POLITIKA

poskytovania kvalifikovanej dôveryhodnej služby validácie kvalifikovaných elektronických podpisov a pečatí

Disig, a.s.
poskytovateľ dôveryhodných služieb

Vypracoval	**Ing.** Jozef Nigut
Dátum platnosti	**30.9.2022**
Verzia	**1.0**
Typ	**POLITIKA**
Schválil	**Ing. Peter Miškovič**

Obsah

1. Úvod

Tento dokument definuje politiku a plnenie bezpečnostných požiadaviek, ktoré sa týkajú prevádzkovej praxe a postupov riadenia poskytovania dôveryhodnej služby validácie kvalifikovaných elektronických podpisov a kvalifikovaných elektronických pečatí (ďalej len „validačná služba“). Poskytovateľom validačnej služby je spoločnosť Disig, a.s., so sídlom Záhradnícka 151, 821 08 Bratislava, IČO: 35975946, zapísaná v Obchodnom registri OS BA I, odd. Sa, vložka č. 3794/B (ďalej len „Poskytovateľ“), prostredníctvom svojho systému validačnej služby.

Táto politika môže byť použitá pre validačnú službu dostupnú verejne ako aj na validačnú službu v uzavretých komunitách. Tento dokument môže byť použitý nezávislými orgánmi ako základ pre potvrdenie, že Poskytovateľ je dôveryhodný na poskytovanie validácie kvalifikovaných elektronických podpisov a pečatí.

1.1 Prehľad

Táto politika sa týka poskytovania dôveryhodných služieb:

- Validácia kvalifikovaných elektronických podpisov
- 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“) [1];
- Schémy dohľadu kvalifikovaných dôveryhodných služieb definovaná orgánom dohľadu [2] .

1.2 Názov dokumentu a jeho identifikácia

Názov:	**Politika poskytovania kvalifikovanej dôveryhodnej služby validácie kvalifikovaných elektronických podpisov a pečatí**
Skratka názvu:	**VP QES Validation Disig***
Verzia:	**1.0**
Schválené dňa:	**30.9.2022**
Platnosť od:	**30.9.2022**
Tejto VP je priradený identifikátor objektu (OID):	**1.3.158.35975946.0.1.0.0.2**

* - v texte tohto dokumentu sa väčšinou používa pri odkaze len skrátená forma VP QESV

Popis použitého identifikátora objektu (OID):

1. – ISO assigned OIDs

1.**3**. – ISO Identified Organization

1.3.**158**. – Identifikačné číslo subjektu (IČO)

1.3.158.**35975946**. – Disig

1.3.158.35975946.0.**1.** – Poskytovateľ dôveryhodných služieb

1.3.158.35975946.0.1.0.0.2 – VP QES Validation Disig

1.3 Účastníci PKI

V rámci poskytovania validačnej služby sú účastníkmi entity uvedené tejto časti.

1.3.1 Jednotka validačnej služby (VSU)

Jednotka validačnej služby:

- je entita, ktorá poskytuje validačnú službu koncovým používateľom (Zákazníci, Spoliehajúce sa strany),
- má celkovú zodpovednosť za poskytovanie validačných služieb špecifikovaných v odstavci 1.1,
- je uvádzaná vo vytvorených správach z validácie ako ich vydavateľ a jej súkromné kľúče sú používané pri vyhotovovaní zdokonalenej pečate na zabezpečenie originality a integrity týchto správ,
- 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 na výkon validačných činností Poskytovateľa.

1.3.2 Zákazník

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

Ak je Zákazníkom 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.

Podmienky, ktoré musí splniť Zákazník, definuje táto VP QESV.

1.3.3 Spoliehajúca sa strana

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

1.3.4 Iní účastníci

Autorita pre správu politiky (Policy Management Authority - ďalej len „PMA“) je zložka Poskytovateľa ustanovená za účelom:

- dohľadu na vytváraním a aktualizáciou VP QESV, vrátane vyhodnocovania zmien a plánov na implementovanie ľubovoľných prijatých zmien,
- revízie výsledkov auditov, aby sa určilo, či Poskytovateľ zodpovedne dodržiava ustanovenia vydaných VP QESV,
- 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 zamestnanca.

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

1.3.5 Poskytovatelia iných služieb

Medzi poskytovateľov iných služieb patria:

- Autorita poskytujúca služby vyhotovovania kvalifikovaných elektronických časových pečiatok,
- Entita poskytujúca službu publikovania dôveryhodných zoznamov kvalifikovaných poskytovateľov dôveryhodných služieb (LoTL),
- Entita, ktorá poskytuje služby súvisiace so štatútom platnosti KC, ktoré sú predmetom validácie (CRL, OCSP responder).

1.4 Použiteľnosť správy z validácie

Správa z validácie vyhotovená v zmysle požiadaviek tejto VP QESV je použiteľná všade, kde je vyžadovaná správa z validácie definovaná v článkoch 32 a 40 Nariadenia eIDAS. [1].

1.5 Správa politiky

1.5.1 Organizácia zodpovedná za správu dokumentu

Za prípravu, vytvorenie a udržiavanie tohto dokumentu je zodpovedný:

Poskytovateľ	
spoločnosť:	**Disig, a.s.**
adresa:	**Záhradnícka 151, 821 08 Bratislava 2**
IČO:	**359 75 946**
telefón	**+421 2 20850140**
e-mail:	**disig@disig.sk**
webové sídlo:	**https://www.disig.sk**

1.5.2 Kontaktná osoba

Na účel tvorby politík a pravidiel má Poskytovateľ vytvorenú autoritu pre správu politík (PMA) (pozri bod 1.3.4), ktorá plne zodpovedá za ich obsah, a ktorá je pripravená odpovedať na všetky otázky týkajúce sa politík a pravidiel Poskytovateľa.

Kontaktné údaje na zložku zodpovednú za prevádzku služby:

Validačná služba Poskytovateľa	
adresa:	**Záhradnícka 151, 821 08 Bratislava 2**
telefón	**+421 2 20850140**
e-mail:	**spravaqesv@disig.sk**
webové sídlo:	**https://eidas.disig.sk**

1.5.3 Osoba rozhodujúca o súlade VP QESV s postupmi

Osobou, ktorá je zodpovedná za rozhodovanie o súlade postupov Poskytovateľa, ktoré sú uvedené v tejto VP QESV je osoba menovaná do roly PMA v zmysle interných predpisov.

1.5.4 Postupy schvaľovania VP QESV

Ešte pred začiatkom prevádzky má mať Poskytovateľ schválenú svoju VP QESV a musí spĺňať všetky jej požiadavky. Obsah VP QESV schvaľuje osoba menovaná do role PMA.

Po schválení zo strany PMA je príslušný dokument publikovaný v súlade s publikačnou a oznamovacou politikou.

1.6 Definície a skratky

1.6.1 Definície

Jednotka služby validácie (Validation Service Unit (VSU)): sústava technických a programových prostriedkov, ktorá je spravovaná ako jednotka a má v danom čase aktívny jeden kľúč na vytváranie správ z validácie

Poskytovateľ dôveryhodnej služby (Trust Service Provider (TSP)): entita, ktorá poskytuje jednu alebo viac dôveryhodných služieb

Systém validácie (QESV system): zostava IT produktov a komponentov zorganizovaných na podporu poskytovania služby validácie kvalifikovaných elektronických podpisov a pečatí

1.6.2 Skratky

CA	—	Certifikačná autorita, autorita vyhotovujúca certifikáty verejného kľúča (Certification Authority)
IT	—	Informačná technológia (Information Technology)
KC	—	Kvalifikovaný certifikát
TSA	—	Autorita časovej pečiatky, vydavateľ časovej pečiatky (Time-Stamping Authority)
VSU	—	Samostatná jednotka vytvárajúca správu z validácie (Validation Service Unit)
QSCD	—	Kvalifikované zariadenie na vyhotovovanie elektronického podpisu/pečate (Qualified electronic Signature/Seal Creation Device)
PoE	—	Dôkaz Existencie (Proof of Existence)
QES	—	Kvalifikovaný elektronický podpis/pečať (Qualified electronic Signature)
QSVSP	—	Kvalifikovaný poskytovateľ služby validácie podpisu/pečate (Qualified Signature/Seal Validation Service Provider)
SD	—	Podpísaný dokument (Signer’s Document)

SDO	—	Podpísaný dátový objekt (Signed Data Object)
SVA	—	Aplikácia pre validáciu elektronického podpisu/pečate (Signature Validation Application)
SVP	—	Validačný Protokol (Signature Validation Protocol)
SVS	—	Služba validácie kvalifikovaných podpisov a pečatí (Signature Validation Service)
SVSP	—	Poskytovateľ Služby validácie podpisu/pečate (Signature Validation Service Provider)
VPR	—	Proces validácie podpisu/pečate (Signature Validation Process)
TSP	—	Poskytovateľ dôveryhodnej služby (Trust Service Provider)
VPS	—	Pravidlá poskytovania Služby Validácie (Validation Practice Statement)
VR	—	Správa z Validácie (Validation Report)
SDR	—	Podpísaný dokument v zastúpení (Signed Document Representation)
DA	—	Aplikácia riadiaca proces (Driving Application)
SVSServ	—	Server použitý na Validáciu (Signature Validation service server)

2. Zverejňovanie informácií a úložiská

2.1 Úložiská

Funkciu úložiska Poskytovateľa bude zastávať webové sídlo validačnej služby Poskytovateľa. Presná URL adresa je uvedená v kapitole 1.5.2. Webové sídlo je prostredníctvom internetu verejne prístupné Zákazníkom, Spoliehajúcim sa stranám a verejnosti vôbec.

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

2.2 Zverejňovanie informácií o validačnej službe

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

- túto VP QESV,
- všeobecné podmienky používania (ďalej len „VPP“),
- certifikáty jednotlivých VSU Poskytovateľa, ktoré patria k jej verejným kľúčom, ktorých zodpovedajúci súkromný kľúč je využívaný pri pečatení správ z validácie.

Okrem vyššie uvedených informácií Poskytovateľ zverejňuje v on-line režime prostredníctvom svojho webového sídla aj ďalšie verejne dostupné dokumenty súvisiace s poskytovaním dôveryhodných služieb v zmysle tejto VP QESV.

2.3 Frekvencia zverejňovania informácií

VP QESV, VPP, prípadne ich revízie, sa musia zverejniť čo najskôr po ich schválení a vydaní.

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

2.4 Kontroly prístupu

Verejné informácie na webovom sídle sú prístupné v režime „na čítanie“.

Poskytovateľ musí chrániť ľubovoľnú informáciu uloženú v úložisku, ktorá nie je určená na verejné rozšírenie. Poskytovateľ musí vynaložiť maximálne úsilie na to, aby zaistil integritu, dôvernosť a dostupnosť dát vyplývajúcich s poskytovaných dôveryhodných služieb. Taktiež musí vykonať logické a bezpečnostné opatrenia, aby

zabránil neautorizovanému prístupu k úložisku osobám, ktoré by mohli akýmkoľvek spôsobom zmeniť, poškodiť, pridať resp. vymazať údaje uložené v úložisku.

3. Všeobecné ustanovenia

3.1 Všeobecné ustanovenia politiky

Tento dokument nadväzuje na dokument „Politika poskytovania dôveryhodných služieb Disig, a.s.“ [3], kde sú popísané všeobecné pravidlá poskytovaných dôveryhodných služieb.

Očakáva sa, že zákazníci a spoliehajúce sa strany budú konzultovať podrobnosti spôsobu poskytovania QESV služby priamo s Poskytovateľom.

Kvalifikované elektronické podpisy a kvalifikované elektronické pečate sú z technického hľadiska podobné. Preto text v tejto politike upravujúci požiadavky pre podpisy sa primerane uplatňuje aj na pečate.

3.2 Služby súvisiace s validačnou službou

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

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

3.3 Poskytovateľ validačnej služby

Poskytovateľ validačnej služby pre potreby Zákazníkov v zmysle tejto VP QESV je spoločnosť Disig, a.s..

Poskytovateľ nesie celkovú zodpovednosť za poskytovanie služieb súvisiacich s validačnou službou, ako sú definované v odstavci 3.2.

Poskytovateľ môže prevádzkovať niekoľko identifikovateľných nezávislých jednotiek na vytváranie validačných správ (VSU).

3.4 Používateľ validačnej služby

Používateľom validačnej služby je Zákazník, resp. koncový používateľ zákazníka.

4. Validačná služba

4.1 Úvod do validačnej služby

Požiadavky na validačnú službu sú definované nariadením eIDAS , konkrétne požiadavky sú uvedené v čl. 32, 33 a 40.

Dôveryhodný zoznam na národnej úrovni obsahuje informácie o poskytovateľoch kvalifikovaných dôveryhodných služieb a informácie o kvalifikovaných dôveryhodných službách, ktoré títo poskytovatelia poskytujú.

Európska komisia vedie zoznam národných dôveryhodných zoznamov, ktoré uverejňujú jednotlivé členské štáty EÚ v zmysle ustanovení vykonávacieho rozhodnutia Komisie č. 2015/1505. Tento európsky zoznam je označovaný ako List of Trust Lists (ďalej len „LoTL“). LoTL je dostupný online: https://ec.europa.eu/tools/lotl/eu-lotl.xml

4.2 Overenie informácií v LoTL

Validačná služba vykonáva pravidelnú kontrolu LoTL v zmysle požiadaviek ETSI TS 119 615 [4].

4.3 Kontrola formátu podpisu

4.3.1 Kontrola základných profilov

Validačná služba overuje formát podpisu v zmysle štandardov uvedených vo vykonávajúcom rozhodnutí Komisie č. 2015/1506.

- Základný profil XAdES - ETSI TS 103171 v.2.1.1
- Základný profil CAdES - ETSI TS 103173 v.2.2.1
- Základný profil PAdES - ETSI TS 103172 v.2.2.2
- Základný profil podpisového kontajnera vo formáte ASiC - ETSI TS 103174 v.2.2.1

Zároveň validačná služba vyhodnocuje aj jednotlivé úrovne základných profilov:

- Základná úroveň – B-Level
- Podpis s časovou pečiatkou – T-Level,
- Podpis s časovou pečiatkou a validačnými údajmi – LT-Level,
- Podpis pre dlhodobú overiteľnosť a integritu validačných údajov – LTA-Level.

4.4 Validačný proces

Validačný proces je vykonaný v zmysle ustanovení schémy dohľadu s posúdením konkrétnych požiadaviek príslušných štandardov pre jednotlivé formáty podpisov.

4.5 Výstup validačného procesu

Výstup validačného procesu je realizovaný vo forme XML súboru, TXT súboru v ASiC kontajneri alebo v PDF súboru.

4.6 Výsledok validácie

Celkový výsledok validácie je vyhodnotený ako je uvedené v tabuľke č. 1.

Tab. č. 1 – Výsledok validácie podpisu

Výsledok	Popis
Platný (úplné overenie)	**Na základe vyhodnotenia parametrov podpisu a dokumentu bolo možné určiť úplnú platnosť podpisu.**
Platný (čiastočné overenie)	**Podpis bol štrukturálne overený ako platný, no zatiaľ nebolo možné plne overiť platnosť všetkých certifikátov, napr. kvôli neaktuálnym údajom o zrušení certifikátov.**
Neplatný	**Na základe vyhodnotenia parametrov podpisu a dokumentu bolo možné určiť úplnú neplatnosť podpisu.**
Nerozhodnutý	**Na základe vyhodnotenia parametrov podpisu a dokumentu nebolo možné určiť úplnú platnosť alebo neplatnosť podpisu.**

4.7 Vymedzenie služby a obmedzenia

4.7.1 Vymedzenie validačnej služby

Validačná služba je prevádzkovaná vo forme webovej služby a je určená pre aplikácie alebo 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.

4.7.2 Obmedzenia validačnej služby

4.7.2.1. Formáty súborov

Validačná služba podporuje formáty definované štandardami uvedenými v ods. 4.3.

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

4.7.2.2. Veľkosť súborov

Veľkosť súboru resp. kontajneru je obmedzená na maximálne 35 MB.

4.7.2.3. Vyhodnotenie podpisu

Validačná služba vyhodnocuje podpisy vytvorené v zmysle nariadenia eIDAS.

4.8 Dostupnosť validačnej služby

Kvalifikovaná validačná služba je štandardne dostupná v režime 365x7x24. Validačná služba môže byť nedostupná počas nevyhnutného času pre správu a údržbu systémov. Jednotlivé podmienky pre dostupnosť služby sú stanovené pre zákazníka zmluvne.

Do započítania dostupnosti služby nemôže byť zahrnutý čas z dôvodu neočakávaných okolností, na ktoré nemal Poskytovateľ žiadny dosah, z dôvodu mimoriadnych okolností na strane Poskytovateľa, ktoré nebolo možné vopred predvídať a rovnako z dôvodu vplyvu vyššej moci.

4.9 Zmluvné podmienky používania Validačnej Služby

Poskytovateľ sprístupní podmienky týkajúce sa svojich služieb všetkým zákazníkom a spoliehajúcim sa stranám.

Zmluvné podmienky používania služby musia v minimálnom rozsahu definovať pre každú politiku dôveryhodných služieb poskytovanú Poskytovateľom nasledovné:

a) politika dôveryhodnej služby bola aplikovaná;

b) akékoľvek obmedzenia týkajúce sa používania služby.

Zákazníci a strany využívajúce dôveryhodnú službu musia byť informovaní o presných podmienkach pred uzavretím zmluvného vzťahu.

Zmluvné podmienky používania Validačnej služby musia byť prístupné v ľahko zrozumiteľnom jazyku.

Zmluvné podmienky používania Validačnej služby sa môžu prenášať aj elektronicky.

5. Ohodnotenie rizík

Pre ohodnotenie rizík platia ustanovenia uvedené v dokumente [3] kapitola 5.

6. Politiky a pravidlá

6.1 Pravidlá pre praktický výkon dôveryhodných služieb

Všeobecné pravidlá pre praktický výkon dôveryhodných služieb sú uvedené v dokumente [3].

6.2 Všeobecné podmienky

Poskytovateľ **zverejňuje všeobecné podmienky validačnej služby na svojom webovom sídle.**

6.3 Politika informačnej bezpečnosti

Politika informačnej bezpečnosti je popísaná v dokumente [5].

6.4 Záväzky Poskytovateľa

6.4.1 Všeobecne

Poskytovateľ validačnej služby sa zaväzuje:

- realizovať všetky požiadavky, kladené na Poskytovateľa v zmysle kapitoly 5, 6, 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 validačnej politike.

6.4.2 Záväzky Poskytovateľa k zákazníkovi

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.

6.5 Informácie pre spoliehajúce sa strany

Všeobecné podmienky, dostupné pre Spoliehajúce sa strany (pozri odstavec 6.2) v prípade, že sa spoliehajú na správu z validácie, musia zahŕňať:

- Povinnosť overenia platnosti podpisu správy z validácie v zmysle príslušných štandardov.
- Všetky obmedzenia pre použitie validačnej služby podľa tejto politiky.
- Všetky ďalšie obmedzenia, uvedené v dohodách alebo kdekoľvek inde.

7. Riadenie a prevádzka

7.1 Vnútorná organizácia

7.1.1 Spoľahlivosť organizácie

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

7.1.2 Delenie povinností

Poskytovateľ má zabezpečené rozdelenie povinností podľa jednotlivých úsekov a v súlade s organizačným poriadkom.

Povinnosti alebo oblasti zodpovednosti, ktoré sú v konflikte, sú oddelené aby sa obmedzili príležitosti pre neautorizovanú alebo neúmyselnú modifikáciu alebo zneužitie aktív Poskytovateľa.

7.2 Ľudské zdroje

Pre ľudské zdroje platia ustanovenia uvedené v dokumente [3] odstavec 7.2.

7.3 Správa aktív

Pre správu aktív platia ustanovenia uvedené v dokumente [3] odstavec 7.3.

7.4 Riadenie prístupu

Pre riadenie prístupu platia ustanovenia uvedené v dokumente [3] odstavec 7.4.

7.5 Kryptografické riadiace prvky

7.5.1 Všeobecne

Vhodné bezpečnostné opatrenia, aplikované na manažment akýchkoľvek kryptografických kľúčov a kryptografických zariadení počas ich životnosti, sú popísané v internej dokumentácii pre prácu s HSM.

7.5.2 Generovanie kľúčov pre VSU

Generovanie kľúčov pre jednotlivé VSU spĺňa nasledovné:

- Je vykonané vo fyzicky bezpečnom prostredí osobami, zaradenými v dôveryhodných rolách, 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.
- Jednotlivé VSU používajú jeden spoločný kľúčový pár s certifikátom na autorizáciu správ z validácie.

7.5.3 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.

7.5.4 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 kvalifikovaným poskytovateľom dôveryhodnej služby vyhotovovania a overovania kvalifikovaných certifikátov pre podpis/pečať.
- VSU nevytvorí správu z validácie pred tým ako jej certifikát verejného kľúča pre overenie autorizácie je načítaný v kryptografickom zariadení VSU.

7.5.5 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.

7.5.6 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.
- Súkromné autorizačné kľúče VSU, uložené v kryptografickom module VSU, sú v prípade vyradenia modulu vymazané takým spôsobom, že je prakticky nemožné ich obnovenie.

7.5.7 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“ zo štandardu ETSI TS 119 312 [6].

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 národného dôveryhodného zoznamu.

7.6 Fyzická a objektová bezpečnosť

Pre ľudské zdroje platia ustanovenia uvedené v dokumente [3] odstavec 7.6.

7.7 Prevádzková bezpečnosť

Pre prevádzkovú bezpečnosť platia ustanovenia, uvedené v dokumente [3], odstavec 7.7 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.

7.8 Sieťová bezpečnosť

Pre sieťovú bezpečnosť platia pre Poskytovateľa ustanovenia, uvedené v dokumente [3], odstavec 7.8 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.

7.9 Riadenie bezpečnostných incidentov

Pre riadenie bezpečnostných incidentov platia ustanovenia, uvedené v dokumente [3], odstavec 7.9.

7.10 Zber dôkazov

Pre zber dôkazov platia ustanovenia, uvedené v dokumente [3], odstavec 7.10 a ďalej musia byť zaznamenávané všetky udalosti týkajúce sa:

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

7.11 Riadenie kontinuity činností organizácie

Pre riadenie kontinuity činnosti organizácie platia ustanovenia, uvedené v dokumente [3], odstavec 7.11 a naviac je potrebné zabezpečiť nasledovné:

- Plán obnovy po pohrome [7] 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 zákazníkom a spoliehajúcim sa stranám popis kompromitácie jej zverejnením v úložisku Poskytovateľa (kap. 2.1).
- 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 zákazníkom 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.

7.12 Ukončenie činnosti Poskytovateľa a plány ukončenia činnosti

Pre ukončenie činnosti Poskytovateľa platia ustanovenia, uvedené v dokumente [3], odstavec 7.12 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.

7.13 Zhoda a právne požiadavky

Pre zhodu a právne požiadavky platia ustanovenia, uvedené v dokumente [3], odstavec 7.1 a naviac Poskytovateľ musí poskytovať svoje služby nasledovne:

a) Prijal vhodné technické a organizačné opatrenia proti neautorizovanému alebo protiprávnemu spracovávaniu osobných údajov a proti strate, zničeniu alebo poškodeniu osobných údajov.

b) Poskytovateľ Služby validácie validovaný dokument po spracovaní neuchováva.

c) Poskytovateľ nesie celkovú zodpovednosť za splnenie požiadaviek definovaných v kapitolách 5 až 8, a to aj keď niektoré alebo všetky jeho funkcie sú využívané subdodávateľmi.

8. Technické požiadavky

8.1 Proces overenia podpisu

Proces validácie vydá indikáciu stavu overenia podpisu, jeden na každý overený podpis, a taktiež správu z validácie podpisu.

Validačný proces pozostáva z postupnosti jednotlivých krokov, ktorými sa určí, či:

a) certifikát, ktorý potvrdzuje podpis, bol v čase podpísania kvalifikovaným certifikátom pre elektronický podpis v súlade s prílohou I;

b) kvalifikovaný certifikát vydal kvalifikovaný poskytovateľ dôveryhodných služieb a v čase podpísania bol platný;

c) údaje na validáciu podpisu zodpovedajú údajom poskytnutým spoliehajúcej sa strane;

d) sa jedinečný súbor údajov reprezentujúcich podpisovateľa v certifikáte správne poskytol spoliehajúcej sa strane;

e) sa použitie pseudonymu jasne oznámilo spoliehajúcej sa strane v prípade, že sa v čase podpísania použil pseudonym;

f) bol elektronický podpis vyhotovený kvalifikovaným zariadením na vyhotovenie elektronického podpisu;

g) nebola narušená integrita podpísaných údajov;

h) boli splnené požiadavky na zdokonalený elektronický podpis uvedené v čl. 26 nariadenia eIDAS.

8.2 Rozhrania

8.2.1 Komunikačný kanál

Komunikačný kanál medzi klientom a Poskytovateľom musí byť zabezpečený t. j. Poskytovateľ ponúkne a zabezpečí spôsob autentifikácie klienta a zabezpečí dôvernosť údajov.

8.3 Správa z Validácie

Ako výstup z dôveryhodnej Služby validácie kvalifikovaných podpisov a pečatí slúži validačná správa.

Služba Validácie vytvorí správu z validácie s technickými podrobnosťami validácie každého z uplatniteľných obmedzení.

Toto ustanovenie špecifikuje minimálne požiadavky na obsah takejto správy. Ak je zapojený ľudský používateľ, Riadiaca aplikácia musí byť schopná predložiť správu spôsobom, ktorý je pre používateľa zmysluplný a zrozumiteľný.

Údaje vrátené Validačnou Aplikáciou musia vyhovovať týmto pravidlám:

a) Keď sa výsledok overenia podpisu vráti ako PLATNÝ:

- Celkový výsledok validácie môže byť PLATNÝ (Úplné overenie) - Podpis bolo možné plne overiť a bol vyhodnotený ako platný.
- Celkový výsledok validácie môže byť PLATNÝ (Čiastočne overenie) - Podpis bol štrukturálne overený ako platný, no zatiaľ nebolo možné plne overiť platnosť všetkých certifikátov, napr. kvôli neaktuálnym údajom o zrušení certifikátov. Po nejakom krátkom čase (typicky pár hodín) bude možné podpis plne overiť ako Platný alebo Neplatný.

b) Keď sa výsledok overenia podpisu vráti ako NEPLATNÝ - Podpis bol overený a je preukázateľné, že je neplatný. Dôvodov môže byť viacero, napr. že bol zmenený obsah dokumentu, podpis bol vytvorený po zrušení certifikátu podpisovateľa a pod.

c) Keď sa výsledok overenia podpisu vráti ako NEROZHODNUTÝ - Proces overenia použil všetky dostupné údaje, ale napriek tomu nebolo možné jednoznačne automaticky rozhodnúť o platnosti podpisu. Dôvodov môže byť viacero, napr. že niektoré údaje sú dočasne nedostupné, alebo vypršala platnosť podpisového certifikátu a podpis neobsahuje platnú časovú pečiatku.

V správe z validácie podpisu sa uvedie každé z obmedzení validácie, ktoré sa spracúva, vrátane akéhokoľvek obmedzenia platnosti, ktoré implementácia implicitne uplatnila.

Keď je Poskytovateľ schopný overiť podpisy na základe dobre identifikovanej politiky overovania podpisu, správa o overení podpisu môže niesť identifikátor politiky overovania podpisu.

V správe z validácie sa uvedie typ podpisu.

Ak politika overovania podpisu nie je úplne spracovaná Službou Validácie, správa okrem správ o overených obmedzeniach by mala hlásiť obmedzenia, ktoré boli ignorované alebo prepísané.

Správa z validácie podpisu musí obsahovať identifikáciu podpisujúceho.

V správe z validácie sa uvedie, či je k dispozícii časová pečiatka podpisu.

Správa z validácie je autorizovaná zdokonalenou elektronickou pečaťou Poskytovateľa s kvalifikovanou časovou pečiatkou.

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

9.1 Požiadavky schémy dohľadu

Schéma dohľadu (ďalej aj ako „SD“) definuje požiadavky na službu validácie kvalifikovaných elektronických podpisov a pečatí v kapitolách:

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

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

9.2 Plnenie požiadaviek eIDAS

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

9.2.1 Plnenie požiadaviek z kapitoly 5.1 SD

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 Disig, a.s. [3], ktorý popisuje všeobecné pravidlá pri poskytovaní dôveryhodných služieb.

9.2.2 Plnenie požiadavky z kapitoly 5.3 SD

Požiadavky, uvedené v kapitole 5.3 Schémy dohľadu, definujú povinné a nepovinné výstupné charakteristiky validačnej služby.

Služba je realizovaná ako webová služba, ktorá prostredníctvom svojho rozhrania umožňuje nahrať dokument, ktorý následne validačná služba overuje.

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

- CAdES - ETSI TS 103173 v.2.2.1,
- PAdES - ETSI TS 103172 v.2.2.2,

- XAdES - ETSI TS 103171 v.2.1.1,
- ASiC - ETSI TS 103174 v.2.2.1

a vykonáva overenie platnosti podpisov/pečatí, vytvorených podľa týchto štandardov, pomocou konceptov a pravidiel zo štandardu verifikácie podpisov ETSI EN 319 102-1.

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“ .

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 SD 5.3, 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.

9.3 Certifikát verejného kľúča VSU a zdroj kvalifikovaných pečiatok

V zmysle SD je správa z validácie autorizovaná zdokonalenou elektronickou pečaťou validačnej služby, spolu s kvalifikovanou elektronickou časovou pečiatkou. Certifikát pre pečať je vydaný Poskytovateľom a kvalifikovaná elektronická časová pečiatka je vydaná TSA autoritou Poskytovateľa.

10. 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. Schéma dohľadu kvalifikovaných dôveryhodných služieb definovaná orgánom dohľadu, Národný bezpečnostný úrad.

3. Politika poskytovania dôveryhodných služieb Disig, a.s.

4. ETSI TS 119615 : Electronic Signatures and Infrastructures (ESI); Trusted lists; Procedures for using and interpreting European Union Member States national trusted lists.

5. Bezpečnostná politika Disig, a.s.

6. Electronic Signatures and Infrastructures (ESI); Cryptographic Suites. ETSI TS 119 312.

7. Bezpečnostný projekt na ochranu osobných údajov držiteľov certifikátov: Postupy zaručenia kontinuity pri havárii alebo inej mimoriadnej udalosti Disig, a.s.

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

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

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

11. NBÚ SR. Schéma dohľadu kvalifikovaných dôveryhodných služieb definovaná orgánom dohľadu. s.l. : NBÚ SR, 2017. 1.3. 1353/2017/IBEP/OA-006.

12. ISO32000. Document management - Portable document format. [Online] http://www.adobe.com/content/dam/Adobe/en/devnet/acrobat/pdfs/PDF32000_2008.pdf. ISO 32000:2008.

13. 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.

14. Electronic Signatures and Infrastructures (ESI); PAdES Baseline Profile. [Online] http://www.etsi.org/deliver/etsi_ts/103100_103199/103172/02.02.02_60/ts_103172v020202p.pdf. ETSI TS 103 172 V2.2.2.

15. Electronic Signatures and Infrastructures (ESI); CAdES Baseline Profile. [Online] http://www.etsi.org/deliver/etsi_ts/103100_103199/103173/02.02.01_60/ts_103173v020201p.pdf. ETSI TS 103173 v.2.2.1.

16. 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.

17. Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation. [Online] https://www.etsi.org/deliver/etsi_en/319100_319199/31910201/01.03.01_60/en_31910201v010301p.pdf . ETSI EN 319 102-1 V1.3.1.

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

19. Electronic Signatures and Infrastructures (ESI); Policy requirements for TSP providing signature validation services. [Online] https://www.etsi.org/deliver/etsi_ts/119400_119499/119441/01.01.01_60/ts_119441v010101p.pdf. ETSI TS 119 441.

História zmien

Verzia	Dátum	Popis revízie; revidoval
0.2	18.5.2017	Prvá verzia dokumentu; Ondriska
1.0	30.9.2022	aktualizácia textu; Nigut