Č. p.:

DKDS3 Certifikačná politika poskytovania kvalifikovanej dôveryhodnej služby validácie kvalifikovaných elektronických podpisov a pečatí

Názov dokumentu:	DKDS3 Certifikačná politika poskytovania kvalifikovanej dôveryhodnej služby validácie kvalifikovaných elektronických podpisov a pečatí		
Označenie dokumentu:	DKDS3 Certifikačná politika validačnej služby SNCA.pdf		
Verzia:	0.9	Status:	*Návrh*
Dátum vytvorenia:	18.11.2020	Platný do:	31.12.2021

História dokumentu

História revízií dokumentu

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

Schválenia

Verzia	Funkcia	V zastúpení	Schválil dňa	Podpis

Distribúcia

Verzia	Spoločnosť	Meno	Počet výtlačkov

Referencie na legislatívne a normatívne dokumenty

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

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

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

[4] Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.

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

[6] ISO32000. Document management - Portable document format.
ISO 32000-2:2017

[7] ETSI TS 103 174 v.2.2.1 - Electronic Signatures and Infrastructures (ESI); ASiC Baseline Profile.
ETSI TS 103 174 V2.2.1

[8] NBÚ SR. Disig QES Signer 4 - Deklarácia výrobcu aplikácie pre kvalifikovaný elektronický podpis/pečať (QES).

[9] ETSI TS 103 173 v.2.2.1 - Electronic Signatures and Infrastructures (ESI); CAdES Baseline Profile.
ETSI TS 103 173 V2.2.1

[10] ETSI TS 103 172 V2.2.2 - Electronic Signatures and Infrastructures (ESI); PAdES Baseline Profile.
ETSI TS 103 172 V2.2.2

[11] ETSI TS 103 171 V2.1.1 - Electronic Signatures and Infrastructures (ESI); XAdES Baseline Profile.
ETSI TS 103 171 V2.1.1

[12] ETSI TS 102 853 V1.1.1 - Electronic Signatures and Infrastructures (ESI); Signature verification procedures and policies.
ETSI TS 102 853 V1.1.1

[13] ETSI EN 319 102-1 V1.0.0 (Draft) - Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation.
ETSI EN 319 102-1 V1.0.0

[14] RFC 3647 „Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework“.
RFC 3647

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

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

[17] ETSI EN 319 401 - Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.
ETSI EN 319 401 V2.1.1

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

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

Zoznam tabuliek

Použité definície a skratky

Tabuľka 1 Použité definície

Definícia	Vysvetlenie definície
Univerzálny koordinovaný čas	Časová škála, založená na sekunde podľa definície v Recommendation ITU-R TF.460-6, „svetový čas“.
Jednotka validačnej služby	Politika poskytovania kvalifikovanej dôveryhodnej služby validácie kvalifikovaných elektronických podpisov/pečatí.
Odberateľ	Odberateľ kvalifikovaných dôveryhodných služieb poskytovaných NASES.
Poskytovateľ	Národná agentúra pre sieťové a elektronické služby.
Prevádzkovateľ	Organizačný útvar, ktorý na základe rozhodnutia poskytovateľa prevádzkuje IS KDS.

Tabuľka 2 Použité skratky

Skratka	Vysvetlenie skratky
CA	Certifikačná autorita.
CP VS	Politika poskytovania kvalifikovanej dôveryhodnej služby validácie kvalifikovaných elektronických podpisov/pečatí.
IS KDS	Informačný systém Kvalifikovaných dôveryhodných služieb.
IT	Informačné technológie.
Nariadenie eIDAS	Nariadenie Európskeho parlamentu a Rady (EÚ) č. 910/2014 [1].
NASES	Národná agentúra pre sieťové a elektronické služby.
NBÚ	Národný bezpečnostný úrad.
PKI	Infraštruktúra verejného kľúča (Public Key Infrastructure).
PMA	Autorita pre riadenie politík (Policy Management Authority).
SNCA	Slovenská národná certifikačná autorita.
TSA	Autorita časovej pečiatky (Time-Stamping Authority).
TSL	Dôveryhodný zoznam (Trusted List).
TSP	Poskytovateľ dôveryhodnej služby (Trust Service Provider).
UTC	Univerzálny koordinovaný čas (Coordinated Universal Time).
VSU	Jednotka validačnej služby (Validation Service Unit).

Obsah

1 Úvod

Tento dokument definuje politiku poskytovania kvalifikovanej dôveryhodnej služby validácie kvalifikovaných elektronických podpisov a validácie kvalifikovaných elektronických pečatí (ďalej len „validačná služba“) a bezpečnostné požiadavky, ktoré sa týkajú postupov riadenia a prevádzkovej praxe pri poskytovaní tejto služby.

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

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

Táto certifikačná politika môže byť použitá pre poskytovanie verejnej validačnej služby ako aj pre poskytovanie validačnej služby v uzavretých komunitách.

Tento dokument môže byť použitý nezávislými orgánmi ako základ pre potvrdenie, že Poskytovateľ s prevádzkovaným systémom validačnej služby je dôveryhodný na poskytovanie služby validácie kvalifikovaných elektronických podpisov a kvalifikovaných elektronických pečatí.

Validačná služba , identifikovaná v tomto dokumente, je využívaná v okruhu pôsobnosti SNCA, zriadenej a prevádzkovanej agentúrou NASES

1.1 Prehľad

Táto certifikačná politika sa týka poskytovania dôveryhodnej služby:

- validácia kvalifikovaných elektronických podpisov a
- validácia kvalifikovaných elektronických pečatí,

v zmysle ustanovení Nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014 z 3. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES (ďalej len „Nariadenie eIDAS“) 0.

2 Názov dokumentu a jeho identifikácia

Politika poskytovania kvalifikovanej dôveryhodnej služby validácie kvalifikovaných elektronických podpisov a validácie kvalifikovaných elektronických pečatí je identifikovaná nasledovným identifikátorom, odvodeným od objektového identifikátora NASES:

1.3.158.42156424.0.1.6

kde jednotlivé zložky OID majú nasledovný význam:

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

2.1 Účastníci PKI

V rámci poskytovania validačnej služby, sú účastníkmi infraštruktúry verejného kľúča entity uvedené tejto časti.

2.1.1 Jednotka validačnej služby

Jednotka validačnej služby (VSU):

- je entita, ktorá poskytuje kvalifikovanú dôveryhodnú službu validácie kvalifikovaných elektronických podpisov a kvalifikovaných elektronických pečatí pre používateľov (Odberatelia, Spoliehajúce sa strany),
- má celkovú zodpovednosť za poskytovanie kvalifikovaných dôveryhodných služieb, špecifikovaných v odstavci 1.1,
- je uvádzaná vo výstupoch z validačnej služby (ďalej len „správa z validácie“) ako vydavateľ a jej súkromné kľúče sú používané pri autorizácii tejto správy,
- zaručuje, že všetky aspekty jej služieb, operácií a infraštruktúry, zviazanej so správami z validácie, vydanými podľa tejto politiky, sú vykonávané v súlade s jej požiadavkami

a ustanoveniami a v súlade s pravidlami poskytovania dôveryhodných služieb Poskytovateľa.

Poskytovateľ môže prevádzkovať viaceré VSU poskytujúce dôveryhodné validačné služby.

2.1.2 Odberateľ

Odberateľom sa rozumie fyzická osoba resp. právnická osoba, ktorej Poskytovateľ poskytuje validačnú službu a ten, na koho sa viažu záväzky odberateľa.

Podmienky, ktoré musí splniť Odberateľ, definuje táto certifikačná politika.

Ak je Odberateľom právnická osoba, táto môže zahŕňať niekoľko koncových používateľov alebo jediného koncového používateľa. Niektoré povinnosti, ktoré sa vzťahujú na túto právnickú osobu, sa zároveň vzťahujú aj na týchto koncových používateľov. V každom prípade, právnická osoba je plne zodpovedná, ak povinnosti dané touto certifikačnou politikou nie sú zo strany koncových používateľov správne splnené, a preto je takáto organizácia zodpovedná za vhodnú informovanosť svojich koncových používateľov.

V prípade, že je Odberateľ zároveň koncovým používateľom, je priamo zodpovedný za neplnenie svojich povinností v zmysle tejto certifikačnej politiky.

2.1.3 Spoliehajúca sa strana

Spoliehajúcou sa stranou je fyzická alebo právnická osoba, ktorá sa pri svojom konaní spolieha na správu z validácie.

2.1.4 Iní účastníci

PMA je zložka Poskytovateľa, ustanovená za účelom:

- dohľadu nad vytváraním a aktualizáciou certifikačnej politiky, vrátane vyhodnocovania zmien a plánov na implementovanie ľubovoľných prijatých zmien,
- revízie výsledkov auditov, aby sa určilo, či Poskytovateľ zodpovedne dodržiava ustanovenia, vydané certifikačnou politikou,
- vydávanie odporúčaní pre Poskytovateľa, týkajúcich sa nápravných a iných vhodných opatrení,
- riadenia a usmerňovania činnosti Poskytovateľa,
- výkonu funkcie interného audítora, pričom touto činnosťou poverí samostatného pracovníka Poskytovateľa.

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

2.2 Použiteľnosť správy z validácie

Správa z validácie vyhotovená v zmysle požiadaviek tejto politiky je použiteľná všade, kde je vyžadovaná validačná správa definovaná v článkoch 32 a 40 Nariadenia eIDAS. 0

2.3 Správa politiky

2.3.1 Organizácia zodpovedná za správu dokumentu

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

Kontaktná adresa:

Národná agentúra pre sieťové a elektronické služby

Detašované pracovisko:

BC Omnipolis,

Trnavská cesta 100/II,

821 01 Bratislava,

Slovenská republika,

http://www.nases.gov.sk

2.3.2 Kontaktná osoba

Bezpečnostný správca SNCA.

Národná agentúra pre sieťové a elektronické služby

Detašované pracovisko:

BC Omnipolis,

Trnavská cesta 100/II,

821 01 Bratislava,

Slovenská republika,

Telefón: +421 2 3278 0700

e-mail: info@nases.gov.sk

2.3.3 Osoba rozhodujúca o súlade CPS s CP

Osobou, ktorá je zodpovedná za súlad postupov Poskytovateľa s ustanoveniami, ktoré sú uvedené v tejto certifikačnej politike je osoba, menovaná do roly bezpečnostný správca SNCA.

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

2.3.4 Postupy schvaľovania CP

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

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

3 Zverejňovanie informácií a úložiská

3.1 Úložiská

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

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

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

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

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

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

3.2 Zverejňovanie informácií o validačnej službe

Poskytovateľ musí zverejňovať v on-line režime úložisko, ktoré je prístupné Odberateľom a Spoliehajúcim sa stranám, ktoré bude obsahovať minimálne tieto informácie:

- túto certifikačnú politiku,
- aktuálne stavy všetkých Európskych TSL využívaných pri činnosti validačnej služby,
- certifikáty jednotlivých VSU Poskytovateľa.

Verejne prístupná dokumentácia SNCA je zverejnená elektronicky na nasledujúcej internetovej stránke:

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

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

3.3 Frekvencia zverejňovania informácií

SNCA zverejňuje informácie určené na zverejnenie v zmysle nariadenia eIDAS a zákona č. 272/2016 Z. z., pričom tieto informácie sú aktualizované neodkladne po každej zmene.

Informácie o zrušenom certifikáte VSU sú dostupné na webovom sídle SNCA, ktoré slúži ako jeho úložisko.

Certifikačná politika, prípadne jej revízie, sa zverejňujú čo najskôr po ich schválení a vydaní.

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

3.4 Kontroly prístupu

Informácie podľa bodu 3.2 tejto certifikačnej politiky, zverejňuje prevádzkovateľ SNCA bez obmedzenia.

Ďalšie informácie nie sú verejnými informáciami a sú dostupné pracovníkom prevádzkovateľa SNCA a tretím stranám, na základe rozhodnutia riaditeľa organizačného útvaru, ktorý prevádzkuje SNCA, vždy však v súlade s platnými právnymi predpismi SR a EÚ.

4 Všeobecné ustanovenia

4.1 Všeobecné ustanovenia politiky

Táto certifikačná politika nadväzuje na dokument „Politika poskytovania dôveryhodných služieb NASES“ [2], kde sú popísané všeobecné požiadavky a pravidlá poskytovania dôveryhodných služieb, ktoré musí NASES ako poskytovateľ dôveryhodných služieb rešpektovať.

Očakáva sa, že Odberatelia a Spoliehajúce sa strany budú konzultovať podrobnosti spôsobu poskytovania validačnej služby priamo s poskytujúcou VSU Poskytovateľa.

4.2 Služby súvisiace s validačnou službou

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

- Poskytovanie validačnej služby – táto služba vytvára správu z validácie.
- Manažment validačnej služby – táto služba monitoruje a riadi procesy validačnej služby, aby sa zaistilo, že služba je poskytovaná v súlade s touto certifikačnou politikou. Súčasťou tohto manažmentu je proces aktivácie resp. de-aktivácie validačnej služby.

4.3 Poskytovateľ validačnej služby

Poskytovateľom dôveryhodnej služby vytvárania správy z validácie pre potreby Odberateľov v zmysle tejto certifikačnej politiky je agentúra NASES.

V súvislosti s poskytovaním validačnej služby, Poskytovateľ nesie celkovú zodpovednosť za poskytovanie všetkých služieb, definovaných v odstavci 4.2.

4.4 Používateľ validačnej služby

Používateľom validačnej služby je Odberateľ, resp. koncový používateľ Odberateľa. Pod používateľom sa myslí fyzická osoba, využívajúca validačnú službu.

5 Úvod do politiky validačnej služby a plnenie všeobecných požiadaviek

5.1 Všeobecne

Tento dokument definuje politiku poskytovania dôveryhodnej služby validácie kvalifikovaných elektronických podpisov a kvalifikovaných elektronických pečatí Poskytovateľom, ktorá vytvára správy z validácie vstupných dokumentov (kontajnerov), opatrené zdokonalenou elektronickou pečaťou predmetnej dôveryhodnej služby a kvalifikovanou časovou pečiatkou.

5.2 Cieľoví používatelia a použitie

5.2.1 Správna prax uplatňovania politiky dôveryhodnej validácie

Táto certifikačná politika môže byť použitá pre verejnú službu poskytovania dôveryhodnej služby validácie kvalifikovaných elektronických podpisov a pečatí ako aj na použitie v uzavretých komunitách.

5.3 Zmena politiky validačnej služby

Túto certifikačnú politiku môže Poskytovateľ dopĺňať a meniť podľa potreby tak, aby zachoval kontinuitu validačnej služby.

Typicky je zmena vyvolaná doplnením štandardov a legislatívnymi zmenami.

6 Politiky a pravidlá

6.1 Ohodnotenie rizík

Pozri kapitolu 5 dokumentu 02].

6.2 Pravidlá pre praktický výkon dôveryhodných služieb

Všeobecné pravidlá pre praktický výkon dôveryhodných služieb sú uvedené v dokumente [2].

6.3 Všeobecné podmienky

Platia všeobecné podmienky popísané v dokumente [2] odstavec 4.2.

6.4 Politika informačnej bezpečnosti

Politika informačnej bezpečnosti je popísaná v dokumente [2] odstavec 4.3.

6.5 Záväzky Poskytovateľa

6.5.1 Všeobecne

Poskytovateľ validačnej služby sa zaväzuje:

- realizovať všetky požiadavky, kladené na Poskytovateľa v zmysle kapitoly 6 a 7;
- používať bezpečné systémy a zaisťovať dostatočnú bezpečnosť postupov, ktoré tieto systémy podporujú vrátane dostatočnej kryptografickej bezpečnosti týchto systémov;
- používať bezpečné systémy pre uchovávanie záznamov;
- zabezpečiť, aby prax vytvárania správ z validácie zodpovedala procedúram popísaným v tejto certifikačnej politike.

6.5.2 Záväzky Poskytovateľa k Odberateľovi

Poskytovateľ si plní svoje záväzky v súlade s podmienkami poskytovania validačnej služby tak, aby táto služba bola maximálne dostupná a bola vykonávaná bezodkladne a s čo najväčšou precíznosťou.

6.6 Informácie pre spoliehajúce sa strany

Všeobecné podmienky, dostupné pre Spoliehajúce sa strany (pozri odstavec 6.3) v prípade, že sa spoliehajú na správu z validácie, musia zahŕňať:

- Povinnosť overenia, že správa z validácie bola riadne autorizovaná a že súkromný kľúč použitý na autorizáciu správy z validácie nebol do času overovania kompromitovaný.
- Počas platnosti certifikátu vydávajúcej VSU musí byť platnosť jeho podpisového kľúča overená na základe aktuálneho stavu jeho platnosti na základe údajov publikovaných Poskytovateľom.
- Všetky obmedzenia pre použitie validačnej služby podľa tejto politiky.
- Všetky ďalšie obmedzenia, uvedené v dohodách alebo kdekoľvek inde.

7 Manažment a prevádzka validačnej služby

7.1 Úvod

Manažment a prevádzka validačnej služby Poskytovateľa sú vykonávané tak, aby prijaté bezpečnostné opatrenia a nástroje na kontrolu ich plnenia poskytli nevyhnutnú dôveru, že budú naplnené.

Poskytovanie validačnej služby a jej dostupnosť je na rozhodnutí Poskytovateľa a závisí na dohode o úrovni poskytovaných služieb s Odberateľom.

7.2 Vnútorná organizácia

Pre vnútornú organizáciu platia ustanovenia, uvedené v dokumente[2], odstavec 5.1 a ďalej platí nasledovné:

Poskytovateľ:

- je právnická osoba, podliehajúca legislatíve Slovenskej republiky,
- má zavedený systém riadenia kvality a informačnej bezpečnosti, primeraný pre poskytovanie validačnej služby,
- zamestnáva dostatočný počet osôb, ktoré majú nevyhnutné vzdelanie, školenia, technické znalosti a skúsenosti vzhľadom na typ, rozsah a množstvo práce, nevyhnutnej na poskytovanie služieb dôveryhodnej validácie.

7.3 Personálna bezpečnosť

Pre personálnu bezpečnosť platia ustanovenia uvedené v dokumente [2] odstavec 5.2.

7.4 Správa aktív

Pre správu aktív platia ustanovenia uvedené v dokumente [2] odstavec 5.3.

7.5 Riadenie prístupu

Pre riadenie prístupu platia ustanovenia uvedené v dokumente [2] odstavec 5.4.

7.6 Kryptografické opatrenia

7.6.1 Všeobecne

Vhodné bezpečnostné opatrenia, aplikované na manažment akýchkoľvek kryptografických kľúčov a kryptografických zariadení počas ich životnosti, sú popísané v dokumente [2] odstavec 5.5.

7.6.2 Generovanie kľúčov pre VSU

Generovanie kľúčov pre jednotlivé VSU spĺňa nasledovné:

- Je vykonané vo fyzicky bezpečnom prostredí (pozri odstavec 7.9) osobami, zaradenými v dôveryhodných rolách (pozri odstavec 7.3), za účasti minimálne dvoch oprávnených osôb.
- Generovanie VSU autorizačného kľúča(-ov) je vykonávané v bezpečnom kryptografickom zariadení.
- Autorizačný kľúč VSU je možné importovať do iného kryptografického modulu len na základe rozhodnutia PMA a za účasti stanoveného počtu oprávnených osôb.
- Každá VSU má v danom čase k dispozícii len jeden aktívny kľúč na autorizáciu správ z validácie. Všetky VSU musia používať ten istý kľúč na autorizáciu správy z validácie.

7.6.3 Ochrana súkromného kľúča VSU

Súkromný kľúč VSU zostáva dôverný a jeho integrita je udržiavaná minimálne s týmito požiadavkami:

- Súkromný autorizačný kľúč VSU je uložený a používaný v bezpečnom hardvérovom zariadení.
- Súkromný kľúč VSU je zálohovaný, kopírovaný, ukladaný a obnovovaný len personálom v dôveryhodných rolách, za dodržania podmienky stanoveného počtu oprávnených osôb a vo fyzicky bezpečnom prostredí. Autorizované osoby na vykonávanie týchto činností sú len tie, ktoré podliehajú pravidlám, ktoré sú uvedené v dokumente [3].
- Akékoľvek záložné kópie súkromného autorizačného kľúča nachádzajúce sa mimo VSU sú chránené tak, že je zabezpečená ich integrita a dôvernosť.

7.6.4 Certifikát verejného kľúča VSU

Poskytovateľ zaručuje integritu a autenticitu verejného kľúča VSU pre overenie autorizácie nasledovne:

- Verejný kľúč VSU, ktorý slúži na overenie autorizácie, je dostupný spoliehajúcim sa stranám v certifikáte verejného kľúča.
- Certifikát verejného kľúča VSU pre overenie autorizácie, je vydaný certifikačnou autoritou, poskytujúcou služby v zmysle normy ETSI EN 319 411-1 [4].
- VSU nevytvorí správu z validácie pred tým ako jej certifikát verejného kľúča pre overenie autorizácie je načítaný v kryptografickom zariadení VSU.

7.6.5 Prepísanie kľúča VSU

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

7.6.6 Manažment životného cyklu podpisového kryptografického hardvéru

Aplikované sú nasledovné požiadavky:

- Do kryptografického hardvéru, kde sú uložené kryptografické kľúče, určené na autorizáciu správy z validácie, nesmie byť svojvoľne zasahované počas jeho prepravy.
- Do kryptografického hardvéru, kde sú uložené kryptografické kľúče, určené na autorizáciu správy z validácie, nesmie byť svojvoľne zasahované počas jeho skladovania.
- Inštalácia, aktivácia a duplikácia autorizačných kľúčov VSU v kryptografickom hardware je vykonávaná iba osobami v dôveryhodných rolách, s minimálne dvojitou kontrolou a vo fyzicky bezpečnom prostredí (pozri odstavec 7.9).
- Súkromné autorizačné kľúče VSU, uložené v kryptografickom module VSU, sú v prípade vyradenia modulu vymazané takým spôsobom, že je prakticky nemožné ich obnovenie.

7.6.7 Ukončenie životného cyklu kľúča VSU

Dátum exspirácie kľúčov VSU je viazaný na koniec platnosti pridružného certifikátu verejného kľúča, ktorý musí zohľadňovať životnosť, definovanú v „odporúčaných veľkostiach kľúča vzhľadom na čas“ z normy ETSI TS 119 312 [5].

Dátum exspirácie kľúčov VSU, môže byť definovaný nastavením periódy použitia súkromného kľúča v certifikáte verejného kľúča VSU.

V prípade, že Prevádzkovateľ služby má záujem poskytovať validačnú službu s kvalifikovaným štatútom aj po dátume exspirácie kľúčov VSU, je povinný vydať na verejný kľúč, používaný pri autorizácii správy z validácie, nový certifikát, s novou platnosťou, ktorý bude následne zaradený do SK TLS.

7.7 Vymedzenie služby a obmedzenia

7.7.1 Vymedzenie validačnej služby

Validačná služba je prevádzkovaná vo forme webovej služby a je určená pre subjekty, ktoré sa na túto službu integrujú podľa príslušnej integračnej dokumentácie. Služba nie je priamo určená pre používateľa, fyzickú osobu, ktorý by k validačnej službe pristupoval prostredníctvom webového prehliadača, ale môže byť určená, napríklad, pre automatizované systémy.

Všetky časy a časové hodnoty, ak nie je explicitne uvedené inak, sú uvádzané vo formáte UTC.

7.7.2 Obmedzenia služby

7.7.2.1 Formáty súborov

Validačná služba podporuje validáciu súborov/kontajnerov s nasledovnými koncovkami a významom.

- PDF – dokument podľa špecifikácie PDF ISO-32000 [6], ktorý je zároveň aj kontajnerom,
- ASICS – ASiC kontajner podľa ETSI TS 103174 [7],
- ASICE – ASiC kontajner podľa ETSI TS 103174 [7],
- SCS – ASiC kontajner podľa ETSI TS 103174 [7],
- SCE – ASiC kontajner podľa ETSI TS 103174 [7],
- ZIP – ASiC kontajner podľa ETSI TS 103174 [7].

Služba predpokladá, že sa jedná o kontajnery podľa špecifikácií, uvedených v príslušnej, odbornej dokumentácii.

7.7.2.2 Veľkosti súborov

Služba akceptuje z bezpečnostných dôvodov súbory do veľkosti 10 MB.

7.7.2.3 Vnorené kontajnery

Validácia vnorených kontajnerov nie je službou podporovaná. Vnorené kontajnery vo validovanom kontajneri sú vyhodnocované ako akékoľvek iné binárne súbory (nie sú už ďalej expandované).

7.8 Vytvorenie správy z validácie

7.8.1 Správa z validácie

Správa z validácie ako výstup z validačnej služby pre daný podpis alebo pečať musí vyhovovať technickým požiadavkám, ktoré sú definované v kapitole 5.1.

Správa z validácie musí byť autorizovaná minimálne zdokonalenou elektronickou pečaťou Poskytovateľa a opatrená časovou pečiatkou.

Predovšetkým:

- Správa z validácie musí byť autorizovaná len s využitím súkromného kľúča vytvoreného pre tento účel.
- Systém vytvárajúci správu z validácie musí zamietnuť akýkoľvek pokus o vytvorenie správy, ak certifikát vydaný na verejnú časť autorizačného kľúča prináležiacemu k súkromnej časti autorizačného kľúča používaného pri autorizácii exspiroval.

7.8.2 Kvalifikovaná časová pečiatka v správe z validácie

Správa z validácie obsahuje kvalifikovanú elektronickú časovú pečiatku. Pečiatka musí byť vyhotovená dôveryhodným poskytovateľom kvalifikovanej služby vyhotovovania kvalifikovanej elektronickej časovej pečiatky.

Systém, vytvárajúci správu z validácie, musí zamietnuť akýkoľvek pokus o vytvorenie správy, ak nie je dostupná vyššie uvedená služba časovej pečiatky.

7.9 Fyzická a objektová bezpečnosť

Pre fyzickú a objektovú bezpečnosť platia ustanovenia, uvedené v dokumente [2], odstavec 5.6 a ďalej nasledovné požiadavky:

- Na kryptografický modul musí byť aplikované riadenie prístupu v súlade s kapitolou 7.5.
- Na správu z validácie sa musia byť aplikované nasledovné dodatočné opatrenia:
  - Technické prostriedky na vytváranie správy z validácie musia byť prevádzkované v prostredí, ktoré fyzicky a logicky chráni služby pred kompromitáciou, ktorá môže byť spôsobená neautorizovaným prístupom k systémom alebo údajom.
  - Každý vstup do fyzicky bezpečnej oblasti musí podliehať nezávislému dohľadu a neautorizovaná osoba musí byť sprevádzaná autorizovanou osobou pokiaľ je v bezpečnej oblasti. Každý vstup a prítomnosť musí byť zaznamenaná.

- Fyzická ochrana musí byť dosiahnutá vytvorením jasne definovanej bezpečnostnej hranice (perimetrom, fyzickou bariérou) okolo správy z validácie. Akékoľvek časti objektu zdieľané s inými organizáciami musia byť mimo tohto perimetra.
- Fyzické a objektové bezpečnostné opatrenia musia chrániť objekty kde sú umiestnené systémy, samotné systémové zdroje a objekty použité na podporu ich prevádzky. Bezpečnostné opatrenia týkajúce sa fyzickej a objektovej bezpečnosti Poskytovateľa musia pokrývať minimálne fyzické riadenie prístupu, ochranu pred prírodnými katastrofami, ochranu pred požiarom, výpadok podporných rozvodov (napr. elektrina, telekomunikácie), zrútenie štruktúry, úniky z potrubí, ochranu proti odcudzeniu, vlámaniu, a obnovu po pohrome.
- Prijaté opatrenia musia chrániť zariadenia, informácie, médiá a softvér týkajúcich sa validačných služieb pred vynesením bez autorizácie.

7.10 Prevádzková bezpečnosť

Pre prevádzkovú bezpečnosť platia ustanovenia, uvedené v dokumente [2], odstavec 5.7 a naviac je potrebné zabezpečiť nasledovné:

- Poskytovateľ je povinný monitorovať kapacitné možnosti poskytovanej služby a v dostatočnom predstihu naplánovať rozšírenie komunikačnej, hardvérovej a softvérovej infraštruktúry VSU tak, aby bol nepretržite zabezpečený a dostupný adekvátny výpočtový výkon a úložný priestor.

7.11 Sieťová bezpečnosť

Pre sieťovú bezpečnosť platia pre Poskytovateľa ustanovenia, uvedené v dokumente [2], odstavec 5.8 a naviac je potrebné zabezpečiť nasledovné:

- Poskytovateľ musí udržiavať a chrániť všetky VSU v bezpečnej zóne,
- všetky systémy VSU musia byť nakonfigurované tak, že budú mať odstránené a/alebo zakázané všetky účty, aplikácie, služby, protokoly a porty, ktoré nie sú používané pre ich prevádzku,
- do bezpečných zón a vysoko bezpečných zón môžu mať prístup len dôveryhodné roly.

7.12 Riadenie bezpečnostných incidentov

Pre riadenie bezpečnostných incidentov platia ustanovenia, uvedené v dokumente [2], odstavec 5.9.

7.13 Zber dôkazov

Pre zber dôkazov platia ustanovenia, uvedené v dokumente [2], odstavec 5.10 a ďalej musia byť zaznamenávané všetky udalosti týkajúce sa:

- riadenia životného cyklu kľúčov VSU;
- riadenia životného cyklu certifikátov VSU.

7.14 Riadenie kontinuity činnosti organizácie

Pre riadenie kontinuity činnosti organizácie platia ustanovenia, uvedené v dokumente [2], odstavec 5.11 a naviac je potrebné zabezpečiť nasledovné:

- Plán obnovy po pohrome sa musí zaoberať kompromitáciou, prípadne podozrením z kompromitácie súkromného kľúča VSU.
- V prípade kompromitácie alebo podozrenia z kompromitácie pri vytváraní správy z validácie, musí Poskytovateľ sprístupniť všetkým odberateľom a spoliehajúcim sa stranám popis kompromitácie, ktorá nastala.
- V prípade kompromitácie prevádzky VSU (napr. kompromitácia kľúča VSU) alebo podozrenia z kompromitácie, nesmie vytvárať správy z validácie, pokiaľ nebudú vykonané kroky na obnovu po kompromitácii.
- V prípade významnej kompromitácie prevádzky Poskytovateľa, musí Poskytovateľ sprístupniť všetkým odberateľom a spoliehajúcim sa stranám informáciu, ktorá môže byť použitá na identifikáciu správy z validácie, ktoré mohli byť ovplyvnené, pokiaľ tým neporuší súkromie používateľov alebo bezpečnosť služieb Poskytovateľa.

7.15 Ukončenie činnosti Poskytovateľa a plány ukončenia činnosti

Pre ukončenie činnosti Poskytovateľa platia ustanovenia, uvedené v dokumente [2], odstavec 5.12 a naviac je potrebné zabezpečiť nasledovné:

- V prípade ukončenia služieb Poskytovateľa, musia byť zrušené všetky platné certifikáty, vydané pre VSU a musí byť zabezpečené, že príslušné súkromné kľúče nebude možne za žiadnych okolností obnoviť.

7.16 Zhoda

Pre zhodu platia ustanovenia uvedené v dokumente [2] odstavec 5.13.

8 Plnenie požiadaviek pre kvalifikovanú službu validácie kvalifikovaných elektronických podpisov a pečatí podľa Nariadenia eIDAS

8.1 Požiadavky

Keďže v čase vydania tejto politiky ešte neboli publikované vykonávacie akty k požiadavkám Nariadenia eIDAS [1], sú platné technické požiadavky definované v Schéme dohľadu (ďalej aj ako „SD“) vydanej NBÚ SR [3].

Schéma dohľadu definuje požiadavky na službu validácie kvalifikovaných elektronických podpisov a pečatí v kapitolách:

- 5.1 – spoločné požiadavky na poskytovateľov kvalifikovaných dôveryhodných služieb – SD5.1
- 5.3 – požiadavky na kvalifikovanú dôveryhodnú službu validácie kvalifikovaných elektronických podpisov a kvalifikovaných elektronických pečatí – SD5.3

Kapitola 5.3 SD kopíruje požiadavky Nariadenia eIDAS [1] a dopĺňa ich o technické požiadavky pre jednotlivé body.

8.2 Plnenie požiadaviek

Požiadavky eIDAS sú splnené vtedy, keď sú splnené technické požiadavky zo Schémy dohľadu.

8.2.1 Plnenie požiadaviek z kapitoly 5.1 Schémy dohľadu

Požiadavky, uvedené v kapitole 5.1 Schémy dohľadu, sú spoločné požiadavky pre všetky kvalifikované služby. Tieto požiadavky sú spracované v dokumente „Politika poskytovania dôveryhodných služieb NASES [2], ktorý popisuje všeobecné pravidlá pri poskytovaní dôveryhodných služieb.

8.2.2 Plnenie požiadavky z kapitoly 5.3 Schémy dohľadu

Požiadavky, uvedené v kapitole 5.4 Schémy dohľadu, definujú povinné a nepovinné výstupné charakteristiky validačnej služby.

Služba je realizovaná ako webová služba, ktorá prostredníctvom svojho rozhrania umožňuje nahrať dokument, podpísaný dokument alebo dokument opatrený pečaťou, zvoliť niektorý z podporovaných formátov správy dôveryhodnej validácie a čas, ku ktorému má byť validácia vykonávaná.

Tvorba výstupných správ z validácie je realizovaná pomocou NBÚ certifikovanej aplikácie Disig QES Signer 4 [8], ktorá implementuje overenie zhody elektronických dokumentov a podpisov so štandardmi základných profilov:

- CAdES - ETSI TS 103173 v.2.2.1 [9],
- PAdES - ETSI TS 103172 v.2.2.2 [10],
- XAdES - ETSI TS 103171 v.2.1.1 [11],
- ASiC - ETSI TS 103174 v.2.2.1 [7]

a vykonáva overenie platnosti podpisov/pečatí, vytvorených podľa týchto štandardov, pomocou konceptov a pravidiel zo štandardu verifikácie podpisov ETSI TS 102 853 v1.1.1 [12] a z pripravovaného štandardu validácie AdES podpisov ETSI EN 319 102-1 [13].

Správa z validácie, vygenerovaná aplikáciou, je ďalej rozšírená o:

- identifikáciu typov (kvalifikovaných) certifikátov a
- identifikáciu typov (kvalifikovaných) podpisov / pečatí

na základe pravidiel, uvedených v tabuľke T1 v kapitole 5.2.3 „Schémy dohľadu NBÚ SR“ [3].

Výsledná správa z validácie je vytvorená z týchto rozšírených dát. Správa môže byť vytvorená v nasledovných formátoch:

- ASiC súbor obsahujúci TXT súbor v UTF-8 štruktúre podľa SD5.3, ktorý je autorizovaný Poskytovateľom a opatrený kvalifikovanou časovou pečiatkou,
- PDF súbor obsahujúci čitateľnejší používateľsky prívetivý alternatívny formát výstupu, ktorý je autorizovaný Poskytovateľom a opatrený kvalifikovanou časovou pečiatkou,
- XML súbor so strojovo spracovateľnými informáciami z dôveryhodnej validácie, ktorý je autorizovaný Poskytovateľom a opatrený kvalifikovanou časovou pečiatkou.

V prípade neúspechu vygenerovania správy z validácie (z akéhokoľvek dôvodu) alebo nezhody dokumentu s podmienkami služby, je používateľovi/systému vrátená chybová správa s popisom dôvodu.

8.3 Certifikát verejného kľúča VSU a zdroj kvalifikovaných pečiatok

V zmysle „Schémy dohľadu NBÚ SR“ [3] je správa z validácie autorizovaná minimálne zdokonalenou elektronickou pečaťou služby, spolu s kvalifikovanou elektronickou časovou pečiatkou. Certifikát pre pečať je vydaný Poskytovateľom a kvalifikovaná elektronická časová pečiatka je vydaná TSA autoritou Poskytovateľa.