Národná agentúra pre sieťové a elektronické služby

Pravidlá poskytovania kvalifikovanej dôveryhodnej služby správy zariadení na vyhotovovanie kvalifikovaných elektronických pečatí na diaľku

(Service practice statement)

Verzia dokumentu	1.1
Dátum vydania	13.05.2026
Názov dokumentu	Pravidlá poskytovania služby správy zariadení na vyhotovovanie kvalifikovaných elektronických pečatí na diaľku (SPS)
Gestor	PMA
Vlastník	NASES

Denník zmien:

Dátum	Verzia	Predmet	Spracoval
20.03.2026	1.0	Prvá verzia dokumentu	Štefan Szilva
01.04.2026	1.1	Aktualizácia dokumentu	Štefan Szilva

Skontroloval:

Funkcia	Meno	Verzia	Dátum	Podpis

Schválil:

Funkcia	Meno	Verzia	Dátum	Podpis
Generálna riaditeľka NASES	Mgr. Jana Molnarová	1.1	29.04.2026	

NÁRODNÁ AGENTÚRA PRE SIEŤOVÉ A ELEKTRONICKÉ SLUŽBY

Obsah

1 Úvod

Tento dokument (SPS) popisuje pravidlá, ktoré sa týkajú prevádzkovej praxe a postupov riadenia poskytovania kvalifikovanej dôveryhodnej služby správy zariadení na vyhotovovanie kvalifikovanej elektronickej pečate na diaľku v súlade s článkom 39a 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 (EÚ) č. 2024/1183 a neskorších predpisov (ďalej len „Nariadenie eIDAS“) 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).

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“), v rámci Ústredného portálu verejnej správy (ďalej aj „ÚPVS“).

Pravidlá sú vypracované v zmysle prevádzkových požiadaviek uvedených v aktuálnej verzii dokumentu „Politika poskytovania dôveryhodných služieb " (ďalej len „CP TSP“).

1.1 Názov dokumentu a jeho identifikácia

Tabuľka 1 Identifikácia dokumentu

Názov:	Pravidlá poskytovania kvalifikovanej dôveryhodnej služby správy zariadení na vyhotovovanie kvalifikovaných elektronických pečatí na diaľku
Skratka názvu:	SPS RQSCD NASES
Verzia:	1.1
Schválené dňa:	02.04.2026
Platnosť od:	02.04.2026
Identifikátor objektu (OID):	1.3.158.42156424.0.0.2.0.1

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.	Služba správy zariadení na vyhotovovanie kvalifikovaných elektronických pečatí na diaľku

1.3.158. 42156424.0.0.2.0	Vyhradené pre NASES
1.3.158. 42156424.0.0.2.0.1	SPS RQSCD

1.1.1 Identifikácia poskytovateľa služby (TSP identification)

Nasledujúca tabuľka obsahuje údaje poskytovateľa (NASES), ktorý je zodpovedný za poskytovanie dôveryhodnej služby.

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/

1.1.2 Podporované politiky služby (Supported signature creation application service component policy/policies)

Služba je implementovaná na úrovni LSP v zmysle ETSI TS 119 431-1, resp. SCAL1 podľa CEN EN 419 241-1, a to počas prechodného obdobia stanoveného Vykonávacím nariadením Komisie (EÚ) 2025/1567 z 29. júla 2025.

1.2 Komponenty a prostredie služby pre vytváranie pečatí (Signature creation application service component environment)

1.2.1 Účastníci (SCASC actors)

- NASES je poskytovateľ služby správy zariadení na vyhotovovanie kvalifikovaných pečatí na diaľku
- Tretie strany, ktoré sú využívané pre dodávanie služby:
  - dodávateľ služieb prevádzky (na základe prevádzkovej zmluvy)
- Kvalifikovaní poskytovatelia dôveryhodnej služby vydávania kvalifikovaných certifikátov pre kvalifikovanú elektronickú pečať, ktorí sú povinní informovať Poskytovateľa o revokácii certifikátu, a to za účelom zničenia kľúčových párov

1.2.2 Architektúra služby (Service architecture)

Základný popis architektúry služby a riešenia

Kvalifikovaná služba správy zariadení na vyhotovovanie kvalifikovaných pečatí na diaľku je poskytovaná v prostredí Ústredného portálu verejnej správy a teda využíva aj jeho komponenty.

Komponenty

Riešenie využíva komponenty:

- HSM moduly - pre správu zariadení na vyhotovovanie kvalifikovaných pečatí na diaľku (certifikované HSM moduly a obslužný softvér)
- IAM - pre autentifikáciu voči službe sa používa autentifikačný modul (IAM)
- CEP - pre funkčnosť priradenia kvalifikovaných certifikátov pre pečať a tým aj kľúčových párov z HSM modulov identite držiteľa sa používa modul Centrálna elektronická podateľňa (CEP)
- pre prístup k službe rozhranie USR modulu G2G a „konštruktor správy“

Rozhrania

Služba je po úspešnej autentifikácii držiteľa certifikátu poskytovaná:

- cez grafické rozhranie cez webový prehliadač, ako súčasť komponentu „konštruktor správy“
- cez aplikačné SOAP rozhranie „USR“ (univerzálne synchrónne rozhranie modulu G2G)

Prístup k službe

Podmienkou pre prístup k službe je:

- v prípade prístupu cez grafické rozhranie použitie prostriedkov elektronickej identifikácie zo strany osoby oprávnenej držiteľom kvalifikovaného certifikátu,
- v prípade prístupu k API služby je vybudovaný VPN tunel a použitie autentifikačného certifikátu zaregistrovaného zo strany držiteľa kvalifikovaného certifikátu pre pečať alebo ním oprávnenej osoby.

Kvalifikovanú službu správy zariadení na vyhotovovanie kvalifikovaných elektronických pečatí na diaľku využíva nekvalifikovaná služba vytvárania kvalifikovaných pečatí na diaľku CEP.

1.3 Definície a skratky (Definitions and abbreviations)

1.3.1 Definície

Pre prevádzkovú bezpečnosť platia ustanovenia uvedené v dokumente CP TSP.

1.3.2 Skraty

CA — Certifikačná autorita, poskytovateľ kvalifikovanej dôveryhodnej služby vydávania kvalifikovaných certifikátov (Certification Authority)

CEP — Centrálna elektronická podateľňa

CRAC — Centrálny register autentifikačných certifikátov v IAM ÚPVS obsahujúci certifikáty používané pri autentifikácii cez API voči službe STS IAM

CSR — Žiadosť o vydanie KC KEPe v elektronickej forme vo formáte PKCS#10 (Certificate signing request)

FOB — Fyzická a objektová bezpečnosť

G2G — Komunikačná časť modulu procesnej integrácie a integrácie údajov (poskytuje univerzálne synchrónne rozhranie USR pre prístup klientov k API služby a interné asynchrónne rozhranie pre interné moduly)

HSM — Hardvérový bezpečnostný modul (Hardware security module), certifikované zariadenie podľa Nariadenia eIDAS

IAM — Identity access management – komunikačná časť autentifikačného modulu v zmysle zákona č. 305/2013 Z.z.

IT — Informačná technológia (Information Technology)

KEPe — Kvalifikovaná elektronická pečať

KSC — Kvalifikovaný systémový certifikát

KC KEPe — Kvalifikovaný certifikát pre kvalifikovanú elektronickú pečať

NBÚ — Národný bezpečnostný úrad, orgán dohľadu

PMA — Autorita pre správu politík (Policy Management Authority)

PKI — Infraštruktúra verejného kľúča (Public Key Infrastructure)

QSCD — Kvalifikované zariadenie na vyhotovovanie elektronického podpisu/pečate (Qualified electronic Signature/Seal Creation Device)

SD — Schéma dohľadu, dokument vydaný NBÚ SR

SPS — Service practice statement, pravidlá poskytovania dôveryhodnej služby

SSAS — Server sealing application service, služba pre vytváranie kvalifikovaných pečatí na diaľku

STS — Security token service, autentifikačná služba IAM ktorej výstupom je SAML token ako potvrdenie o úspešnej autentifikácii

TS — Dôveryhodná služby (Trust Service)

TSA — Autorita časovej pečiatky, vydavateľ kvalifikovanej časovej pečiatky (Time-Stamping Authority)

TSP — Poskytovateľ dôveryhodnej služby (Trust Service Provider)

TSU — Jednotka dôveryhodnej služby (Trust Service Unit)

UTC — Univerzálny koordinovaný čas (Coordinated Universal Time)

V niektorých interných dokumentoch ešte môže byť použitý pojem Kvalifikovaný systémový certifikát (KSC) ale podľa ustanovenia Zákona[1] sa jedná o kvalifikovaný certifikát pre kvalifikovanú elektronickú pečať.

„Kvalifikovaný systémový certifikát vydaný podľa doterajších predpisov sa považuje za kvalifikovaný certifikát pre kvalifikovanú elektronickú pečať podľa osobitného predpisu, 11) do uplynutia jeho platnosti alebo jeho zrušenia.“

1.4 Politiky a pravidlá (Policies and practices)

1.4.1 Organizácia zodpovedná za správu dokumentácie (Organization administrating the TSP documentation)

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

Tabuľka 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] § 18 Prechodné ustanovenia, odsek (4) Zákona

1.4.2 Kontaktná osoba (Contact person)

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.

Osoba rozhodujúca o súlade s pravidlami poskytovania služby (SPS) s politikami

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

Pravidlá schvaľovania SPS

- Poskytovateľ musí mať schválené SPS ešte pred začiatkom prevádzky dôveryhodnej služby.
- Obsah pravidiel poskytovania schvaľuje generálny riaditeľ NASES na základe návrhu PMA.

1.4.3 Použitie dokumentácie poskytovateľa - TSP (public) documentation applicability

Pri poskytovaní dôveryhodnej služby sa uplatňuje:

- Postupy poskytovania služby pre vytváranie kvalifikovaných pečatí na diaľku v kapitole 1.4.4 tohto dokumentu (SSAS practice statement)
- Všeobecné podmienky ÚPVS
- Politika služby (referencia): služba je implementovaná na úrovni LSP v zmysle ETSI TS 119 431-1, resp. SCAL1 podľa CEN EN 419 241-1, a to počas prechodného obdobia stanoveného Vykonávacím nariadením Komisie (EÚ) 2025/1567 z 29. júla 2025
- Hodnotenie rizík a politika informačnej bezpečnosti
    - NASES má zavedené riadenie rizík informačnej a kybernetickej bezpečnosti a primerane sa vzťahuje aj na kvalifikovanú službu správy zariadení
- Dokumentácia funkčnosti a bezpečnostných požiadaviek procesu autentifikácie a autorizácie tretích strán voči kľúčovému materiálu uloženému v HSM / ÚVPS v súlade s alternatívnym postupom certifikácie QSCD a SAM Rakúska podľa článku 30 Nariadenia Európskeho parlamentu a Rady EÚ č. 910/2014 (interný dokument posudzovaný v rámci auditu)

1.4.4 Postupy poskytovania služby pre vytváranie kvalifikovaných pečatí na diaľku (SSAS practice statement)

Inicializácia kľúčového páru pre kvalifikovanú elektronickú pečať a jeho priradenie držiteľovi

- Inicializácia a priradenie kľúčového páru identite sa riadi Metodickým usmernením č. 3/2015 ku konaniu o vydanie a inicializáciu kvalifikovaného certifikátu pre kvalifikovanú elektronickú pečať na Ústrednom portáli verejnej správy.

  Základné kroky procesu:

- Žiadateľ predkladá žiadosť s úradne overeným podpisom oprávnenej osoby, poverením, prípadne zaručene skonvertovaným poverením alebo odoslaním z jej elektronickej schránky.
- Poskytovateľ po splnení podmienok a kontrole údajov v žiadosti vygeneruje CSR (PKCS#10) s údajmi uvedenými v žiadosti a doručí ho žiadateľovi.
- Pre kľúčové páry vygenerované v službe správy zariadení sú na základe CSR (PKCS#10) vydávané kvalifikované certifikáty pre kvalifikovanú elektronickú pečať, a to poskytovateľmi kvalifikovanej dôveryhodnej služby vydávania kvalifikovaných certifikátov pre kvalifikovanú elektronickú pečať ako je NASES SNCA alebo ľubovoľný iný kvalifikovaný poskytovateľ, ktorého žiadateľ uviedol v žiadosti.
- Žiadateľ doručí vydaný kvalifikovaný certifikát pre kvalifikovanú elektronickú pečať Poskytovateľovi.
- Kľúčový pár a kvalifikovaný certifikát sú následne osobami v dôveryhodných roliach priradené osobe žiadateľa a tieto údaje sa pri priraďovaní kontrolujú.

Inicializácia vytvorenia kvalifikovanej pečate

- Kvalifikovaná pečať vzniká na základe úspešnej autentifikácie držiteľa alebo oprávneného zástupcu držiteľa kvalifikovaného certifikátu použitím služby vytvorenia kvalifikovanej pečate na diaľku:
  - cez API volaním služby „PodpisanieDokumentov“ alebo „PodpisanieDokumentov2“ popísanej v integračnom manuáli modulu CEP, pričom informačný systém (technický účet) sa autentifikuje s platným SAML tokenom vydaným pre aktuálne platný autentifikačný certifikát zaregistrovaný v centrálnom registri autentifikačných certifikátov IAM ÚPVS (CRAC) a zároveň musí mať zo strany držiteľa kvalifikovaného certifikátu priradenú rolu R_CEP_SIGN_SYNC, ktorá povoľuje vytváranie

kvalifikovaných elektronických pečatí a kontroluje sa pri každom volaní služby.

- v grafickom rozhraní konštruktora správy pri vytváraní elektronickej úradnej správy kliknutím na tlačidlo „Zapečatiť“ zo strany používateľa zastupujúceho orgán verejnej moci, a to podľa zverejnených návodov, pričom používateľ musí mať zo strany držiteľa udelené oprávnenie na disponovanie s elektronickou schránkou a pridelenú rolu R_EDESK_SIGN, ktorá povoľuje vytváranie kvalifikovaných elektronických pečatí a kontroluje sa pri každom použití služby (štatutár organizácie ako držiteľ má rolu pridelenú v rámci procesu priradenia kvalifikovaného certifikátu pre pečať).

- Podmienkou pre použitie služby je autentifikácia voči modulu IAM:
  - cez službu IAM WebSSO pre prístup cez grafické rozhranie, ktorej výstupom je WebSSO SAML token s platnosťou 20 minút a následným automatickým obnovovaním prístupu; pri použití služby pečatenia bude po uplynutí určenej doby vyžiadaná opätovná autentifikácia.
  - cez službu IAM STS pre prístup cez API, ktorej výstupom je STS SAML token s platnosťou 120 minút; pri každej autentifikácii sa kontroluje, že autentifikačný certifikát nebol zrušený.
- Služba správy zariadení na vyhotovovanie kvalifikovanej elektronickej pečate na diaľku kontroluje pred každým vytvorením kvalifikovanej pečate zhodu autentifikovanej osoby voči držiteľovi kvalifikovaného certifikátu a teda aj kľúčového páru; kľúčový pár je použitý výlučne v prípade zhody, v opačnom prípade je na výstupe zaslaná chybová správa.

Zásady ochrany prístupu k službe zo strany odberateľa (klienta):

- Systém klienta využívajúci prístup cez API musí zabezpečiť vytváranie kľúčových párov pre autentifikáciu výlučne v chránenom prostredí.
- Systém volajúci službu cez API musí chrániť prístupy cez VPN a vydané STS SAML tokeny vo vzťahu k použitiu služby.
- Používatelia grafického rozhrania musia konať vždy len pod vlastnou autentifikáciou a nesmú umožniť prístup inej osobe k aplikácii.

2. Riadenie a prevádzka dôveryhodnej služby (Trust Service management and operation)

2.1 Vnútorná organizácia (Internal organization)

Organizačné zabezpečenie NASES ako poskytovateľa dôveryhodnej služby je popísané v rámci vnútorného organizačného poriadku Poskytovateľa.

Poskytovateľ:

- je rozpočtová organizácia podliehajúca legislatíve Slovenskej republiky.
- má zavedené opatrenia na riadenia kvality a informačnej bezpečnosti primerané pre poskytované dôveryhodné služby,
- zamestnáva dostatočný počet osôb, ktoré majú nevyhnutné vzdelanie, školenia, technické znalosti a skúsenosti vzhľadom na typ, rozsah a množstvo práce nevyhnutnej na poskytovanie dôveryhodnej služby.

2.1.1 Spoľahlivosť organizácie (Organization reliability)

Organizačné zabezpečenie NASES je popísané v rámci vnútorného organizačného poriadku NASES.

Dodávatelia sú viazaní politikami poskytovateľa dôveryhodných služieb.

2.1.2 Segregácia oprávnení (Segregation of duties)

Proces riadenia prístupu a oddelenia rolí je ustanovený internými pravidlami NASES.

Dôveryhodné role zahŕňajú najmä nasledovné zodpovednosti:

a. Bezpečnostný správca – má celkovú zodpovednosť za správu a implementáciu bezpečnostných postupov.
b. Systémový administrátor – inštaluje, konfiguruje a udržiava dôveryhodný systém Poskytovateľa z pohľadu riadenia služieb. Má zodpovednosť za každodennú prevádzku dôveryhodného systému Poskytovateľa a zálohovanie systému.
c. Audítor – je autorizovaný na kontrolovanie prevádzky dôveryhodných služieb a prezeranie archívov a auditných záznamov dôveryhodného systému Poskytovateľa.
d. PMA – vykonáva dohľad nad tvorbou politík a pravidiel súvisiacich s poskytovaním dôveryhodných služieb a rozhodovanie v prípade sporných udalostí, ktoré môžu pri poskytovaní dôveryhodných služieb nastať.

2.2 Ľudské zdroje (Human resources)

Proces zaistenia personálnej bezpečnosti je ustanovený internými pravidlami NASES. Osoby v dôveryhodných roliach absolvujú pravidelne, najmenej raz za 12 mesiacov, aktualizačné školenia zamerané na nové hrozby a aktuálne bezpečnostné postupy.

2.3 Správa aktív (Asset management)

Proces riadenia aktív je ustanovený internými pravidlami NASES.

2.3.1 Všeobecné požiadavky (General requirements)

Proces riadenia aktív je ustanovený internými pravidlami NASES.

2.3.2 Manipulácia s médiami (Media handling)

S každým médiom musí byť zaobchádzané bezpečne v zmysle požiadaviek klasifikačnej schémy informácií. Médiá obsahujúce citlivé údaje musia byť bezpečne zlikvidované, ak už nie sú ďalej potrebné.

2.4 Riadenie prístupu (Access control)

Proces riadenia prístupu je ustanovený internými pravidlami NASES.

Prístupy klientov k službe sú uvedené v kapitole 1.2.2 (časť Rozhrania a časť Prístup k službe)

2.5 Kryptografické opatrenia (Cryptographic controls)

Generovanie kľúčov

- Kľúčové páry sú generované na základe žiadosti klienta a sprístupnené na použitie klientovi až po dodaní kvalifikovaného certifikátu a napárovaní na identitu osobou v dôveryhodnej roli.
- Generovanie kľúčov je vykonané vo fyzicky bezpečnom prostredí.
- Generovanie privátnych kľúčov je vykonávané v kvalifikovanom kryptografickom zariadení (HSM).
- Kľúčové páry generuje osoba v dôveryhodných roli.
- Súkromný podpisový kľúč Klienta je uložený a používaný v bezpečnom zariadení na vytváranie elektronickej pečate (HSM modul s platnou certifikáciou s kľúčmi uloženými v zašifrovanom stave na úložisku servera).
- Súkromný kľúč klienta nie je nikdy exportovaný a ukladaný v nezašifrovanom stave.

- Pri kopírovaní kľúčových párov na jednotlivé HSM moduly sa uplatňuje pravidlo 4 očí (dve osoby v dôveryhodných roliach).
- Akékoľvek záložné kópie súkromných kľúčov Klientov sú chránené tak, že je zabezpečená ich integrita a dôvernosť.

Prevádzkované HSM

- Prevádzkované sú HSM zariadenia Thales Solo 500+ a 6000+ vo verzii firmware 2.61.2, ktoré sú vedené ako certifikované SSCD zariadenia https://eidas.ec.europa.eu/efda/browse/notification/qscd-sscd, krajina Taliansko.
- Kvórum HSM security world: 1/x

Kryptografické algoritmy a veľkosť generovaných kľúčových párov:

- veľkosť kľúča: minimálne 3072 bit
- algoritmus: RSA SHA 256
- pri určovaní algoritmov a veľkosti kľúčov sa postupuje v súlade s ETSI TS 119 312

Ukončenie životného cyklu kľúča

- Dátum exspirácie kľúčov pre KEPe je koniec platnosti pridružného certifikátu verejného kľúča (KC KEPe), kde musí zohľadňovať životnosť definovanú v „odporúčaných veľkostiach kľúča vzhľadom na čas“ z normy ETSI TS 119 312.
- V prípade zrušenia platnosti certifikátu (revokácie) je vydavateľ certifikátu povinný informovať Poskytovateľa. Po doručení informácie o zrušení certifikátu je na strane Poskytovateľa zadaná požiadavka na zničenie/odstránenie kľúčového páru. Zálohy kľúčového páru vykonávané v rámci prevádzkových záloh sú odstraňované len po uplynutí príslušných retenčných dôb.
- Kľúčový pár musí byť zničený/odstránený aj na žiadosť klienta, bez ohľadu na revokáciu kvalifikovaného certifikátu.
- Kľúčový pár, pre ktorý nie je vydaný kvalifikovaný certifikát do 90 dní od jeho vygenerovania, bude zničený/odstránený v rámci procesov poskytovateľa.
- Súkromný kľúč pre KEPe nebude použitý po skončení jeho životného cyklu.
- Prevádzkovateľ zabezpečí predovšetkým, že súkromné kľúče pre KEPe, alebo ľubovoľná časť kľúča, zahrňujúc akékoľvek kópie, budú likvidované tak, aby súkromné kľúče prakticky nebolo možné obnoviť.

2.6 Fyzická a objektová bezpečnosť (Physical and environmental security)

Proces fyzickej a objektovej bezpečnosti (FOB) je ustanovený v dokumente Bezpečnostná politika NASES. Nasledujúce ustanovenia sa vzťahujú špecificky na komponenty infraštruktúry poskytovanej dôveryhodnej služby správy zariadení na vyhotovovanie kvalifikovaných elektronických pečatí na diaľku.

Komponenty infraštruktúry dôveryhodnej služby — predovšetkým HSM zariadenia, servery modulu CEP a IAM a sieťové prvky — sú umiestnené v dátových centrách prevádzkovaných v rámci infraštruktúry ÚPVS a sú vybavené konštrukčnými prvkami brániacimi neautorizovanému prístupu, poškodeniu alebo rušeniu.

Fyzické riadenie prístupu

Prístup do priestorov, v ktorých sú prevádzkované komponenty dôveryhodnej služby, je riadený na základe princípu minimálnych oprávnení. Na kryptografický modul je aplikované riadenie prístupu v súlade s odstavcom 2.4 a dokumentáciou.

Platia tieto pravidlá:

- prístup je povolený výlučne osobám v dôveryhodných roliach alebo nimi autorizovaným osobám (napr. technici dodávateľa prevádzky) na základe vopred schválenej žiadosti,
- každý vstup do fyzicky bezpečnej oblasti podlieha nezávislému dohľadu; neautorizovaná osoba musí byť po celý čas pobytu sprevádzaná autorizovanou osobou,
- každý vstup a prítomnosť v chránenej oblasti sú zaznamenávané
- fyzická ochrana je dosiahnutá jasne definovanou bezpečnostnou hranicou (perimetrom) tvorenou fyzickými bariérami — stavebnou konštrukciou, mrežami, bezpečnostnými dverami a kamerovým systémom,
- časti objektu zdieľané s inými organizáciami alebo tretími stranami sú umiestnené mimo bezpečnostného perimetra dôveryhodnej služby.
- 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

Na HSM zariadenia je uplatňované osobitné riadenie fyzického prístupu: prístup k HSM modulom (fyzická manipulácia, pripojenie zariadení, zmena konfigurácie security world) si vyžaduje súčasnú autorizáciu minimálne dvoch osôb v dôveryhodných roliach (pravidlo štyroch očí).

2.7 Prevádzková bezpečnosť (Operation security)

Pre prevádzkovú bezpečnosť platia ustanovenia uvedené v dokumente CP TSP odstavec 7.7 a ďalej toto:

- NASES monitoruje kapacitné možnosti poskytovanej služby a včas zapracúva do budúcich požiadaviek na kapacitu, aby sa zabezpečil dostupný adekvátny výkon a úložný priestor.

2.8 Sieťová bezpečnosť (Network security)

Pre sieťovú bezpečnosť platia pre NASES ustanovenia uvedené v dokumente CP TSP odstavec 7.8 a ďalej tieto:

- všetky TSU sú udržiavané a chránené v bezpečnej zóne,
- všetky systémy TSU sú nakonfigurované tak, že majú odstránené a/alebo zakázané všetky účty, aplikácie, služby, protokoly a porty, ktoré nie sú používané pre ich prevádzku,
- do bezpečných zón a vysoko bezpečných zón majú prístup len dôveryhodné roly.
- v rámci sieťovej bezpečnosti sa zároveň vykonávajú pravidelné skeny zraniteľností minimálne raz za štvrťrok.

2.9 Riadenie incidentov (Incident management)

Proces riadenia bezpečnostných incidentov je ustanovený v dokumente CP TSP odstavec 7.9.

2.10 Zber dôkazov (Collection of evidence)

Pre zber dôkazov platia ustanovenia uvedené v dokumente CP TSP odstavec 7.10 a ďalej sú zaznamenávané všetky udalosti týkajúce sa:

- riadenia životného cyklu kľúčov,
- riadenia životného cyklu certifikátov.

2.11 Riadenie kontinuity činnosti (Business continuity management)

Poskytovateľ má spracované postupy obnovy v prípade poškodenia časti infraštruktúry.

Pre riadenie kontinuity činnosti NASES platia ustanovenia uvedené v dokumente CP TSP odstavec 7.11.

Procedúry pre prípad kompromitácie súkromného kľúča

- Zaevidovaný incident – Kroky sú vykonávané na základe zaevidovaného kritického bezpečnostného incidentu, na základe kontroly záznamov prístupov k HSM a službe CEP.
- Zablokovanie použitia kompromitovaného privátneho kľúča/kľúčov a kvalifikovaného certifikátu v CEP / HSM.
- Informovanie vydavateľa certifikátu (obvykle SNCA alebo externú CA) s odporúčaním na revokáciu certifikátu.
- Informovanie klienta/klientov o kompromitácii kľúča, zablokovaní jeho použitia a odporúčanej revokácii certifikátu (NASES).
- Informovanie NBÚ o významnom incidente (NASES)
- SNCA / príslušná CA revokuje kvalifikované certifikáty a NASES informuje Globaltel cez ServiceDesk so žiadosťou o odstránenie kľúčových párov z HSM.
- Odstránenie všetkých kľúčových párov z HSM po každej revokácii.

2.12 Plány ukončenia poskytovania služby (TSP termination and termination plans)

Pre ukončenie činnosti Poskytovateľa platia ustanovenia uvedené v dokumente CP TSP odstavec 7.12 a ďalej toto:

- V prípade ukončenia dôveryhodnej služby NASES musia byť informované vydávajúce certifikačné autority a nimi zrušené všetky certifikáty vydané pre Klientov NASES.

2.13 Zhoda (Compliance)

Pre zhodu platia ustanovenia uvedené v dokumente CP TSP odstavec 7.13 a zároveň:

Zoznam požiadaviek ETSI TS 119 431-1, s ktorými nie je služba v súlade:

- Sú dodržané všetky požiadavky uvedené v 6.3 okrem okamžitej detekcie činnosti správcov, pričom tieto sú kontrolované v plánovaných intervaloch spätne.
- Služba je implementovaná na úrovni LSP v zmysle ETSI TS 119 431-1, resp. SCAL1 podľa CEN EN 419 241-1, a to počas prechodného obdobia stanoveného Vykonávacím nariadením Komisie (EÚ) 2025/1567 z 29. júla 2025.
- Namiesto formátu SAD (Signature Activation Data) a SAP (Signature Activation Protocol) sa používajú postupy podľa Dokumentácie funkčnosti a bezpečnostných požiadaviek procesu autentifikácie a autorizácie tretích strán voči kľúčovému materiálu uloženému v HSM / ÚVPS v súlade s alternatívnym postupom certifikácie QSCD a SAM Rakúska podľa článku 30 Nariadenia Európskeho parlamentu a Rady EÚ č. 910/2014 (interný dokument posudzovaný v rámci auditu), a to na základe prechodného obdobia do roku 2027 stanoveného Vykonávacím nariadením Komisie EÚ č. 2025/1567. Každá jednotlivá operácia pečatenia je vykonaná až po overení oprávnenia (rola, väzba na držiteľa) a je dôkazne viazaná na konkrétnu reprezentáciu DTBS/R prostredníctvom auditných záznamov.

Pre každú operáciu pečatenia sa zaznamenáva minimálne:

(a) identita autentifikovanej osoby a držiteľa,

(b) identifikátor relácie a čas (UTC),

(c) identifikátor DTBS/R (hash),

(d) identifikátor kľúča/certifikátu,

(e) výsledok operácie,

(f) príslušné tokeny/overenia (referencie).

Retenčná doba v súlade s EN 319 401 a národným právom.

3. Technické požiadavky na aplikáciu pre vytváranie pečatí (Signature creation application service component technical requirements)

Prístup k rozhraniam služby správy zariadení na vyhotovovanie kvalifikovaných pečatí na diaľku majú výlučne vnútorné komponenty Centrálnej elektronickej podateľne, ktoré zabezpečujú samotné vyhotovovanie kvalifikovaných pečatí.

3.1 Rozhrania (Interfaces)

Rovnako ako v kapitole 1.2.2 (Rozhrania a Prístup k službe).

Pri poskytovaní služby sú dodržiavané povinné požiadavky kapitoly 8.2 *ETSI TS 119 431-2 a zároveň ETSI TS 119 101*.

3.2 Vytváranie zdokonalených elektronických pečatí (AdES digital signature creation)

Rovnako ako v kapitole 1.2.2 (Rozhrania a Prístup k službe)

Ku kvalifikovaným pečatiam vytváraným v automatizovanom režime internými procesmi ÚPVS (napríklad na doručenkách, potvrdeniach o odoslaní podania, na platobných príkazoch) nemá držiteľ certifikátu (MIRRI SR) priamy prístup z dôvodu automatizovaného vyhotovovania. Vytvorené pečate sú však uchovávané v rámci logov a držiteľ k nim môže na požiadanie získať prístup.

Vytvárané formáty zdokonalených elektronických podpisov a obmedzenia služby sú uvedené v Dokumentácii funkčnosti Centrálnej elektronickej podateľne (kapitola 5.2).

Pri poskytovaní služby sú dodržiavané povinné požiadavky kapitoly 8.2 *ETSI TS 119 431-2 a zároveň ETSI TS 119 101*.