NBÚ SR. Schéma dohľadu kvalifikovaných dôveryhodných služieb definovaná orgánom dohľadu. s.l. : NBÚ SR, 2019. 1.4. 05968/2019/ORD-001.

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

[5] NASES – Pravidlá poskytovania kvalifikovaných dôveryhodných služieb uchovávania kvalifikovaných elektronických podpisov a uchovávania kvalifikovaných elektronických pečatí

[6] ETSI TS 119 511 - Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques