NASES
NÁRODNÁ AGENTÚRA PRE SIEŤOVÉ A ELEKTRONICKÉ SLUŽBY

Národná agentúra pre sieťové a elektronické služby

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

Verzia dokumentu	2.2
Dátum vydania	03.12.2024
Názov dokumentu	Pravidlá 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
27.12.2017	1.0	Prvá verzia dokumentu	Ing. Dana Gáliková
11.11.2022	2.0	Revízia dokumentu: - Referencia CPS na ETSI TS 119 511 (kap. 1) - Identifikácia tretích strán (kap. 1.3.4) - Doplnenie frekvencie revízie CPS (kap. 1.5) - Spresnenie funkčnosti TSU a doplnenie odkazov na dostupnú dokumentáciu (kap. 1.3.1, 3, 3.1, 3.2, 3.3) - Doplnenie informácií o ukončení poskytovania služby (kap. 4.8) - Zosúladenie referenčných dokumentačných odkazov (kap. 9)	Ing. Marek Žáčik, Štefan Szilva
06.12.2023	2.1	Zmena adresy detašovaného pracoviska a webového sídla	Štefan Szilva
11.11.2024	2.2	Formálne úpravy	Štefan Szilva

Skontroloval:

Funkcia	Meno	Verzia	Dátum	Podpis
Riaditeľ SB NASES	Mgr. Peter Frolo	1.0	27.12.2017	
PMA	Štefan Szilva	2.0	24.11.2022	
PMA	Štefan Szilva	2.1	06.12.2023	
PMA	Štefan Szilva	2.2	11.11.2024	

Schválil:

Funkcia	Meno	Verzia	Dátum	Podpis
Generálny riaditeľ NASES		1.0		
PMA	Štefan Szilva	2.0	24.11.2022	
Generálny riaditeľ NASES		2.1	06.12.2023	
Generálny riaditeľ NASES	Ing. Ľubomír Mindek	2.2	12.11.2024	

OBSAH:

1 ÚVOD

Tento dokument (CPS) popisuje pravidlá, ktoré sa týkajú prevádzkovej praxe a postupov riadenia poskytovania kvalifikovaných dôveryhodných služieb uchovávania kvalifikovaných elektronických podpisov a uchovávania kvalifikovaných elektronických pečatí (ďalej aj „dôveryhodné služby“). Poskytovateľom týchto služieb 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 dôveryhodných služieb.
Pravidlá sú vypracované v zmysle požiadaviek uvedených v aktuálnej verzii dokumentu „Politika poskytovania kvalifikovaných dôveryhodných služieb uchovávania kvalifikovaných elektronických podpisov a uchovávania kvalifikovaných elektronických pečatí" [9] (ďalej len „CP LTA“) a v súlade so všeobecnými podmienkami poskytovania dôveryhodných služieb, ktoré NASES definoval v dokumente „Politika poskytovania dôveryhodných služieb“ [5] .
Poskytovanie kvalifikovaných dôveryhodných služieb sa riadi predovšetkým požiadavkami definovanými v normách ETSI EN 319 401 [4] a ETSI EN 119 511 [12] .
Niektoré časti CP LTA plne nahradzujú obsah niektorých kapitol, odsekov a bodov týchto CPS a v tom prípade nie sú v týchto CPS uvádzané žiadne nové ustanovenia, čo je vyznačené textom „Žiadne ustanovenia“ v predmetnej časti dokumentu.

1.1 Prehľad

Tieto pravidlá sa týkajú poskytovania kvalifikovaných dôveryhodných služieb:

- Služba uchovávania kvalifikovaných elektronických podpisov (ďalej aj „KEP“),
- Služba uchovávania kvalifikovaných elektronických pečatí (ďalej aj „KEPe“).

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 (ďalej len „Nariadenie eIDAS“) [1] , a v súlade s národnými ustanoveniami v zmysle Zákona č. 272/2016 Z. z. o dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zmene a doplnení niektorých zákonov (Zákon o dôveryhodných službách) [8] .

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

1.2 Názov dokumentu a jeho identifikácia

Tabuľka 1 Identifikácia dokumentu

Názov:	Pravidlá poskytovania kvalifikovaných dôveryhodných služieb uchovávania kvalifikovaných elektronických podpisov a uchovávania kvalifikovaných elektronických pečatí
Skratka názvu:	CPS LTA NASES
Verzia:	2.2
Schválené dňa:	11.11.2024
Platnosť od:	03.12.2024
Identifikátor objektu (OID):	1.3.158. 42156424.0.0.2.0.2

Tabuľka 2 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. 0.0.2.0.2	CPS LTA

1.3 ÚČASTNÍCI

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 14 721), 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 certifikovaných kvalifikovaných zariadení pre el. podpis a pečať.
Samotný princíp dlhodobej overiteľnosti KEP/KEPe je založený na vytváraní integritných elektronických podpisov (pečatí) pre zoznam digitálnych odtlačkov vytvorený z KEP/KEPe a 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 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.
Klienti sú v rámci modulov ÚPVS pridelení do samostatných systémových rolí.

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 Služby tretích strán

Prevádzku infraštruktúry ÚPVS a MDÚRZ zabezpečuje zmluvný partner, resp. konzorcium spoločností, na základe podpísanej Zmluvy o zabezpečení služieb a ich prevádzky. Podmienky a rozsah zmluvných činností sú publikované v rámci verejného repozitára zmlúv na webovom sídle https://crz.gov.sk. Pri výkone činností je zmluvný partner viazaný definovanými bezpečnostnými politikami a postupmi NASES, vrátane relevantných politík poskytovania kvalifikovaných dôveryhodných služieb. Dodávatelia sú zároveň držiteľmi platných certifikácií systému riadenia informačnej bezpečnosti v zmysle ISO/IEC 27001.

1.3.5 Iní účastníci

Autorita pre správu politík – PMA
Pozri ustanovenia CP [9] , kap. 1.3.4.

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 pravidiel

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 3 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 4 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 Osoba rozhodujúca o súlade CPS s politikami

Osobou, ktorá je zodpovedná za rozhodovanie o súlade CPS LTA s CP LTA je osoba menovaná do roly PMA. Frekvencia revízie CPS je minimálne raz za 2 roky.

1.5.4 Pravidlá schvaľovania CPS

- Poskytovateľ musí mať schválené CPS ešte pred začiatkom prevádzky dôveryhodnej služby.
- Obsah certifikačnej politiky schvaľuje generálny riaditeľ NASES na základe návrhu PMA.Poskytovateľ musí v CPS spĺňať všetky požiadavky schválenej CP.
- CPS sú určené najmä na interné použitie pre pracovníkov zaradených do dôveryhodných rolí NASES.

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

Pre pracovníkov NASES v dôveryhodných rolách sú CPS k dispozícii na vyhradenom úložisku v rámci interného IS NASES.
Pre klientov – OVM a spoliehajúce sa tretie strany sú CPS dostupné na základe osobitnej žiadosti klienta a verejne sa nepublikujú.

2.2 Zverejňovanie informácií o dôveryhodnej službe

NASES zverejňuje informácie súvisiace s poskytovaním kvalifikovaných dôveryhodných služieb na adresách uvedených v kapitole 1.5.1, v rámci Tabuľka 3.

2.3 Frekvencia zverejňovania informácií

CPS LTA sa sprístupňujú v internom IS NASES čo najskôr po ich schválení a vydaní. CPS LTA sa aktualizujú okamžite po každej zmene súvisiacej s poskytovaním dôveryhodných služieb, ako napr. pri zmene legislatívy, zmení pravidiel poskytovania služieb alebo zmene cenníka služieb.

2.4 Kontrola prístupu k repozitárom

Certifikačné informácie podľa bodu 2.3 týchto CPS zverejňuje prevádzkovateľ NASES bez obmedzenia.

Ďalšie certifikačné informácie nie sú verejnými informáciami a sú dostupné zamestnancom prevádzkovateľa NASES a tretím stranám na základe rozhodnutia PMA, vždy však v súlade s platným právnymi predpismi SR a EÚ.

3 SLUŽBY UCHOVÁVANIA KEP/KEPe

Potreba zabezpečenia autenticity obsahu a nepopierateľnosti pôvodcu správy v elektronickej komunikácii je hlavným dôvodom zavedenia elektronického podpisu, resp. elektronickej pečate. Praktické zavedenie kvalifikovaného elektronického podpisu/pečate v komunikácii občanov a podnikateľov s orgánmi verejnej správy na Slovensku a potreba dôveryhodne uchovávať históriu tejto komunikácie so sebou prináša nutnosť zabezpečiť dlhodobé uchovávanie elektronicky podpísaných dokumentov.

Modul dlhodobého uchovávania elektronických registratúrnych záznamov (MDURZ) 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 MDURZ je najmä:

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

Základné služby, ktoré bude MDUERZ poskytovať sú:

- príjem registratúrneho záznamu,
- príjem registratúrneho záznamu(ov) vo forme spisu (najmä pre uzavreté spisy),
- poskytnutie registratúrneho záznamu,
- poskytnutie registratúrneho záznamu(ov) vo forme spisu alebo konkrétneho registratúrneho záznamu zo spisu (najmä pre uzavreté spisy),
- služby elektronickej bádateľne pre pôvodcu registratúrneho záznamu alebo iné oprávnené subjekty (najmä pre uzavreté spisy, do budúcna je možné uvažovať aj o sprístupnení pre externé subjekty v zmysle aktuálne platnej legislatívy pre archív).

Ďalšie základné interné funkcie MDUERZ sú nasledovné:

- indexovanie obsahu, vytvorenie trvale čitateľného náhľadu pri prijatí záznamu do MDUERZ,
- vyhľadanie registratúrneho záznamu,
- vyradenie registratúrneho záznamu,
- overenie a obnovenie časovej pečiatky integritného podpisu,
- kontrola integrity.

Z dôvodu robustnosti systému modul MDUERZ môže plniť zároveň funkciu archivačného modulu pre ostatné moduly ÚPVS všade tam, kde je to potrebné (napríklad archivácia transakčných logov, vyradených formulárov, krízových notifikácií a podobne).

Dlhodobé uchovávanie znamená spoľahlivé uloženie obsahu nad rámec životnosti nosičov a HW (ochrana na bitovej úrovni) a účinnou ochranou v prípade katastrofických udalostí (zálohovanie, geograficky vzdialené úložiská, a pod.). Počas doby uloženia musí byť uložený záznam čitateľný so zrozumiteľným obsahom aj v prípade zmeny pôvodného formátu v ktorom bol pôvodne uložený. E-dokument podpísaný kvalifikovaným elektronickým podpisom alebo opatrený kvalifikovanou elektronickou pečaťou, musí mať zabezpečenú dlhodobú platnosť podpisu aj po vypršaní, alebo zrušení platnosti certifikátu podpisového kľúča, ktorým bol pôvodne podpísaný, alebo zmeny algoritmu použitého v KEP/KEPe.

Na ochranu podpisu podpisovateľa z dlhodobého hľadiska, aby bolo možné podpis overiť a považovať ho za platný aj v prípadoch, ak dôjde ku kompromitácii TSP alebo znemožneniu prístupu k informáciám o CRL, OCSP alebo, ak algoritmy použité na vytvorenie podpisu sa po

dlhšej dobe stanú menej bezpečnými, sa vyhotovuje integritný el. podpis (pečať). Integritný podpis zapečatí zoznam digitálnych odtlačkov vytvorený z uchovávaných KEP/KEPe a z údajov (CRL a certifikátov) potrebných pre ich overenie. Ten je vyhotovený prostredníctvom modulu CEP a jeho služby. Na vyhotovenie integritného podpisu sa využíva certifikát kvalifikovanej elektronickej pečate, ktorý vydal zmluvný TSP. Pred koncom platnosti integritného elektronického podpisu sa vykoná prevod tohto integritného podpisu na archívnu formu. V takýchto prípadoch bude možné podpis overiť a považovať za platný vďaka tomu, že archívny podpis zabezpečí dlhodobejšie dôveryhodné uzavretie obsahu všetkých potrebných informácií na overenie podpisu.

Prevod el. podpisu na archívnu formu je automatická funkcia slúžiaca na periodické obnovovanie el. pečatí integritných podpisov, ktoré umožňujú predlžovať dôveryhodnosť uchovávaných kvalifikovaných elektronických podpisov a pečatí používateľov.

Funkcionalita pravidelne kontroluje platnosť certifikátov vyhotovených integritných elektronických podpisov. Na tento účel MDUERZ eviduje všetky certifikáty časových pečiatok, ktoré boli použité počas jeho činnosti a sleduje dátumy konca platnosti časových pečiatok.

Táto funkcionalita vyžaduje spoluprácu s dôveryhodným poskytovateľom služieb ktorý vydáva časové pečiatky a prípadne s modulom CEP pre získavanie potrebných informácií na overenie KEP/KEPe a časovej pečiatky, resp. na vytvorenie archívneho formátu el. podpisov.

Predĺženie platnosti integritného podpisu sa zaznamená do evidencie MDUERZ.

Systém zaznamenáva činnosti tejto služby.

Činnosť tejto funkcionality je možné monitorovať a takisto je možné obmedziť, kedy sa táto služba nevykonáva (napr. aby nezaťažovala systém v úradných hodinách a pod.).
Súčasťou funkcie overenia a obnovenia časovej pečiatky je aj informovanie administrátorov systému pomocou notifikačného modulu pri významných chybových stavoch alebo ak služba je neplánovane nedostupná a pod.

Služby dlhodobého uchovávania KEP/KEPe sú v zmysle nariadenia eIDAS kvalifikovanými dôveryhodnými službami, ktoré môže prevádzkovať výlučne kvalifikovaný poskytovateľ dôveryhodných služieb (ďalej „TSP“).

Služby sú poskytované s obmedzeniami, ktoré sú definované v dokumente Dokumentácia technickej funkčnosti Modulu dlhodobého uchovávania a známych obmedzení [17] .

3.1 Popis riešenia

Služba je poskytovaná na základe nasledujúcich funkčných komponentov systému:

- Príjem záznamov (Ingest) – Záznamy sú získavané prostredníctvom aplikačného programového rozhrania systému alebo priamo z ÚPVS, z komponentu eDesk, slúžiaceho na vzájomnú komunikáciu používateľov ÚPVS (OVM, občania a podnikatelia) s elektronickou schránkou. V rámci nej majú OVM možnosť vybrať konkrétne dokumenty (napr. podania alebo rozhodnutia) pre ich uloženie do TSU.
- Poskytovanie záznamov (Access) – záznamy uložené v TSU si môžu klienti kedykoľvek vyžiadať, pokiaľ k nim majú oprávnenie (tzn. sú vlastníkmi dokumentu, ktorí rozhodli o ich uložení do TSU), alebo oprávnenie získajú od majiteľa dokumentu. Pre tento účel TSU poskytuje samostatný schvaľovací postup, ktorý je kompletne riešený v rámci rozhrania ÚPVS.
- Uchovávanie záznamov (Preservation) – Záznamy sú uchovávané v podobe samostatných elektronických dokumentov ošetrených integritným podpisom v zmysle požiadaviek nariadenia eIDAS a súvisiacej národnej legislatívy.
- Katalóg (Data Management) – kontrolu a riadenie prístupov zabezpečuje samostatný komponent pre správu dát, ktorý riadi najmä správu dát (životný cyklus dokumentu),

riadenie prístupových práv, vyhľadávanie a sprístupňovanie záznamov, obnovu el. podpisov/pečatí a vyraďovací mechanizmus záznamov.
- Archívne úložisko – úložisko dát je navrhnuté tak, aby poskytovalo dostatočnú záruku zabezpečenia dostupnosti, dôvernosti a integrity uchovávaných záznamov.
- Administrácia systému – v rámci systému sú stanovené samostatné roly min. pre úroveň používateľov, administrátorov a audítorov systému.
- Plánovanie uchovávania – systém uchovávania je riadený tak, aby bolo pre každý záznam zrejmé, na akú dobu je uchovaný a s akými pravidlami. Používatelia sú notifikovaní o blížiacom sa konci uchovávania záznamov s možnosťou rozhodnúť o ich vyradení, alebo predĺžení uchovávania v rámci MDURZ.

3.2 Archivované údaje

TSU predlžuje dôveryhodnosť KEP / KEPe aj po uplynutí ich technologickej platnosti len v prípade, ak spĺňajú požiadavky na správny formát podpisu. Komponent implementuje vytváranie a obnovovanie integritných podpisov - kvalifikovaných elektronických pečatí (hromadné archívne podpisy vo formáte ASiC-XAdES založené na koncepte podpísania zoznamu digitálnych odtlačkov chránených súborov uvedených v štruktúre XML; viď [2] , [3]), ktoré zabezpečujú predlžovanie dôveryhodnosti uchovávaných podpisov a pečatí. Komponent implementuje predlžovanie dôveryhodnosti KEP a KEPe vo formátoch podporovaných modulom Centrálnej elektronickej podateľne (ďalej „CEP“), prevádzkovanej v rámci internej infraštruktúry ÚPVS. Podporované formáty KEP a KEPe sú uvedené v kapitole 5.1 dokumentu [18] „Dokumentácia funkčnosti Centrálnej elektronickej podateľne“ dostupného na adrese:
https://www.slovensko.sk/_img/CMS4/Dokumentacia_funkcnosti_CEP.pdf

Integritný elektronický podpis zároveň zabezpečí aj kontrolu integrity obsahu. Aplikuje sa na podpísaný aj nepodpísaný obsah. V prípade podpísaných dokumentov integritný podpis sa aplikuje aj na údaje potrebné pre overenie kvalifikovaného elektronického podpisu alebo pečate. Služba je poskytovaná s obmedzeniami, ktoré sú definované v dokumente Dokumentácia technickej funkčnosti Modulu dlhodobého uchovávania a známych obmedzení [17] .

3.3 Prístup k dôveryhodným službám

Pre prístup k dôveryhodným službám je potrebná zriadená elektronická schránka v rámci modulu eDesk na ÚVPS a pridelenie do jednej z rolí:
- R_MDURZ_READER,
- M_MDURZ_WRITER.

Tieto role má automaticky pridelené:
- Štatutár (PO, OVM),
- Majiteľ schránky (FO, živnostník),
- Osoba, ktorej je udelené oprávnenie na disponovanie so schránkou (napríklad zo strany štatutára).

Prístup do používateľského prostredia modulu MDURZ je možný prostredníctvom portálu:
https://www.slovensko.sk/sk/centralne-ulozisko-zaznamov

Službu je možné používať aj prostredníctvom aplikačných programových rozhraní (API) po schválení integračného zámeru zo strany NASES a úspešnej integrácii systému.

Pravidlá pre používateľov sú všetkým autorizovaným subjektom sprístupnené súčasne so zabezpečením prístupu k službe, dokumentáciou, ktorá je zverejnená priamo na ÚPVS:

Všeobecné podmienky:
- https://www.slovensko.sk/_img/CMS4/vseobecne_podmienky_UPVS.pdf

Príručky / dokumentácia pre používateľov:

- https://www.slovensko.sk/_img/CMS4/Navody/navod_MDU.pdf
- https://www.slovensko.sk/_img/CMS4/Navody/navod_mdu_ovm.pdf

Dokumentácia funkčnosti MDU a známych obmedzení:

- https://www.slovensko.sk/_img/CMS4/OPortali/Dokumentacia_funkcnosti_MDU.pdf

3.3.1 Dostupné činnosti používateľov v rámci TSU

Používateľom sú dostupné nasledovné typy operácií:

- Jednoduché vyhľadávanie záznamov
- Rozšírené vyhľadávanie záznamov
- Zobrazenie vlastností záznamu
- Zobrazenie zoznamu oprávnení pre prístup k vlastným záznamom
- Vloženie nového záznamu
- Požiadavka na poskytnutie záznamu
- Požiadavka na poskytnutie vybraného dokumentu zo záznamu
- Zmena popisných údajov záznamu
- Žiadosť o prístup k záznamu
- Schválenie žiadosti o prístup k záznamu
- Predĺženie doby uchovávania záznamu
- Požiadavka na ukončenie uchovávania záznamu

4 FYZICKÉ, PROCEDURÁLNE A PERSONÁLNE BEZPEČNOSTNÉ OPATRENIA

4.1 Opatrenia fyzickej bezpečnosti

Proces FOB je ustanovený v dokumente Bezpečnostná politika NASES [10] . Pre fyzickú a objektovú bezpečnosť platia ustanovenia uvedené v dokumente Smernica o režimových opatreniach NASES [11] 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 sú umiestnené v bezpečných priestoroch chránených pred neautorizovaným prístupom nepovolaných osôb, pred živelnými pohromami a haváriami v inžinierskych sieťach.

4.1.2 Fyzický prístup

Bezpečnostné opatrenia na fyzickú a objektovú bezpečnosť sú stanovené pre každú lokalitu, v rámci ktorej sú prevádzkované komponenty tech. infraštruktúry. Prístup do priestorov umiestnenia infraštruktúry poskytujúcej dôveryhodné služby je riadený. NASES má pripravené spôsoby a postupy na ochranu svojich počítačových systémov, údajov a archívov proti neoprávnenej manipulácii, krádeži a prezradeniu.

4.1.3 Napájanie a vzduchotechnika

Komponenty systému sú chránené viacerými zdrojmi elektrického napájania. Priestory, v ktorých sa nachádza infraštruktúra poskytujúca dôveryhodné služby, sú vybavené klimatizáciou.

4.1.4 Možné vystavenia vode

Priestory sú chránené proti nebezpečenstvu pôsobenia vody.

4.1.5 Predchádzanie požiarom a ochrana pred požiarmi

Priestory sú chránené dymovými a požiarnymi detektormi.

4.1.6 Uchovávanie médií

NASES uskladňuje všetky médiá, ako sú pásky a dokumenty, v bezpečnom prostredí.

Médiá sú uchovávané tak, aby boli chránené pred poškodením (voda, oheň, elektromagnetické poškodenie). Médiá obsahujúce záznamy pre audit, archívne alebo zálohované informácie sú 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, sú likvidované v zmysle postupov, stanovených záväznými vnútornými predpismi NASES, kde je uvedená klasifikačná schéma citlivosti informácií.

4.1.8 Záložné prevádzkové priestory

Okrem prevádzkových priestorov umiestnenia disponuje NASES záložnými prevádzkovými priestormi určenými na ukladanie pravidelných záložných kópií a archívnych dát.

4.2 Procedurálne opatrenia

4.2.1 Dôveryhodné roly

Bezpečnostné role a zodpovednosti (špecifikované v politike informačnej bezpečnosti Poskytovateľa) sú zdokumentované v popise práce alebo v dokumentoch dostupných všetkým zainteresovaným zamestnancom. Dôveryhodné role, na ktorých závisí bezpečnosť prevádzky Poskytovateľa sú jasne identifikované. Tieto role sú menované a akceptované manažmentom Poskytovateľa a osobou, ktorá v danej roli pracuje.

Činnosti, vykonávané v rámci modulov NASES, sú popísané formou prevádzkových postupov a smerníc. Prevádzkové procedúry sú špecifikáciou základných činností pri obsluhe komponentov NASES a infraštruktúry ÚPVS. Špecifikácia prevádzkovej procedúry obsahuje popis činností pri obsluhe, pravidlá na bezpečnú realizáciu činností a identifikáciu roly pracovníka, ktorý smie dané činnosti vykonávať.

Spôsob a bezpečnosť vykonávania procedúr je pravidelne kontrolovaná.

Na zabezpečenie činností boli pre jednotlivých pracovníkov prevádzky definované roly. Definícia roly pokrýva: 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.

Pre prevádzkovanie NASES sú definované nasledujúce základné roly:

1) PMA
2) bezpečnostný správca NASES,
3) systémový administrátor modulu MDURZ,
4) audítor.

PMA

Hlavnou úlohou PMA je predovšetkým dohľad nad tvorbou politík a pravidiel súvisiacich s poskytovaním dôveryhodných služieb a rozhodovanie v prípade sporných udalostí, ktoré môžu pri poskytovaní dôveryhodných služieb nastať.

Bezpečnostný správca NASES

Hlavnou úlohou bezpečnostného správcu je prideľovanie rolí a prístupových práv v systémoch NASES, odsúhlasovanie zmien v konfigurácii komponentov ÚPVS, atď.

Administrátor modulu MDURZ

Táto rola má zodpovednosť primárne za prevádzku a správu Modulu dlhodobého uchovávania registratúrnych záznamov, najmä z pohľadu nastavenia aplikácie, overenia funkčnosti systému, spúšťania / zastavovania komponentov systému, profylaktiku systému, incident manažmentu a pod.

Audítor

Audítori predstavujú nezávislý spôsob kontrolovania prevádzky ÚPVS. Rola audítora nie je zlučiteľná s rolami, ktoré sa podieľajú na správe a obsluhe komponentov. t.j. administrátori a operátori.

4.2.2 Počet pracovníkov vyžadovaných na vykonávanie činností

V zmysle organizačného poriadku NASES.

4.2.3 Identifikácia a autentizácia pre každú rolu

Každá rola sa identifikuje a autentizuje bezpečným prostriedkom.

4.2.4 Nezlučiteľnosť rolí

V zmysle organizačného poriadku NASES.

4.3 Personálne opatrenia

Každý pracovník je 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 sú 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

V zmysle smernice pre personálnu bezpečnosť.

4.3.3 Požiadavky na školenia personálu

Osoby zabezpečujúce činnosti v prevádzke ÚPVS a TSU sú 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

V zmysle smernice pre personálnu bezpečnosť.

4.3.5 Frekvencia a postupnosť rotácie rolí

V zmysle smernice pre personálnu bezpečnosť.

4.3.6 Sankcie za neoprávnené činnosti

Udeľovanie sankcií za neoprávnené činnosti s a riadi politikou pre IB 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, má 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 je poskytnutá pracovníkom vykonávajúcim túto rolu dokumentácia v potrebnom rozsahu.

Pracovníci obsluhy NASES sú povinní používať dokumenty, ktoré obdržali, len na účely, na ktoré sú určené. Každý pracovníci je oboznámený s bezpečnostnou politikou NASES.

4.4 Procedúry spojené s auditnými záznamami

Poskytovateľ zaznamenáva a v primeranej dobe udržuje 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 sú 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 zaznamenávajú tieto typy udalostí (záznamov) súvisiacich so základnými funkciami TSU:

a) vloženie záznamu (ingescia).
b) poskytnutie záznamu (diseminácia).
c) kontrola záznamu.
d) vyradenie záznamu.
e) predĺženie doby uloženia záznamu.
f) obnova elektronického integritného podpisu.

Okrem toho sa archivujú kompletné záznamy o aktivitách ďalších modulov ÚPVS súvisiacich s poskytovaním služby. Typy udalostí, ktoré sa zaznamenávajú, sú popísané v rámci dokumentácie k jednotlivým modulom ÚPVS.

4.4.2 Frekvencia spracovania záznamov

Záznamy sa spracovávajú v pravidelných denných intervaloch. Na vyhodnocovanie prevádzkových záznamov ÚPVS je 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 a ostatných súvisiacich logov sa uchovávajú ako aktívne záznamy po dobu 14 dní od ich vzniku. Po uplynutí definovanej doby aktívneho života sú záznamy preradené do archívu.

4.4.4 Ochrana auditných záznamov

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

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

4.4.5 Procedúry zálohovania auditných záznamov

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

4.4.6 Systém zberu auditných záznamov

Systém zberu elektronických prevádzkových záznamov je kombináciou automatických činností vykonávaných operačnými systémami a aplikáciami komponentov ÚPVS a manuálnych činností vykonávaných personálom prevádzky.

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

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

4.4.7 Notifikácia subjektu, ktorý spôsobil udalosť

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

4.4.8 Posudzovania zraniteľností

Poskytovateľ vykonáva posúdenie rizík s cieľom identifikovať, analyzovať a vyhodnotiť riziká súvisiace s poskytovaním dôveryhodných služieb.
Poskytovateľ vyberá 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 sú zdokumentované v bezpečnostnej politike NASES a v pravidlách na výkon dôveryhodných služieb.
Manažment NASES schvaľuje posúdenie rizík a akceptuje zvyškové riziká.

4.5 Archivácia záznamov

NASES vypracoval samostatné pravidlá pre zálohovanie a archiváciu modulu MDURZ, vrátane komplexných postupov zálohovania databáz, úložiska obsahu, ako aj konfiguračné a aplikačné zálohy.

Prevádzkové záznamy a dokumenty sú 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 je opatrený časovým údajom o dátume jeho vytvorenia.

4.5.2 Doba archivácie

Doba uchovávania archivovaných údajov je 30 rokov.

Po vymazaní záznamu ostávajú uchovávané informácie o zázname ako názov a vlastník, ale samotný záznam a súvisiace KEP/KEPe sa neuchovávajú.

Modul CEP zabezpečujúci kryptografické operácie archivuje informácie o svojej činnosti v zmysle pravidiel stanovených pre modul.

4.5.3 Ochrana archívu

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

4.5.4 Procedúry zálohovania archívu

Procedúry zálohovania archívu sú navrhnuté tak, aby zaisťovali kompletné obnovenie služieb. Podrobnosti sú špecifikované v pláne zabezpečenia kontinutiy činností NASES.

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 postavený na internom riešení modulu MDURZ. Pozri aj kap. 3.

4.5.7 Procedúry na získanie a overenie archívnych informácií

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

4.6 Zmena kľúčov

Neuplatňuje sa – pozri kap. 5.1.

4.7 Kompromitácia a havarijný plán

4.7.1 Procedúry pre riešenie incidentov

Na zabezpečenie integrity služieb ÚPVS implementuje NASES postupy zálohovania údajov a ich obnovy. NASES má 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 má 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.

4.7.4 Schopnosť business kontinuity po havárii

Ako 4.7.2

4.8 Ukončenie poskytovania služeb

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 pre kvalifikovanú dôveryhodnú službu uchovávania.
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

Žiadne ustanovenia oproti CP.

5.1 Generovanie kľúčového páru a inštalácia

Žiadne ustanovenia oproti CP.

5.1.1 Generovanie kľúčového páru

Žiadne ustanovenia oproti CP.

5.1.2 Doručenie súkromného kľúča žiadateľovi

Žiadne ustanovenia oproti CP.

5.1.3 Doručenie verejného kľúča vydavateľovi certifikátu

Žiadne ustanovenia oproti CP.

5.1.4 Doručenie verejného kľúča CA spoliehajúcim sa stranám

Žiadne ustanovenia oproti CP.

5.1.5 Dĺžky kľúčov

Žiadne ustanovenia oproti CP.

5.1.6 Parametre generovania verejného kľúča a kontrola kvality

Žiadne ustanovenia oproti CP.

5.1.7 Účely použitia kľúča

Žiadne ustanovenia oproti CP.

5.2 Ochrana súkromného kľúča a opatrenia inžinierstva kryptografického modulu

5.2.1 Štandardy a opatrenia pre kryptografický modul

Súkromný kľúč NASES je uložený na špeciálnych hardvérových zariadeniach (ďalej „kryptografický modul“). Kryptografické moduly použité v NASES sú odolné voči nedovolenej manipulácii a chránené pred neautorizovaným prístupom (aj fyzickým). Sú certifikované podľa medzinárodného štandardu FIPS 140-2 na úroveň (level) 3.

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.

5.2.3 Obnova súkromného kľúča

Neuplatňuje sa.

5.2.4 Zálohovanie súkromného kľúča

Súkromné kľúče sú zálohované v zašifrovanej forme, na ich obnovu je nutná súčasná autorizácia dvoch určených pracovníkov. Po ukončení platnosti certifikátu NASES, ktorý je zviazaný s verejným kľúčom prislúchajúcim k zálohovanému súkromnému kľúču, bude záloha súkromného kľúča zničená.

5.2.5 Archivácia súkromného kľúča

Neuplatňuje 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 a pod dohľadom oprávneného administrátora.

5.2.7 Uloženie súkromného kľúča v kryptografickom module

Súkromný kľúč sa generuje priamo prostriedkami kryptografického modulu. Na vygenerovanie súkromného kľúča je potrebná súčasná autorizácia dvoch určených pracovníkov. Súkromný kľúč je uložený na kryptografickom module v zašifrovanom tvare. Funkčné, technické a bezpečnostné vlastnosti kryptografického modulu, na ktorom je uložený súkromný kľúč, spĺňajú požiadavky nariadenia eIDAS a zákona o dôveryhodných službách.

5.2.8 Metóda aktivácie súkromného kľúča

Kľúče sú uložené v HSM module, ktorého aktivácia je podmienená autorizáciou min. 2 pracovníkov.

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.

5.2.10 Metóda zničenia súkromného kľúča

Využitím funkcionality HSM modulu.

5.2.11 Hodnotenie kryptografického modulu

Kryptografické moduly v správe NASES spĺňajú požiadavky medzinárodného štandardu FIPS 140-2 úroveň 3. Bezpečnosť kryptografických modulov je pravidelne monitorovaná a testovaná. Všetky činnosti súvisiace s prevádzkou kryptografických modulov sú zaznamenávané a vyhodnocované.

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 je zhodná s prevádzkovou dobou platnosti príslušných vydaných certifikátov. Dobu používania stanovuje TSP, ktorý vydáva certifikát. Minimálna požadovaná doba je 3 roky.

5.4 Aktivačné údaje

5.4.1 Generovanie a inštalácia aktivačných údajov

Pozri 5.1.

5.4.2 Ochrana aktivačných údajov

Aktivačné údaje sa neukladajú v nešifrovanej forme a nie sú dostupné nikomu s výnimkou oprávnených pracovníkov NASES.

5.4.3 Ostatné aspekty aktivačných údajov

Je zabezpečené, že sa súkromné kľúče nikdy nedostanú v nezašifrovanej forme mimo modul, kde sú uložené.
Nikto nemá mať prístup k súkromnému podpisovému kľúču.

5.5 Opatrenia počítačovej bezpečnosti

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

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

Základné 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 uplatňuje 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

Vykonávajú sa 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, sú oddelené od ďalších komponentov ÚPVS riadením sieťových pravidiel prístupu a nie sú priamo dostupné z verejnej siete Internet.

5.8 Časová pečiatka

V zmysle 4.5.5.

6 PROFILY CERTIFIKÁTOV, ZOZNAMOV CRL A OCSP

Profily definuje TSP, ktorý vydáva certifikát pre NASES.

7 AUDIT ZHODY A INÉ POSUDZOVANIA

Na zaistenie stabilného dohľadu nad bezpečnosťou prevádzky ÚPVS sa vykonáva bezpečnostný audit.

7.1 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.

7.2 Identita/kvalifikácie posudzovateľa

Požiadavky na orgán posudzovania zhody sú stanovené v nariadení eIDAS [1] a v medzinárodnej norme ISO/IEC 17065:2012 [19] a európskej norme ETSI EN 319 403 [20] .

7.3 Vzťah posudzovateľa voči posudzovanej entite

Osoba vykonávajúca audit NASES musí spĺňať kód správania sa audítora v zmysle Prílohy A ETSI EN 319 403 [20] minimálne vo verzii 2.2.2.

7.4 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.

7.5 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.

7.6 Komunikácia výsledkov

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

Správa interného auditu podlieha pravidlám interných smerníc NASES.

Záverečná správa externého auditu pozostáva z:

a) výroku audítora a zhodnotenia celkového stavu bezpečnosti TSP v čase výkonu bezpečnostného auditu;

b) popisu zistení o nedostatkoch bezpečnostného charakteru;

c) odporúčaní na odstránenie zistených nedostatkov.

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

8 OSTATNÉ USTANOVENIA A PRÁVNE USTANOVENIA

8.1 Poplatky

8.1.1 Poplatky za vydanie alebo obnovu certifikátu

Neuplatňuje sa.

8.1.2 Poplatky za prístup k certifikátu

Neuplatňuje sa.

8.1.3 Poplatky za prístup k informáciám o zrušení alebo stave certifikátu

Neuplatňuje sa.

8.1.4 Poplatky za ostatné služby

NASES poskytuje služby uchovávania KEP/KEPe bezodplatne.

8.1.5 Politika refundácie

Neuplatňuje sa.

8.2 Finančná zodpovednosť

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

8.2.1 Poistné krytie

Poistenie prevádzkovateľa je určené platnými právnymi predpismi SR.

8.2.2 Iné aktíva

Neuplatňuje sa.

8.2.3 Poistenie alebo záručné krytie voči koncovým entitám

Neuplatňuje sa.

8.3 Dôvernosť obchodných informácií

8.3.1 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 [6] .

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“) [7] ,
- výsledky posúdenia zhody (auditu).

8.3.2 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 sú zverejnené na webovom sídle NASES dostupnom na adrese https://www.nases.gov.sk.

8.3.3 Zodpovednosť za ochranu dôverných informácií

NASES, v prípade získania dôverných informácií alebo prístupu k nim, tieto chráni 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.

8.4 Dôvernosť osobných údajov

8.4.1 Politika ochrany osobných údajov

NASES spracováva osobné údaje v zmysle zákona č. 122/2013 Z.z.[7]

8.4.2 Informácie považované za osobné údaje

Viď. bod 8.4.1.

8.4.3 Informácie nepovažované za osobné údaje

Neuplatňuje sa

8.4.4 Zodpovednosť chrániť osobné údaje

Viď. bod 8.4.1.

8.4.5 Oznámenie o používaní osobných údajov súhlas so spracovaním osobných údajov

Viď. bod 8.4.1.

8.4.6 Poskytnutie získaných osobných údajov pre účely súdneho alebo správneho konania

Viď. bod 8.4.1.

8.4.7 Iné okolnosti sprístupnenia osobných údajov

Neuplatňuje sa.

8.5 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 Certifikačný poriadok (CP) má NASES.

8.6 Zastupovanie a záruky

8.6.1 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 2 nemožno vopred vylúčiť.

8.6.2 Zastupovanie a záruky RA

Viď relevantné časti bodu 8.6.1 týchto CPS.

8.6.3 Zastupovanie a záruky držiteľa certifikátu

Neuplatňuje sa

8.6.4 Zastupovanie a záruky spoliehajúcich sa strán

Neuplatňuje sa

8.6.5 Zastupovanie a záruky ostatných strán

Neuplatňuje sa.

8.7 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.

8.8 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;

8.9 Zodpovednosť za škodu

Kto poruší svoju povinnosť alebo akýkoľvek záväzok, vyplývajúci z týchto CPS, resp. odpovedajúcej 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 týchto CPS resp. odpovedajúcej 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.

8.10 Doba platnosti a ukončenie platnosti CPS

8.10.1 Doba platnosti CPS

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

8.10.2 Ukončenie platnosti CPS

Platnosť tejto verzie CPS skončí dňom publikovania novej verzie s vyšším číslom (podľa Denníka zmien)

8.10.3 Dôsledok ukončenia platnosti CPS 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 týchto CPS týkajúce sa poskytovania kvalifikovaných dôveryhodných služieb, ktoré je povinný NASES dodržať po ukončení svojej činnosti.

8.11 Individuálne oznámenia a komunikácia so zúčastnenými účastníkmi

Neuplatňuje sa.

8.12 Dodatky

8.12.1 Procedúra platná pre dodatky

Neuplatňuje sa.

8.12.2 Mechanizmus a doby oznamovania zmien

NASES zmeny oznamuje na svojom webovom sídle.

8.12.3 Okolnosti pre zmenu OID

OID sa riadi pravidlami uvedenými v kap. 1.2. v prípade zmeny formátu OID bude o zmenách informovať NASES dotknuté strany v zmysle 8.12.2.

8.13 Opatrenia pre riešenie sporov

Spory ktoré sa týkajú používania kvalifikovaných dôveryhodných služieb, sa riešia v zmysle platných zákonov a ostatných všeobecne záväzných predpisov SR.

Pokiaľ vznikne spor v súvislosti s týmto CPS, strany sa zaväzujú v dobrej viere vynaložiť maximálne úsilie ukončiť spor dohodou alebo s pomocou tretej strany.

Ak strany nie sú schopné riešiť spor v primeranom čase, potom sa strany spoločne dohodnú na nezávislom rozhodcovi s primeranou kvalifikáciou a praktickými skúsenosťami s riešením sporov a dohodnú sa na záväznosti výroku rozhodcu.

Spory s cudzími TSP, ktoré nie sú slovenskými právnymi subjektmi, ale boli uznané NBÚ, týkajúce sa otázok poskytovania dôveryhodných služieb a zodpovednosti za škody spôsobené

pri poskytovaní dôveryhodných služieb a ostatných problémov spojených s poskytovaním dôveryhodných služieb, sa riešia v zmysle platných právnych predpisov SR, pričom miestom konania sporu je SR.

Pri riešení sporov sa postupuje na základe všeobecne záväzných právnych predpisov, platných v SR.

V prípade, že ktorékoľvek ustanovenie (jedno alebo viac) tohto CPS je z nejakých dôvodov uznané za neplatné, nezákonné alebo právne nevynútiteľné, toto nemá vplyv na ostatné ustanovenia. CPS sa v takomto prípade vykladá tak, ako keby neplatné ustanovenia vôbec neobsahoval, a aktualizácia CPS sa vykoná v súlade s ustanoveniami kapitoly 8 tohto dokumentu.

Ak sa tieto CPS preložia do iného jazyka ako do slovenského, bude slovenská verzia rozhodujúca.

8.14 Riadiace právo

Interpretácia a vynucovanie týchto CPS sa riadia platnými právnymi predpismi SR a EÚ.

8.15 Zhoda s právnymi predpismi

Všetky strany, na ktoré sa vzťahujú tieto CPS konajú v zhode s týmito platnými právnymi predpismi:

- nariadenie eIDAS,
- zákon o dôveryhodných službách.

8.16 Rôzne ustanovenia

8.16.1 Rámcová dohoda

Neuplatňuje sa.

8.16.2 Postúpenie práv

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

8.16.3 Oddeliteľnosť ustanovení

Neuplatňuje sa.

8.16.4 Presadzovanie práva

Neuplatňuje sa.

8.16.5 Vyššia moc

Podľa bodu 7.16.5 CP LTA.

8.17 Ostatné ustanovenia (Other provisions)

Nie sú.

9 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 .

[2] Electronic Signatures and Infrastructures (ESI); ASiC Baseline Profile. [Online] http://www.etsi.org/deliver/etsi_ts/103100_103199/103174/02.02.01_60/ts_103174v020201p.pdf. ETSI TS 103174 v.2.2.1.

[3] Electronic Signatures and Infrastructures (ESI); XAdES Baseline Profile. [Online] http://www.etsi.org/deliver/etsi_ts/103100_103199/103171/02.01.01_60/ts_103171v020101p.pdf. ETSI TS 103 171 V2.1.1.

[4] Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers. ETSI EN 319 401.
[5] NASES: Politika poskytovania dôveryhodných služieb, ver. 1.0
[6] Zákon č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
[7] Zákon č. 122/2013 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov
[8] Zákon č. 272/2016 o dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zmene a doplnení niektorých zákonov (zákon o dôveryhodných službách)
[9] NASES: Politika poskytovania kvalifikovaných dôveryhodných služieb uchovávania kvalifikovaných elektronických podpisov a uchovávania kvalifikovaných elektronických pečatí
[10] Bezpečnostná politika NASES
[11] NASES: Smernica o režimových opatreniach NASES
[12] 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
[13] Všeobecné podmienky poskytovania služieb prostredníctvom Ústredného portálu verejnej správy (dostupné online: https://www.slovensko.sk/_img/CMS4/vseobecne_podmienky_UPVS.pdf)
[14] Všeobecné podmienky prevádzky Ústredného portálu verejnej správy – spojené s Všeobecnými podmienkami poskytovania služieb prostredníctvom ÚPVS (dostupné online: https://www.slovensko.sk/_img/CMS4/vseobecne_podmienky_UPVS.pdf)
[15] Návod na používanie modulu dlhodobého uchovávania (MDU) (dostupné online: https://www.slovensko.sk/_img/CMS4/Navody/navod_MDU.pdf)
[16] Návod na používanie MDU pre OVM (dostupné online: https://www.slovensko.sk/_img/CMS4/Navody/navod_mdu_ovm.pdf)
[17] Dokumentácia technickej funkčnosti Modulu dlhodobého uchovávania a známych obmedzení (dostupné online: https://www.slovensko.sk/_img/CMS4/OPortali/Dokumentacia_funkcnosti_MDU.pdf)
[18] Dokumentácia funkčnosti Centrálnej elektronickej podateľne (dostupné online: https://www.slovensko.sk/_img/CMS4/Dokumentacia_funkcnosti_CEP.pdf)
[19] STN EN ISO/IEC 17065 Posudzovanie zhody. Požiadavky na orgány vykonávajúce certifikáciu výrobkov, procesov a služieb (ISO/IEC 17065: 2012)
[20] ETSI EN 319 403-1 Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 1: Requirements for conformity assessment bodies assessing Trust Service Providers