# Certifikačná Politika (CP) poskytovania kvalifikovanej dôveryhodnej služby validácie kvalifikovaných elektronických podpisov a pečatí (QESV)

Verzia: **1.0**

Dátum účinnosti: 1.7.2024

**PO-01**

Politika

**Verejné**


**Vytvoril:**

Ing. Martin Berzák
Bezpečnostný manažér

1.7.2024

**Schválil:**

Ing. Eduard Baraniak
Konateľ brainit.sk, s. r. o.

1.7.2024

**brainit.sk, s. r. o.**

Veľký Diel 3323, 010 08 Žilina
IČO: 52577465

*www.brainit.sk*

## História zmien

| Verzia | Dátum | Autori | Popis | Dôvod zmien |
|---|---|---|---|---|
| 1.0 | 1.7.2024 | Ing. Martin Berzák<br>Ing. Michal Šterbák | Prvá schválená verzia dokumentu | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

## OBSAH

**Definície a skratky ..... 7**
**1 Úvod ..... 9**
*1.1 Prehľad ..... 9*
**2 Názov a identifikácia dokumentu ..... 10**
*2.1 Účastníci PKI ..... 10*
2.1.1 Poskytovateľ (Jednotka validačnej služby - VSU) ..... 11
2.1.2 Zákazník ..... 11
2.1.3 Spoliehajúca sa strana ..... 11
2.1.4 Ostatní účastníci ..... 11
*2.2 Použiteľnosť správy z validácie ..... 12*
*2.3 Správa politiky ..... 12*
2.3.1 Informácie o poskytovateľovi a jeho kontaktné údaje ..... 12
2.3.2 Uplatniteľnosť dokumentácie ..... 13
**3 Zverejnenie a zodpovednosť za uloženie údajov ..... 14**
*3.1 Úložiská ..... 14*
*3.2 Zverejnenie informácií o validačnej službe ..... 14*
*3.3 Čas a frekvencia zverejňovania informácií ..... 14*
*3.4 Kontroly prístupu k úložiskám ..... 14*
**4 Identifikácia a autentifikácia ..... 15**
*4.1 Počiatočné overenie totožnosti ..... 15*
*4.2 Autentifikácia k validačnej službe ..... 15*
*4.3 Ukončenie využívania validačnej služby ..... 15*
*4.4 Riadenie používateľských účtov ..... 15*
**5 Všeobecné ustanovenia ..... 16**
*5.1 Všeobecné ustanovenia politiky ..... 16*
*5.2 Služby súvisiace s kvalifikovanou validačnou službou ..... 16*
*5.3 Poskytovateľ validačnej služby ..... 16*
*5.4 Používateľ validačnej služby ..... 16*
**6 Kvalifikovaná validačná služba ..... 17**
*6.1 Opis validačnej služby ..... 17*
*6.2 Overenie informácií v LoTL ..... 17*
*6.3 Kontrola formátu podpisu a technické parametre kvalifikovanej validačnej služby ..... 18*
6.3.1 Kontrola a overovanie základných profilov ..... 18
6.3.2 Overované certifikáty ..... 18
6.3.3 Kontrola a overovanie formátov podpisov a pečatí ..... 18
*6.4 Validačný proces ..... 18*
6.4.1 Požiadavky na proces overovania podpisov/pečatí ..... 19
6.4.2 Model overovania podpisov ..... 20
*6.5 Komunikačný kanál ..... 20*

*6.6 Výsledok validačného procesu ... 20*
*6.7 Výstup validačného procesu ... 27*
6.7.1 Štruktúrované XML súbory ... 27
6.7.2 PDF dokument ... 27
*6.8 Vymedzenie služby a obmedzenia ... 28*
6.8.1 Vymedzenie validačnej služby ... 28
6.8.2 Obmedzenia validačnej služby ... 28
*6.9 Dostupnosť validačnej služby ... 28*
*6.10 Uchovávanie informácií pre overovanie platnosti elektronických podpisov a pečatí ... 28*
*6.11 Zmluvné podmienky používania validačnej služby ... 28*
**7 Ohodnotenie rizík ... 30**
**8 Politiky a pravidlá ... 31**
*8.1 Pravidlá pre praktický výkon dôveryhodných služieb ... 31*
*8.2 Všeobecné podmienky ... 31*
*8.3 Politika informačnej bezpečnosti ... 31*
*8.4 Záväzky Poskytovateľa ... 31*
8.4.1 Všeobecne ... 31
8.4.2 Záväzky Poskytovateľa k Zákazníkovi ... 31
*8.5 Informácie pre spoliehajúce sa strany ... 31*
**9 Riadenie, prevádzka a fyzická bezpečnosť ... 32**
*9.1 Fyzická bezpečnosť ... 32*
9.1.1 Priestory ... 32
9.1.2 Fyzický prístup ... 32
9.1.3 Napájanie a klimatizácia ... 33
9.1.4 Ochrana pred vodou ... 33
9.1.5 Prevencia a ochrana proti požiaru ... 33
9.1.6 Úložisko médií ... 33
9.1.7 Likvidácia odpadu ... 33
9.1.8 Zálohovanie mimo hlavnú lokalitu ... 33
9.1.9 Delenie povinností ... 33
*9.2 Procesná bezpečnosť, ľudské zdroje ... 33*
9.2.1 Dôveryhodné role ... 33
9.2.2 Počet osôb požadovaných pre zaistenie jednotlivých činností ... 33
9.2.3 Identifikácia a autentifikácia pre každú rolu ... 34
9.2.4 Role vyžadujúce rozdelenie zodpovednosti ... 34
*9.3 Personálne bezpečnostné opatrenia ... 34*
9.3.1 Požiadavky na kvalifikáciu, skúsenosti a previerky ... 34
9.3.2 Požiadavky previerky ... 34
9.3.3 Požiadavky na školenie ... 35
9.3.4 Frekvencia obnovy školení ... 35

9.3.5 Frekvencia rotácie rolí ..... 35
9.3.6 Sankcie za neoprávnené konanie ..... 35
9.3.7 Požiadavky na externých dodávateľov ..... 35
9.3.8 Dokumentácia poskytnutá zamestnancom ..... 35
*9.4 Kryptografické riadiace prvky ..... 35*
9.4.1 Všeobecne ..... 35
9.4.2 Generovanie kľúčov pre VSU ..... 36
9.4.3 Ochrana súkromného kľúča VSU ..... 36
9.4.4 Certifikát verejného kľúča VSU ..... 36
9.4.5 Prepísanie kľúča VSU ..... 36
9.4.6 Riadenie životného cyklu podpisového kryptografického hardvéru ..... 36
9.4.7 Ukončenie životného cyklu kľúča VSU ..... 37
*9.5 Prevádzková bezpečnosť ..... 37*
*9.6 Sieťová bezpečnosť ..... 37*
*9.7 Riadenie bezpečnostných incidentov ..... 37*
*9.8 Postupy získavania auditných záznamov (logov) ..... 37*
9.8.1 Typy zaznamenaných udalostí ..... 38
9.8.2 Frekvencia spracovania auditných záznamov ..... 38
9.8.3 Lehota uchovania protokolu auditu ..... 38
9.8.4 Ochrana auditných záznamov ..... 38
9.8.5 Postupy zálohovania protokolu auditu ..... 38
9.8.6 Systém zhromažďovania auditov (interný vs. externý) ..... 38
9.8.7 Oznámenie subjektu iniciujúceho audit ..... 38
9.8.8 Posúdenie zraniteľnosti ..... 38
*9.9 Uchovávanie informácií a dokumentácie ..... 39*
9.9.1 Typy uchovávaných informácií a dokumentácie ..... 39
9.9.2 Lehota uchovania uchovávaných informácií a dokumentácie ..... 39
9.9.3 Ochrana úložiska uchovávaných informácií a dokumentácie ..... 39
9.9.4 Postupy zálohovania uchovávaných informácií a dokumentácie ..... 39
9.9.5 Požiadavky na používanie časových pečiatok pri uchovávaní informácií a dokumentácie ..... 39
9.9.6 Postupy na získanie a overenie uchovávaných informácií a dokumentácie ..... 39
*9.10 Obnova po kompromitácií a katastrofe ..... 39*
9.10.1 Postupy pri riešení kompromitácie a katastrof ..... 40
9.10.2 Poškodenie výpočtových prostriedkov, softvéru alebo dát ..... 40
9.10.3 Zachovanie kontinuity činnosti po katastrofe ..... 40
*9.11 Ukončenie činnosti CA alebo RA ..... 40*
*9.12 Zhoda a právne požiadavky ..... 41*
**10 Technické bezpečnostné opatrenia ..... 42**
*10.1 Bezpečnosť životného cyklu ..... 42*
10.1.1 Riadenie vývoja softvéru ..... 42

10.1.2 Kontroly riadenia bezpečnosti ..... 42
10.1.3 Riadenie bezpečnosti životného cyklu ..... 42
**11 Audit súladu a ďalšie hodnotenia ..... 43**
*11.1 Frekvencia alebo okolnosti posudzovania ..... 43*
*11.2 Totožnosť a kvalifikácia posudzovateľa ..... 43*
*11.3 Vzťah hodnotiteľa k hodnotenému subjektu ..... 43*
*11.4 Hodnotené oblasti ..... 43*
*11.5 Opatrenia prijaté v dôsledku nedostatku ..... 43*
*11.6 Postup v prípade zistených nedostatkov ..... 43*
*11.7 Oznámenie výsledkov ..... 44*
**12 Plnenie požiadaviek pre kvalifikovanú validačnú službu kvalifikovaných elektronických podpisov a pečatí podľa nariadenia eIDAS ..... 44**
*12.1 Požiadavky schémy dohľadu ..... 44*
*12.2 Plnenie požiadaviek eIDAS ..... 44*
12.2.1 Plnenie požiadaviek z kapitoly 5.1 SD ..... 44
12.2.2 Plnenie požiadaviek z kapitoly 5.3 SD ..... 44
*12.3 Certifikát verejného kľúča VSU a zdroj kvalifikovaných pečiatok ..... 45*
**13 Odkazy ..... 46**

## Definície a skratky

Na účely tohto dokumentu sú použité nasledujúce termíny a definície:

**Jednotka validačnej služby** – Politika poskytovania kvalifikovanej dôveryhodnej služby validácie kvalifikovaných elektronických podpisov/pečatí.

**Poskytovateľ** – spoločnosť brainit.sk, s.r.o., ktorá ponúka Zákazníkom kvalifikované dôveryhodné služby validácie kvalifikovaných elektronických podpisov/pečatí.

**Zákazník** – Odoberateľ kvalifikovaných dôveryhodných služieb poskytovaných Poskytovateľom.

**Poskytovateľ dôveryhodnej služby (TSP)** – entita, ktorá poskytuje jednu alebo viac dôveryhodných služieb.

**Systém validácie (QESV)** – zostava IT produktov a komponentov zorganizovaných na podporu poskytovanie služby validácie kvalifikovaných elektronických podpisov/pečatí.

Na účely tohto dokumentu sú použité nasledujúce skratky:

- **CA** – Certifikačná autorita, autorita vybavujúca
- **CP** – Certifikačná politika
- **CPS** – Pravidlá pre výkon certifikačných činností
- **PKI** – Infraštruktúra verejných kľúčov (Public Key Infrastructure)
- **RA** – Registračná autorita
- **QES** – Kvalifikovaný elektronický podpis
- **QES-S** – Kvalifikovaná elektronická pečať
- **KC** – Kvalifikovaný certifikát
- **CRL** – Zoznam zrušených certifikátov (Certification Revocation List)
- **OCSP** – Online Certificate Status Protocol
- **LoTL** – List of Trusted List
- **TSP** – Trust Service Provides (Dôveryhodný poskytovateľ služieb)
- **FO** – Fyzická osoba
- **PO** – Právnická osoba
- **IT** – Informačná technológia
- **TSA** – Autorita časovej pečiatky
- **VSU** – Samostatná jednotka vytvárajúca správu z validácie (Validation Service Unit)
- **QSCD** – Kvalifikované zariadenie na vyhotovovanie elektronického podpisu/pečate
- **PoE** – Dôkaz Existencie (Proof of Existence)
- **QES** – Kvalifikovaný elektronický podpis/pečať
- **QSVSP** – Kvalifikovaný poskytovateľ služby validácie podpisu/pečate (Qualified Signature/Seal Validation Service Provider)
- **SD** – Podpísaný dokument (Signed 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)

# 1 Úvod

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

Poskytovateľom tejto dôveryhodnej služby je:

**Názov spoločnosti:** brainit.sk s. r. o.

**Sídlo spoločnosti:** Veľký Diel 3323, Žilina 010 08

**IČO:** 52577465

**Webové sídlo:** https://nfqes.sk / www.nfqes.com

zapísaná v Obchodnom registri Okresného súdu Žilina, oddiel: Sro, vložka č. 72902/L (ďalej iba „Poskytovateľ“), prostredníctvom svojho systému validačnej služby.

Táto CP je záväzným dokumentom, ktorého ustanovenia musia dodržiavať všetky zúčastnené strany. CP môže byť použitý nezávislými orgánmi na posudzovanie zhody, ako základ pre potvrdenie, že Poskytovateľ je kvalifikovaným poskytovateľom na prevádzkovanie validačnej služby kvalifikovaných elektronických podpisov a pečatí.

Základný rámec pre poskytovanie kvalifikovaných dôveryhodných služieb tvoria:

- 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 (ďalej môže byť uvádzané ako „nariadenie eIDAS“).
- Zákon č. 272/2016 Z. z. z 20. septembra 2016 o dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zmene a doplnení niektorých zákonov (zákon o dôveryhodných službách).
- Schéma dohľadu kvalifikovaných dôveryhodných služieb definovaná orgánom dohľadu - NBÚ SR.

## 1.1 Prehľad

Táto CP definuje pravidlá pre poskytovanie kvalifikovaných dôveryhodných služieb (alebo Signature Validation Service (ďalej môže byť uvádzané ako „SVS“) v zmysle ustanovení nariadenia eIDAS:

- **Kvalifikovaná dôveryhodná služba validácie kvalifikovaných elektronických podpisov**
- **Kvalifikovaná dôveryhodná služba validácie kvalifikovaných elektronických pečatí**

***Verzia dokumentu:*** *1.0*

***Dátum účinnosti:*** *1.7.2024*

***Názov dokumentu:*** Certifikačná politika poskytovania kvalifikovanej dôveryhodnej služby validácie kvalifikovaných elektronických podpisov a pečatí

# 2 Názov a identifikácia dokumentu

Politika poskytovania kvalifikovanej dôveryhodnej služby validácie kvalifikovaných elektronických podpisov a validácie kvalifikovaných elektronických pečatí je identifikovaná objektovým identifikátorom OID 1.3.158.52577465.0.0.0.1.7.1, kde jednotlivé zložky OID majú nasledovný význam:

- **1** ISO
- **3** ISO Identified Organization
- **158** Slovakia
- **52577465** jedinečný identifikátor firmy brainit.sk s.r.o. (IČO)
- **0.0.0.1** CA NFQES
- **7** Dokument „Certifikačná politika poskytovania kvalifikovanej dôveryhodnej služby validácie kvalifikovaných elektronických podpisov a validácie kvalifikovaných elektronických pečatí“
- **1** major verzia dokumentu

Validačné politiky na základe ktorých prebieha validačný proces a ktoré sú súčasťou tohto dokumentu v Prílohe A a Prílohe B sú označované podobne ako CP a CPS, s tým rozdielom, že za verziou dokumentu je ďalšie označujúce číslo, ktoré určuje validačnú politiku nasledovne:

**QES validačná politika**

- **1** ISO
- **3** ISO Identified Organization
- **158** Slovakia
- **52577465** jedinečný identifikátor firmy brainit.sk s.r.o. (IČO)
- **0.0.0.1** CA NFQES
- **7** Dokument „Certifikačná politika poskytovania kvalifikovanej dôveryhodnej služby validácie kvalifikovaných elektronických podpisov a validácie kvalifikovaných elektronických pečatí“
- **1** major verzia dokumentu
- **1** validačná politika pre kvalifikované overovanie (QES validation policy)

**AdES validačná politika**

- **1** ISO
- **3** ISO Identified Organization
- **158** Slovakia
- **52577465** jedinečný identifikátor firmy brainit.sk s.r.o. (IČO)
- **0.0.0.1** CA NFQES
- **7** Dokument „Certifikačná politika poskytovania kvalifikovanej dôveryhodnej služby validácie kvalifikovaných elektronických podpisov a validácie kvalifikovaných elektronických pečatí“
- **1** major verzia dokumentu
- **2** validačná politika pre pokročilé overovanie (AdES validation policy)

## 2.1 Účastníci PKI

Táto kapitola popisuje totožnosť alebo typy entít, ktoré plnia úlohy účastníkov v rámci kvalifikovanej validačnej služby. V rámci poskytovania validačnej služby, sú účastníkmi infraštruktúry verejného kľúča entity uvedené v tejto časti.

### *2.1.1 Poskytovateľ (Jednotka validačnej služby - VSU)*

Poskytovateľ je zodpovedný za poskytovanie dôveryhodných služieb, ktorých sa táto CP týka podľa ustanovení uvedených v tejto CP. Poskytovateľ môže byť označený aj ako Signature Validation Service Provider (SVSP). SVSP má celkovú zodpovednosť za splnenie požiadaviek definovaných v danej CP ako aj v ETSI TS 119 441 V1.1. v odsekoch 5 až 8.

Poskytovateľ:

- je entita, ktorá poskytuje kvalifikovanú dôveryhodnú službu validácie kvalifikovaných elektronických podpisov a kvalifikovaných elektronických pečatí koncovým používateľom (Zákazníci, Spoliehajúce sa strany),
- má celkovú zodpovednosť za poskytovanie kvalifikovaných dôveryhodných služieb špecifikovaných v kapitole 1.1,
- je uvádzaná vo vytvorených výsledných správach z validačnej služby ako ich vydavateľ a jej súkromné kľúče sú používané pri autorizácii tejto správy, a to vyhotovovaním kvalifikovanej pečate na zabezpečenie originality a integrity týchto správ,
- zaručuje, že všetky aspekty jej služieb, operácií a infraštruktúry, zviazanej s výslednými správami z validačnej služby, vydanými podľa tejto CP, sú vykonávané v súlade s jej požiadavkami a ustanoveniami a v súlade s pravidlami poskytovania dôveryhodných služieb Poskytovateľa.

Poskytovateľ môže prevádzkovať viaceré VSU (napr. prostredníctvom externých RA) poskytujúce dôveryhodné validačné služby.

### *2.1.2 Zákazník*

Zákazníkom sa rozumie FO alebo PO, ktorej Poskytovateľ poskytuje validačnú službu a ten využíva validačné služby Poskytovateľa podľa tejto CP a viažu sa na neho záväzky zákazníka.

Ak je Zákazníkom PO, tá môže zahŕňať niekoľko koncových používateľov alebo jediného koncového používateľa. Niektoré povinnosti, ktoré sa vzťahujú na túto PO, sa zároveň vzťahujú aj na týchto koncových používateľov. V každom prípade, PO je plne zodpovedná, ak povinnosti dané touto CP nie sú zo strany koncových používateľov správne a riadne splnené, a preto je takáto PO zodpovedná za vhodnú informovanosť svojich koncových používateľov.

V prípade, že je Zákazník zároveň koncovým používateľom, je priamo zodpovedný za neplnenie svojich povinností v zmysle tejto CP. Všetky podmienky, ktoré musí Zákazník dodržiavať a spĺňať, definuje táto CP.

### *2.1.3 Spoliehajúca sa strana*

Spoliehajúcou sa stranou je FO alebo PO, ktorá sa pri svojom konaní spolieha na výslednú správu z validačnej služby.

### *2.1.4 Ostatní účastníci*

**Policy Management Authority**

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

- dohľadu nad vytváraním a aktualizáciou CP, vrátane vyhodnocovania zmien a plánov na implementovanie ľubovoľných prijatých zmien,
- revízie CPS, aby sa zaručilo, že prax Poskytovateľa vyhovuje príslušnej CP,

- revízie výsledkov auditov, aby sa určilo, či Poskytovateľ zodpovedne dodržiava ustanovenia vydaných CP a CPS,
- vydávania odporúčaní pre Poskytovateľa týkajúcich sa nápravných a iných vhodných opatrení,
- riadenia a usmerňovania činnosti Poskytovateľa a RA,
- 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.

**Poskytovatelia iných služieb**

Medzi poskytovateľov iných služieb patria:

- Autorita poskytujúca služby vyhotovovania kvalifikovaných elektronických časových pečiatok,
    - *(pre potreby tejto služby si Poskytovateľ môže vydať kvalifikované elektronické časové pečiatky sám vlastnou CA)*
- Entita poskytujúca službu publikovania dôveryhodných zoznamov kvalifikovaných poskytovateľov dôveryhodných služieb (LoLT),
- Entita, ktorá poskytuje služby súvisiace so štatútom platnosti KC, ktoré sú predmetom validácie (CRL, OCSP responder).

**Iní účastníci**

- Dôveryhodný Poskytovatelia (TSP), ktorý sú vo vzťahu k podpisovateľovi pečate
    - TSP, ktorý je vydavateľom jeho certifikátu
    - akýkoľvek TSP, ktorý sa nejakým spôsobom podieľa na generovaní podpisu/pečate
    - TSP spravujúci QSCD v mene podpisovateľa pečate
    - TSP poskytujúci služby použitých časových pečiatok
- Poskytovatelia dôveryhodných zoznamov členských štátov EÚ
- Európska komisia poskytujúca zoznam dôveryhodných zoznamov

Participácia ďalších účastníkov je vymedzená platnými právnymi predpismi (orgán dohľadu, orgány činné v trestnom konaní a podobne).

## 2.2 Použiteľnosť správy z validácie

Výslednú správu z validácie vyhotovenú v zmysle požiadaviek tejto CP je možné použiť všade, kde je vyžadovaná správa z validácie definovaná v článkoch 32 a 40 Nariadenia eIDAS.

## 2.3 Správa politiky

### *2.3.1 Informácie o poskytovateľovi a jeho kontaktné údaje*

Nasledujúce informácie poskytujú údaje Poskytovateľa, ktorý je zodpovedný za prípravu, vytvorenie a udržiavanie tohto dokumentu.

***Názov:*** brainit.sk, s. r. o.

***Sídlo:*** Veľký Diel 3323, 010 08 Žilina

***IČO:*** 52577465

***DIČ:*** 2121068763

***IČ DPH:*** SK2121068763

***Register:*** Obchodný register okresného súdu Žilina, oddiel Sro, vložka číslo 72902/L

Na účel tvorby politík má Poskytovateľ vytvorenú samostatnú autoritu pre správu politík (PMA), ktorá plne zodpovedá za jej obsah a ktorá je pripravená odpovedať na všetky otázky týkajúce sa politík Poskytovateľa. Osobou, ktorá je zodpovedná za rozhodovanie o súlade postupov Poskytovateľa, ktoré sú uvedené v tejto CP je osoba menovaná do roly PMA v zmysle interných predpisov a postupov (viď. kapitola 2.1.4).

**Kontakt:**

*Mobil:* +421 918 022 030

*E-mail:* info@brainit.sk

*Webové sídlo Poskytovateľa:* https://nfqes.sk / https://nfqes.com

*Webové sídlo k Dôveryhodným službám:* https://zone.nfqes.sk

### *2.3.2 Uplatniteľnosť dokumentácie*

Poskytovateľ musí mať schválenú svoju CP a príslušnú CPS ešte pred začiatkom poskytovania dôveryhodných služieb a musí spĺňať všetky požiadavky uvádzané v týchto dokumentoch. Obsah dokumentov CP a CPS schvaľuje osoba menovaná do role PMA.

Po schválení zo strany PMA je potrebné zabezpečiť, aby bol príslušný dokument publikovaný v súlade s publikačnou a oznamovacou politikou. PMA musí informovať o svojich rozhodnutiach takým spôsobom, aby boli tieto informácie vhodne prístupné zákazníkom a spoliehajúcim sa stranám.

# 3 Zverejnenie a zodpovednosť za uloženie údajov

## 3.1 Úložiská

Úložiská musia byť umiestnené tak, aby boli prístupné Zákazníkom a v súlade s celkovými bezpečnostnými požiadavkami. Webové sídlo Poskytovateľa pre kvalifikovanú validačnú službu bude zastávať funkciu úložiska. Presná URL adresa je uvedená v kapitole 2.3.1. Webové sídlo Poskytovateľa musí byť verejne dostupné prostredníctvom internetu Zákazníkom, Spoliehajúcim sa stranám a celkovo verejnosti. Všetky verejne dostupné informácie uvedené na webovom sídle Poskytovateľa majú charakter riadeného prístupu.

## 3.2 Zverejnenie informácií o validačnej službe

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

- túto CP,
- VP používania,
- aktuálne stavy všetkých Európskych TSP využívaných pri činnosti validačnej služby,
- certifikáty jednotlivých validačných jednotiek Poskytovateľa, ktoré patria k jej verejným kľúčom a príslušné súkromné kľúče k nim sú využívané pri pečatení výsledných správ z validačnej služby.

Okrem vyššie spomenutého, Poskytovateľ musí zverejňovať v on-line režime prostredníctvom svojho webového sídla aj ďalšie verejné dokumenty súvisiace s poskytovaním dôveryhodných služieb v zmysle tejto CP.

## 3.3 Čas a frekvencia zverejňovania informácií

Poskytovateľ musí zverejňovať informácie určené na zverejnenie v zmysle nariadenia eIDAS a zákona č. 272/2016 Z. z., pričom tieto informácie sú aktualizované bezodkladne po každej zmene.

CP, CPS, VP a/alebo ich revízie Poskytovateľ musí zverejniť čo najskôr po ich schválení a vydaní.

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

## 3.4 Kontroly prístupu k úložiskám

Všetky verejne dostupné informácie na webovom sídle Poskytovateľa by mali byť prístupné v režime iba na čítanie. Poskytovateľ musí chrániť každú informáciu uloženú v úložisku, ktorá nie je určená na verejné rozšírenie. Poskytovateľ musí vynaložiť maximálne úsilie na to, aby zaistil dôvernosť, integritu a dostupnosť dát vyplývajúcich z poskytovaných dôveryhodných služieb. Taktiež musí vykonať logické a bezpečnostné opatrenia, aby zabránil neautorizovanému prístupu k úložisku osobám, ktoré by mohli akýmkoľvek spôsobom poškodiť, zmeniť, pridať resp. vymazať údaje uložené v úložisku.

# 4 Identifikácia a autentifikácia

## 4.1 Počiatočné overenie totožnosti

Validačná služba bude dostupná iba pre Zákazníkov, Používateľov, Spoliehajúce sa strany a subjekty, ktorí/é už sú overené/í a identifikované/í pre potreby využívania validačnej služby.

## 4.2 Autentifikácia k validačnej službe

Autentifikácia k validačnej službe musí byť zabezpečená a možná iba prostredníctvom rozhrania služby prevádzkovaného Poskytovateľom pomocou pridelených autentifikačných prihlasovacích údajov.

## 4.3 Ukončenie využívania validačnej služby

V prípade nedodržania podmienok pre využívanie validačnej služby definovaných v tejto CP je Poskytovateľ oprávnený pozastaviť prístup používateľa k validačnej službe. V prípade závažných pochybení je Poskytovateľ oprávnený ukončiť používateľovi prístup k validačnej službe. Pozastavenie prístupu používateľa k validačnej službe na základe závažných pochybení musí byť používateľovi oznámené včas a vhodným spôsobom.

## 4.4 Riadenie používateľských účtov

Pozastavenie a/alebo zrušenie používateľských účtov alebo prístupov k validačnej službe sa musí vykonávať na základe:

- písomnej žiadosti oprávnenej osoby,
- automaticky v prípade ukončenia poskytovania validačnej služby Poskytovateľom,
- automaticky v prípade ukončenia platnosti používateľského prístupu do rozhrania validačnej služby.

# 5 Všeobecné ustanovenia

## 5.1 Všeobecné ustanovenia politiky

Táto CP nadväzuje na dokument Všeobecné podmienky, CP NFQES CA a NFQES CPS, kde sú popísané všeobecné požiadavky a pravidlá poskytovania dôveryhodných služieb, ktoré musí Poskytovateľ dôveryhodných služieb rešpektovať a dodržiavať. Pri poskytovaní validačnej služby sa očakáva, že Zákazníci a Spoliehajúce sa strany budú konzultovať podrobnosti spôsobu poskytovania validačnej služby priamo s Poskytovateľom validačnej služby.

Z dôvodu, že QES a QES-S sú z technického a implementačného hľadiska podobné, je zvyšný text tejto CP upravujúci požiadavky pre QES primerane uplatňovaný aj pre QES-S.

## 5.2 Služby súvisiace s kvalifikovanou validačnou službou

Služby súvisiace s validačnou službou sú vo všeobecnosti prevádzkové monitorovacie a riadiace služby spojené s poskytovaním validačnej služby, pomocou ktorej sa vyhotovuje výsledná správa z validačného procesu. Pre potreby uchovávania informácií a auditných záznamov o správnom fungovaní validačnej služby Poskytovateľ musí vytvárať záznamy podľa tejto CP.

## 5.3 Poskytovateľ validačnej služby

Poskytovateľ kvalifikovanej dôveryhodnej služby vytvárania správy z validácie pre potreby Zákazníkov a Spoliehajúce sa strany je v zmysle tejto CP spoločnosť brainit.sk s.r.o.

Poskytovateľ nesie celkovú zodpovednosť v súvislosti s poskytovaním validačnej služby a za poskytovanie služieb súvisiacich s dôveryhodnou validačnou službou a jej súvisiacimi službami (pozri kapitolu 5.2). Poskytovateľ môže prevádzkovať niekoľko validačných služieb, ktoré sú nezávislé a prevádzkované inými jednotkami na vytváranie validačných správ (napr. externou registračnou autoritou, ktorá musí spĺňať všetky ustanovenia tejto CP).

## 5.4 Používateľ validačnej služby

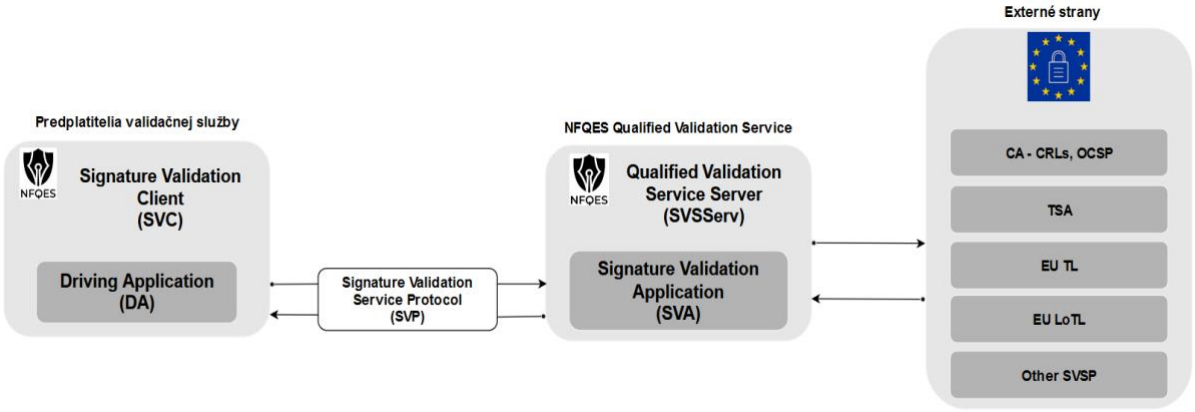
Používateľom validačnej služby je Zákazník, respektíve koncový používateľ Zákazníka. Pod používateľom sa myslí FO alebo PO využívajúca validačnú službu.

# 6 Kvalifikovaná validačná služba

Služba kvalifikovanej validácie bude spracovávať na vstupe celý dokument podpísaný podľa technických špecifikácií a noriem definovaných v ETSI na ktoré je odkazované v Nariadení Európskeho parlamentu a Rady EU č. 910/2014 o elektronickej identifikácii a službách vytváraných pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES.

Vstupom pre validačnú službu bude jediné rozhranie, ktoré je poskytované Poskytovateľom tejto služby. Využívanie validačnej služby iným spôsobom, ako je definované Poskytovateľom, nie je povolené a je vnímané ako hrubé porušenie podmienok poskytovania validačnej služby.

Nižšie uvedený diagram zobrazuje zjednodušenú architektúru validačnej služby poskytovanej Poskytovateľom a jej zúčastnené strany.




## 6.1 Opis validačnej služby

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

Dôveryhodný zoznam na národnej úrovni obsahuje informácie o poskytovateľoch kvalifikovaných dôveryhodných služieb, ako aj informácie o všetkých kvalifikovaných dôveryhodných službách, ktoré títo poskytovatelia poskytujú. Európska komisia vedie zoznam národných dôveryhodných zoznamov, ktoré zverejňujú jednotlivé členské štáty EÚ v zmysle ustanovení vykonávacieho rozhodnutia Komisie č. 2015/1505. Tento európsky zoznam je známy pod označením List of Trust Lists (ďalej iba „LoTL“).

LoTL je dostupný online vo formáte XML na adrese: https://ec.europa.eu/tools/lotl/eu-lotl.xml

Validačnú službu je možné využívať iba Zákazníkmi Poskytovateľa alebo zmluvní Zákazníci brainit.sk. K validačnej službe je možné pristupovať iba pomocou definovaných rozhraní a aplikácií zverejnených Poskytovateľom validačnej služby. Používateľ validačnej služby je povinný chrániť rozhranie služby pred neoprávneným používaním a zabezpečiť primeranú bezpečnosť pri využívaní validačných služieb. To platí pre akékoľvek rozhranie používané na prístup k validačnej službe. Týmto rozhraním sa rozumie najmä webový portál na používanie validačnej služby alebo akákoľvek aplikácia alebo integračné rozhranie dodávané výhradne spoločnosťou brainit.sk alebo integrátorom určeným Poskytovateľom validačnej služby.

## 6.2 Overenie informácií v LoTL

Kvalifikovaná validačná služba musí pravidelne vykonávať kontrolu LoTL v zmysle požiadaviek ETSI TS 119 615.

## 6.3 Kontrola formátu podpisu a technické parametre kvalifikovanej validačnej služby

### *6.3.1 Kontrola a overovanie základných profilov*

Validačná služba musí overovať 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 ASiC kontajnera - 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.

### *6.3.2 Overované certifikáty*

Validačná služba musí vykonávať overovanie elektronických podpisov a elektronických pečatí založených na kvalifikovaných certifikátoch podľa nariadenia eIDAS.

Kvalifikovanosť jednotlivých KC alebo TSP, ktorí certifikáty vydávajú musí byť overovaná voči Dôveryhodným zoznamom (Trusted Lists - TL). Zoznam adries všetkých zverejnených dôveryhodných zoznamov členských štátov je zverejňovaný Európskou komisiou (pozri kapitolu 6.1).

### *6.3.3 Kontrola a overovanie formátov podpisov a pečatí*

Validačná služba musí overovať platnosť elektronických podpisov a pečatí vo formátoch, ktoré sú uvedené v zmysle Európskej komisie vo vykonávajúcom rozhodnutí č. 2015/1506. Jedná sa o formáty:

- PAdES – formát využívaný pre podpisovanie/pečatenie dokumentov vo formátoch PDF a PDF/A podľa technických špecifikácií ETSI TS 103 172, resp. ETSI EN 319 142,
- XAdES – formát využívaný pre podpisovanie/pečatenie štruktúrovaných dokumentov s dátovou XML štruktúrou podľa technickej špecifikácie ETSI TS 103 171, resp. ETSI EN 319 132,
- CAdES – formát využívaný pre podpisovanie/pečatenie všeobecných binárnych dát a dokumentov u ktorých nie je možné použiť vložený podpis podľa technickej špecifikácie ETSI TS 103 173, resp. ETSI EN 319 122,
- ASiC – formát pre kontajner s pridruženým podpisom/pečaťou podľa technickej špecifikácie ETSI TS 103 174, resp. ETSI EN 319 162-1.
- Formát S/MIME v3 – RFC 2632, RFC 3850, RFC 5750, RFC 5751

## 6.4 Validačný proces

Validačný proces kvalifikovanej validačnej služby musí byť vykonávaný v zmysle ustanovení schémy dohľadu s posúdením konkrétnych požiadaviek príslušných štandardov pre jednotlivé formáty podpisov.

Validačná služba Poskytovateľa podporuje validačný proces pre základné podpisy (Basic Signatures), podpisy s časovou pečiatkou (Signatures with Timestamp) a podpisy s dlhodobými validačnými údajmi (Signatures with Long-Term Validation data).

### *6.4.1 Požiadavky na proces overovania podpisov/pečatí*

Postupy validačnej služby na určenie, či je elektronický podpis alebo elektronická pečať technicky platná, vychádzajú z procesu opísaného v ETSI TS 119 102.

Nasledujúce časti vysvetľujú spôsob, akým validačná služba vykonáva jednotlivé komponenty validačných procedúr, uvádza prebiehajúce procesy a obmedzenia. Ak v tomto dokumente nie sú stanovené žiadne špecifické požiadavky, v celom rozsahu platia požiadavky a pravidlá z ETSI TS 119 102 odsek 5. Ak sú v tejto CP stanovené špecifické požiadavky a pravidlá, majú prednosť pred zodpovedajúcimi požiadavkami z ETSI TS 119 102. V prípade nezrovnalostí medzi týmito špecifikáciami a špecifikáciami z ETSI TS 119 102 majú prednosť špecifikácie z tejto CP.

Jednotlivé typy podpisov a pečatí v podporovaných formátoch podľa kapitoly 6.3.3 umožňujú rôznu úroveň overovania platnosti elektronického certifikátu pre podpis/pečať. Z toho dôvodu validačná služba obsahuje rôzne validačné procesy podľa typu podpisu/pečate a informácií, ktoré sú v ňom zahrnuté.

Proces validácie musí vydávať indikáciu stavu overenia podpisu, jeden na každý overený podpis/pečať, a taktiež výslednú správu z validácie podpisu/pečate.

Validačný proces musí pozostávať z postupnosti viacerých krokov, ktorými sa určí či:

- certifikát, ktorý potvrdzuje podpis/pečať, bol v čase podpísania kvalifikovaným certifikátom pre elektronický podpis/pečať,
- kvalifikovaný certifikát vydal kvalifikovaný poskytovateľ dôveryhodných služieb a v čase podpísania bol platný,
- údaje na validáciu podpisu zodpovedajú údajom poskytnutým spoliehajúcej sa strane,
- sa jedinečný súbor údajov reprezentujúcich podpisovateľa v certifikáte správne poskytol spoliehajúcej sa strane,
- sa použitie pseudonymu jasne oznámilo spoliehajúcej sa strane v prípade, že sa v čase podpísania použil pseudonym,
- bol elektronický podpis/pečať vyhotovený kvalifikovaným zariadením na vyhotovenie elektronického podpisu/pečate,
- nebola narušená integrita podpísaných údajov,
- boli splnené požiadavky na zdokonalený elektronický podpis v čl. 26 nariadenia eIDAS.

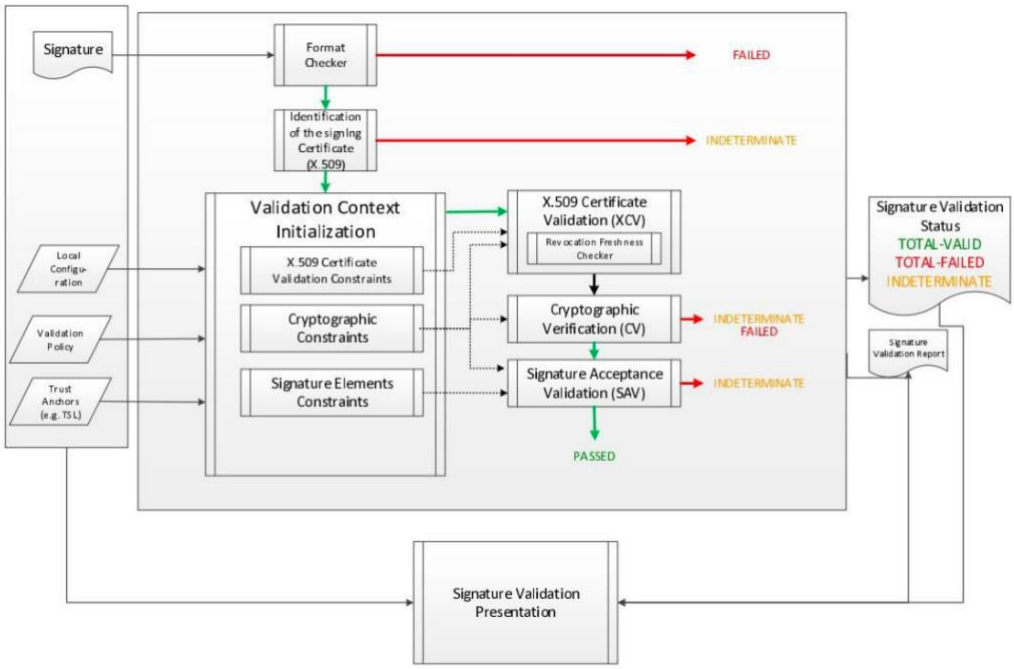
Procesy validačnej služby Poskytovateľa identifikujú kvalifikované a zdokonalené elektronické podpisy a pečate. Procesy musia potvrdiť platnosť kvalifikovaného elektronického podpisu a pečate, pokiaľ vyhovuje podmienkam definovaným v nariadení eIDAS podľa článku 32.

Režim pre využitie validačnej služby ako kvalifikovanej validačnej služby musí byť vždy určený použitím validačnej politiky pre kvalifikované overovanie, resp. jej identifikátorom 1.3.158.52577465.0.0.0.1.7.1.1.

Vlastný validačný proces prebieha v súlade s požiadavkami ETSI EN 319 102-1 a ďalej pre jednotlivé formáty v súlade s ETSI TS 103 172 a ETSI EN 319 142 pre formát PAdES, ETSI TS 103 171 a ETSI EN 319 132 pre formát XAdES, ETSI TS 103 173 a ETSI EN 319 122 pre formát CAdES, ETSI TS 103 174 a ETSI EN 319 162 pre formát ASiC.

Pre využitie validačnej služby v režime zdokonalenej validačnej služby je možné použiť základnú ponúkanú politiku, resp. identifikátor pokročilej validačnej služby 1.3.158.52577465.0.0.0.1.7.1.2.

### *6.4.2 Model overovania podpisov*




Podľa koncepčného modelu overovania podpisu/pečate definovaného v uvedenej špecifikácii vystupuje validačná služba ako SVA. SVA je vyvolaná aplikáciou DA, ktorej musí vrátiť výsledky validačného procesu vo forme výslednej správy z validačného procesu.

DA pre validačnú službu poskytovanú Poskytovateľom môže byť:

- portál NFQES – dostupný na https://zone.nfqes.com
- NFQES Validation Service API

## 6.5 Komunikačný kanál

Komunikačný kanál medzi klientom a Poskytovateľom musí byť zabezpečený, pomocou spoľahlivo chráneného kanála s využitím protokolu HTTPS a pomocou TLS šifrovania s certifikátom. Poskytovateľ musí zaručiť, že môže vytvoriť bezpečný kanál s klientom a zachovať dôvernosť údajov. Poskytovateľ musí ponúknuť, zabezpečiť a vyžiadať od klienta autentifikáciu k službe prostriedkami elektronickej identifikácie a až potom môže mať klient prístup k validačnej službe. Z tohto dôvodu Poskytovateľ musí zabezpečiť, že nahrávané informácie sú prístupné len pre konkrétneho identifikovaného klienta.

V prípade, že Poskytovateľ ponúka validačnú službu inak ako cez portál (API, gateway), Poskytovateľ musí žiadať od používateľa autorizáciu pomocou autorizačného tokenu, ktorý zaisťuje, že nahrané informácie sú prístupné len pre konkrétneho identifikovaného klienta, prípadne je možné použiť aj IP ochranu a obmedzenie komunikácia pomocou tzv. whitelistu.

## 6.6 Výsledok validačného procesu

Pokiaľ sú elektronický podpis alebo elektronická pečať dokumentu porušené a poškodené, je validačný proces pozastavený a ďalej sa už nepokračuje v overovaní jeho/jej atribútov a overovanie je ukončené výsledkom chyby o porušení podpisu a/alebo pečate.

Validačná služba poskytuje komplexnú správu o validácii (pozri časť 6.7), ktorá umožňuje DA kontrolovať detail rozhodnutí prijatých počas validácie a skúmať podrobné príčiny indikácie stavu

poskytovanej služby. Všetky validačné služby uvedené v časti 6.4.2 prezentujú správu zmysluplným spôsobom, v čitateľnej forme pre používateľa (pozri časť 6.7).

Vyhodnotenie procesu validácie elektronického podpisu alebo pečate je priamo závislé na zvolenej validačnej politike. Súčasťou výstupných informácií a samotného výstupného súboru musia byť podrobné informácie, na základe ktorých bolo rozhodnuté o výsledku validačného procesu.

Podľa algoritmu špecifikovaného v ETSI TS 119 102-1 môže byť stav overenia podpisu, a teda výsledok validačného procesu nadobúdať tieto hodnoty:

| **Indikácia stavu** | **Popis** | **Súvisiace údaje správy o overení** |
| --- | --- | --- |
| TOTAL-PASSED | Výsledkom procesu overenia podpisu je TOTAL-PASSED na základe nasledujúcich úvah:<br>• úspešné kryptografické kontroly podpisu (vrátane kontrol hashov jednotlivých dátových objektov, ktoré boli podpísané nepriamo);<br>• všetky obmedzenia vzťahujúce sa na certifikáciu identity podpisovateľa boli pozitívne overené (t. j. podpisový certifikát bol následne uznaný za dôveryhodný);<br>• podpis bol pozitívne overený voči overovacím obmedzeniam, a preto sa považuje za zhodný s týmito obmedzeniami.<br>Úplne overenie na základe vyhodnotenia parametrov podpisu a dokumentu čím bolo možné určiť plnú platnosť podpisu.<br>Indikácia označuje, že podpis prešiel overením a je v súlade s politikou overovania podpisu. | Proces validácie vygeneruje podpisový certifikát, ktorý sa používa v procese validácie, spolu so špecifickým podpísaným atribútom, ak je prítomný a považuje sa za dôkaz validácie. |
| TOTAL-FAILED | Výsledkom procesu overenia podpisu je TOTAL-FAILED, pretože zlyhali kryptografické kontroly podpisu (vrátane kontrol hashov jednotlivých dátových objektov, ktoré boli podpísané nepriamo) alebo sa dokázalo, že vygenerovanie podpisu prebehlo po odvolaní podpisu. podpisový certifikát.<br>Na základe vyhodnotenia parametrov podpisu a dokumentu bolo možné určiť úplnú neplatnosť podpisu.<br>Indikácia naznačuje, že je nesprávny formát podpisu alebo, že overenie hodnoty digitálneho podpisu zlyhá. | Proces validácie poskytuje dodatočné informácie na vysvetlenie indikácie TOTAL-FAILED pre každé z validačných obmedzení, ktoré sa zohľadnili a pre ktoré sa vyskytol negatívny výsledok. |

| | | |
|---|---|---|
| INDETERMINATE | Dostupné informácie nestačia na to, aby sa zistilo, že podpis má byť TOTAL-PASSED alebo TOTAL-FAILED.<br>Na základe vyhodnotenia parametrov podpisu a dokumentu nebolo možné určiť úplnú platnosť alebo neplatnosť podpisu.<br>Indikácia naznačuje, že overenie formátu digitálneho podpisu nezlyhalo, ale nie je dostatok informácií na určenie, či ej elektronický podpis platný. | Proces validácie poskytuje dodatočné informácie, ktoré vysvetľujú indikáciu NEISTOTY a pomáhajú overovateľovi identifikovať, ktoré údaje chýbajú na dokončenie procesu validácie. |

Validačný proces je závislý na čase posudzovania počas ktorého sa má overovanie vykonávať. Pokiaľ je čas posudzovania a overovania zadaný od používateľa, za takýto údaj je zodpovedný používateľ danej služby a tým pádom aj za interpretáciu výsledku overovania, ktoré je platné k tomuto zadanému časovému okamžiku. V prípade, že používateľ nezadá požadovaný čas posúdenia a overenia je pre vyhodnotenie overenia použitý časový okamžik preukázateľnej existencie (PoE) dokumentu, ktorý môže byť:

- čas prijatia dokumentu validačnou službou na overenie,
- kvalifikovaná elektronická časová pečiatka, ktorá je súčasťou dokumentu.

Okrem hlavného stavu obsahuje správa overenia podpisu aj sekundárnu indikáciu s nasledujúcou sémantikou:

| **Hlavná indikácia** | **Pod-identifikácia** | **Súvisiace údaje správy o overení** | **Popis** |
|---|---|---|---|
| TOTAL-FAILED | FORMAT_FAILURE | Proces validácie poskytne všetky dostupné informácie, prečo analýza podpisu zlyhala. | Podpis nie je v súlade s jedným zo základných štandardov do tej miery, že stavebný blok kryptografického overovania ho nedokáže spracovať. |
| | HASH_FAILURE | Proces validácie musí poskytnúť: Identifikátor(y) (napr. URI alebo OID) jedinečne identifikujúci prvok v rámci podpísaného dátového objektu (ako sú atribúty podpisu alebo SD), ktorý spôsobil zlyhanie. | Výsledkom procesu overenia podpisu je TOTALFAILED, pretože aspoň jeden hash podpísaného dátového objektu (objektov), ktorý bol zahrnutý do procesu podpisovania, sa nezhoduje so zodpovedajúcou hodnotou hash v podpise. |
| | SIG_CRYPTO_FAILURE | Výsledkom procesu validácie je: Podpisový certifikát použitý v procese validácie. | Výsledkom procesu overenia podpisu je TOTALFAILED, pretože hodnotu podpisu v podpise nebolo možné overiť pomocou verejného kľúča podpisovateľa v podpisovom certifikáte. |

| | | | |
|---|---|---|---|
| | REVOKED | Proces validácie poskytuje tieto informácie:<br>• Reťazec certifikátov použitý v procese overovania.<br>• Čas a, ak je k dispozícii, dôvod zrušenia podpisového certifikátu. | Výsledkom procesu overenia podpisu je TOTALFAILED, pretože:<br>• podpisový certifikát bol zrušený; a<br>• existuje dôkaz, že podpis bol vytvorený po čase odvolania. |
| | EXPIRED | Výstupom procesu je:<br>• Overený reťazec certifikátov | Výsledkom procesu overenia podpisu je TOTALFAILED, pretože existuje dôkaz, že podpis bol vytvorený po dátume ukončenia platnosti (notAfter) podpisového certifikátu. |
| | NOT_YET_VALID | ---------- | Výsledkom procesu overenia podpisu je TOTALFAILED, pretože existuje dôkaz, že podpis bol vytvorený pred dátumom vydania (notBefore) podpisového certifikátu. |
| INDETERMINATE | SIG_CONSTRAINTS_FAILURE | Proces validácie poskytuje:<br>Súbor obmedzení, ktoré neboli splnené podpisom. | Výsledkom procesu overenia podpisu je INDETERMINATE, pretože jeden alebo viacero atribútov podpisu nezodpovedá obmedzeniam overenia platnosti. |
| | CHAIN_CONSTRAINTS_FAILURE | Výsledkom procesu validácie je:<br>• Reťazec certifikátov použitý v procese overovania.<br>• Množina obmedzení, ktoré reťaz nesplnila. | Výsledkom procesu overovania podpisu je INDETERMINATE, pretože reťazec certifikátov použitý v procese overovania nezodpovedá overovacím obmedzeniam súvisiacim s certifikátom. |
| | CERTIFICATE_CHAIN_GENERAL_FAILURE | Proces vygeneruje:<br>Dodatočné informácie týkajúce sa dôvodu. | Výsledkom procesu overenia podpisu je INDETERMINATE, pretože sada certifikátov dostupných na overenie reťazca spôsobila chybu z nešpecifikovaného dôvodu. |
| | CRYPTO_CONSTRAINTS_FAILURE | Výstupom procesu je:<br>• Identifikácia materiálov (podpis, certifikát), ktoré sú vyrobené pomocou algoritmu alebo veľkosti kľúča pod požadovanou úrovňou kryptografickej bezpečnosti. | Výsledkom procesu overenia podpisu je NEURČITÝ, pretože aspoň jeden z algoritmov, ktoré boli použité v materiáloch (napr. hodnota podpisu, certifikát...), ktoré sa podieľajú na overovaní podpisu, alebo veľkosť kľúča |

| | | | |
|---|---|---|---|
| | | • Ak je známy, čas, do ktorého sa algoritmus alebo veľkosť kľúča považovali za bezpečné. | použitého s takýmto algoritmom, je pod požadovanou úrovňou kryptografickej bezpečnosti a:<br>• tento materiál bol vyrobený po čase, do ktorého bol tento algoritmus/kľúč považovaný za bezpečný (ak je taký čas známy); a<br>• materiál nie je chránený dostatočne silnou časovou značkou aplikovanou pred časom, do ktorého bol algoritmus/kľúč považovaný za bezpečný (ak je taký čas známy). |
| | POLICY_PROCESSING_ERROR | Proces validácie poskytne dodatočné informácie o probléme. | Výsledkom procesu overenia podpisu je INDETERMINATE, pretože daný formálny súbor politík nebolo možné z akéhokoľvek dôvodu spracovať (napr. nie je prístupný, nedá sa analyzovať, nezhoda v súhrne atď.). |
| | SIGNATURE_POLICY_NOT_AVAILABLE | ---------- | Výsledkom procesu overenia podpisu je INDETERMINATE, pretože elektronický dokument obsahujúci podrobnosti o politike nie je dostupný. |
| | TIMESTAMP_ORDER_FAILURE | Proces validácie vydá zoznam časových pečiatok, ktoré nerešpektujú obmedzenia objednávania. | Výsledkom procesu overenia podpisu je INDETERMINATE, pretože nie sú rešpektované niektoré obmedzenia týkajúce sa poradia časových pečiatok podpisov a/alebo podpísaných údajových objektov (objektov). |
| | NO_SIGNING_CERTIFICATE_FOUND | ---------- | Výsledkom procesu overenia podpisu je INDETERMINATE, pretože podpisový certifikát nemožno identifikovať. |
| | NO_CERTIFICATE_CHAIN_FOUND | ---------- | Výsledkom procesu overenia podpisu je INDETERMINATE, pretože pre identifikovaný |

| | | | |
|---|---|---|---|
| | | | podpisový certifikát sa nenašiel žiadny reťazec certifikátov. |
| | REVOKED_NO_POE | Proces validácie poskytuje tieto informácie:<br>• Reťazec certifikátov použitý v procese overovania.<br>• Čas a dôvod zrušenia podpisového certifikátu. | Výsledkom procesu overenia podpisu je INDETERMINATE, pretože podpisový certifikát bol v deň/čas overenia zrušený. Algoritmus overenia podpisu však nemôže zistiť, či čas podpisu leží pred časom odvolania alebo po ňom. |
| | REVOKED_CA_NO_POE | Proces validácie poskytuje tieto informácie:<br>• Reťazec certifikátov, ktorý zahŕňa odvolaný certifikát CA.<br>• Čas a dôvod zrušenia certifikátu. | Výsledkom procesu overenia podpisu je INDETERMINATE, pretože sa našiel aspoň jeden reťazec certifikátov, ale sprostredkujúci certifikát CA je zrušený. |
| | OUT_OF_BOUNDS_NOT_REVOKED | ---------- | Výsledkom procesu overenia podpisu je INDETERMINATE, pretože platnosť podpisového certifikátu vypršala alebo ešte nie je platný v deň/čas overenia a algoritmus overenia podpisu nemôže zistiť, že čas podpisu je v intervale platnosti podpisového certifikátu. Je známe, že certifikát nie je zrušený. |
| | OUT_OF_BOUNDS_NO_POE | ---------- | Výsledkom procesu overenia podpisu je INDETERMINATE, pretože platnosť podpisového certifikátu vypršala alebo ešte nie je platný v deň/čas overenia a algoritmus overenia podpisu nemôže zistiť, že čas podpisu leží v intervale platnosti podpisového certifikátu. |
| | CRYPTO_CONSTRAINTS_FAILURE_NO_POE | Výstupom procesu je:<br>• Identifikácia materiálov (podpis, certifikát), ktoré sú vyrobené pomocou algoritmu alebo veľkosti kľúča pod požadovanou úrovňou kryptografickej bezpečnosti.<br>Ak je známy, čas, do ktorého sa algoritmus alebo veľkosť kľúča považovali za bezpečné. | Výsledkom procesu overovania podpisu je INDETERMINATE, pretože aspoň jeden z algoritmov, ktoré boli použité v objektoch (napr. hodnota podpisu, certifikát atď.), ktoré sa podieľajú na overovaní podpisu, alebo veľkosť kľúča použitého s takýmto algoritmom, je pod požadovanou úrovňou |

| | | | |
|---|---|---|---|
| | | | kryptografickej bezpečnosti a neexistuje žiadny dôkaz, že tento materiál bol vyrobený pred časom, dokedy sa tento algoritmus/kľúč považoval za bezpečný. |
| | NO_POE | Proces validácie musí identifikovať aspoň podpísané objekty, pre ktoré chýbajú POE.<br>• Proces overovania by mal poskytnúť dodatočné informácie o probléme. | Proces overenia podpisu má za následok INDETERMINATE, pretože chýba dôkaz o existencii, aby sa zistilo, že podpísaný objekt bol vyrobený pred nejakou kompromitujúcou udalosťou (napr. narušený algoritmus). |
| | TRY_LATER | V procese validácie sa uvedie čas, kedy sa očakáva, že budú k dispozícii potrebné informácie o zrušení. | Výsledkom procesu overenia podpisu je INDETERMINATE, pretože nie všetky obmedzenia možno splniť pomocou dostupných informácií. Možno to však bude možné urobiť pomocou dodatočných informácií o zrušení, ktoré budú k dispozícii neskôr. |
| | SIGNED_DATA_NOT_ FOUND | Proces by mal mať výstup, keď je k dispozícii:<br>Identifikátor(y) (napr. URI) podpísaných údajov, ktoré spôsobili zlyhanie. | Výsledkom procesu overenia podpisu je INDETERMINATE, pretože nie je možné získať podpísané údaje. |

Poskytovateľ musí priradiť každej validačnej politike identifikátor objektu (OID) a podporuje dve validačné politiky:

| Validačná politika | Identifikátor objektu |
|---|---|
| **QES validačná politika**<br>• **Prísnejšia validácia:** vyžaduje platné kvalifikované elektronické podpisy a pečate. Kvalifikované elektronické podpisy majú rovnaký právny účinok ako vlastnoručné podpisy podľa nariadenia EÚ č. 910/2014 (eIDAS).<br>Podrobné obmedzenia validácie sú definované v prílohe A tejto CP. | 1.3.158.52577465.0.0.0.1.7.1.1 |
| **AdES validačná politika**<br>• **Základná validácia:** kontroluje, či dokument nebol pozmenený a poskytuje potrebné informácie o právnom type a platnosti elektronických podpisov a pečatí podľa nariadenia EÚ č. 910/2014 (eIDAS).<br>Podrobné obmedzenia validácie sú definované v prílohe B tejto CP. | 1.3.158.52577465.0.0.0.1.7.1.2 |

## 6.7 Výstup validačného procesu

Validačná služba musí poskytovať výstup validačného procesu vo formáte štruktúrovaných XML súborov po integrácii do aplikácií tretích strán a ďalej ako PDF dokument s ľudsky čitateľným výstupom o výsledku validačného procesu. Používateľ služby si prostredníctvom jej rozhrania môže zvoliť aký výstup požaduje.

Výstup procesu overovania podpisu/pečate musí minimálne obsahovať:

- zoznam podpisov/pečati,
- stav označujúci výsledky procesu overovania podpisu/pečate,
- chyby popisujúce dôvod prečo je podpis/pečať neplatný (TOTAL-FAILED) alebo indikácie popisujúce, prečo SVS nedokázalo určiť stav podpisu/pečate (INDETERMINATE),
- označenie politiky, ktorou bol podpis/pečať overovaný,
- použitie akéhokoľvek pseudonymu je jasne oznámené spoliehajúcej sa strane, ak bol pseudonym použitý v čase podpisovania/pečatenia.

Vlastná odpoveď rozhrania služby musí byť z dôvodu autenticity a overiteľnosti odpovede zo služby zabezpečená minimálne zdokonalenou elektronickou pečaťou Poskytovateľa.

### *6.7.1 Štruktúrované XML súbory*

Pre integráciu do nadväzujúcich informačných systémov môže služba ponúkať výstup v troch typoch výstupných XML dokumentoch, ktoré si používateľ môže pri volaní služby zvoliť. Dodatočne je možné si stiahnuť aj ostatné typy výstupných formátov.

**Simple_report.xml** – obsahuje iba základné zjednodušené informácie o vykonanom procese overovania platnosti elektronických podpisov a pečatí pre všetky podpisy, pečate a časové pečiatky v rámci dokumentu. Tento výstupný dokument nemusí obsahovať elektronickú pečať Poskytovateľa minimálne na zdokonalenej úrovni.

**Detailed_report.xml** – obsahuje podrobné informácie o všetkých vykonaných krokoch validačného, vyhodnocovacieho a overovacieho procesu v rámci validačného procesu pre všetky podpisy, pečate a časové pečiatky v rámci dokumentu. Tento výstupný dokument nemusí obsahovať elektronickú pečať Poskytovateľa minimálne na zdokonalenej úrovni.

**Diagnostic_data.xml** – obsahuje všetky informácie, na základe ktorých bolo rozhodnuté o výsledku validačného procesu pre všetky podpisy, pečate a časové pečiatky v rámci dokumentu. Medzi tieto informácie napríklad patria informácie o všetkých použitých certifikátoch, CRL alebo OCSP odpovedí. Tento výstupný dokument je vždy zabezpečený minimálne pokročilou elektronickou pečaťou Poskytovateľa vo formáte XAdES.

### *6.7.2 PDF dokument*

Pre jednoduchšiu prezentáciu výsledkov validačného procesu koncovým používateľom validačnej služby, môže služba poskytovať výstup vo formáte PDF, ktorý umožňuje prezentovať priebeh a výsledky validačného procesu prehľadnou grafickou formou. Služba poskytuje dva typy výstupných správ vo formáte PDF, ktoré svojim obsahom odpovedajú základným štruktúrovaným XML súborom podľa kapitoly 6.7.1.

**Simple_report.pdf** – obsahuje v grafickej podobe informácie v rozsahu informácií, ktoré zodpovedajú štruktúrovanému XML výstupu *simple_report.xml*, ktorý je spolu s XML výstupom *diagnostic_data.xml* vložený do dokumentu ako príloha. Tento výstupný dokument je vždy zabezpečený minimálne zdokonalenou elektronickou pečaťou Poskytovateľa.

**Detailed_report.pdf** – obsahuje v grafickej podobe detailné informácie v rozsahu informácií, ktoré zodpovedajú kombinácií štruktúrovaných XML výstupov *simple_report.xml* a *detailed_report.xml*, ktoré sú spolu so štruktúrovaným XML výstupom *diagnostic_data.xml* vložené do dokumentu ako prílohy. Tento výstupný dokument je vždy zabezpečený minimálne zdokonalenou elektronickou pečaťou Poskytovateľa vo formáte PAdES.

## 6.8 Vymedzenie služby a obmedzenia

### *6.8.1 Vymedzenie validačnej služby*

Validačná služba musí byť prevádzkovaná vo forme webovej služby a webového portálu (viď. kapitola 2.3.1). Je určená pre aplikácie alebo subjekty, ktoré sa na túto službu integrujú podľa príslušnej integračnej dokumentácie. Služba je určená a poskytovaná aj pre koncového používateľa, FO, PO, ktorý k validačnej službe pristupuje prostredníctvom webového prehliadača cez webové sídlo dôveryhodných služieb Poskytovateľa.

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

### *6.8.2 Obmedzenia validačnej služby*

**Formáty súborov**

Validačná služba podporuje formáty definované štandardami uvedenými v kapitole 6.3 tejto CP.

**Veľkosť súborov**

Žiadne ustanovenia.

**Vyhodnotenie podpisu**

Validačná služba vyhodnocuje podpisy vytvorené v zmysle nariadenia eIDAS.

## 6.9 Dostupnosť validačnej služby

Poskytovateľ musí zabezpečiť aby kvalifikovaná validačná služba bola štandardne dostupná v režime 365x7x24. Na službu sa nevzťahuje dodržanie tohto času a môže byť nedostupná počas nevyhnutného času pre správu a údržbu systémov. Okrem toho je z tohto času vyčlenená potrebná doba pre obnovu validačnej služby po havárii, na ktorú nemal Poskytovateľ služby vplyv a nemohol ju nijak ovplyvniť. 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.

Poskytovateľ musí garantovať vysokú spoľahlivosť služby v rámci svojich služieb a aplikácií, ktoré používa a poskytuje. Jednotlivé podmienky pre minimálnu dostupnosť služby musia byť stanovené pre zákazníka osobitne a prípadne aj zmluvne.

## 6.10 Uchovávanie informácií pre overovanie platnosti elektronických podpisov a pečatí

Poskytovateľ musí zabezpečiť dobu počas ktorej Poskytovateľ uchováva súbory potrebné pre overenie platnosti elektronických podpisov a pečatí na minimálne 10 rokov.

## 6.11 Zmluvné podmienky používania validačnej služby

Poskytovateľ musí sprístupniť podmienky týkajúce sa svojich služieb všetkým zákazníkom a spoliehajúcim sa stranám vhodným spôsobom.

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

- politika dôveryhodnej služby bola aplikovaná,
- akékoľvek obmedzenia týkajúce sa používania služby.

Zákazníci a strany využívajúce dôveryhodnú službu musia byť informovaní o presných podmienkach pred uzatvorením zmluvného vzťahu. Zmluvné podmienky používania Kvalifikovanej validačnej služby musia byť prístupné v ľahko zrozumiteľnom jazyku. Zmluvné podmienky používania Kvalifikovanej validačnej služby sa môžu prenášať aj elektronicky.

# 7 Ohodnotenie rizík

Pre ohodnotenie rizík platia ustanovenia uvedené v dokumente Analýza_Rizík v aktuálnej verzii *(dokument AR je súčasťou dokumentácie ISMS).*

# 8 Politiky a pravidlá

## 8.1 Pravidlá pre praktický výkon dôveryhodných služieb

Všeobecné pravidlá pre praktický výkon dôveryhodných služieb sú uvedené v dokumentoch Všeobecné podmienky a Vyhlásenie o certifikačnej politike NFQES QESV, ktoré sú zverejnené na webovom sídle Poskytovateľa (viď. kapitola 2.3.1).

## 8.2 Všeobecné podmienky

Poskytovateľ zverejňuje VP celkovo pre poskytovanie kvalifikovaných služieb, ktoré zahrňujú aj VP kvalifikovanej validačnej služby na svojom webovom sídle.

## 8.3 Politika informačnej bezpečnosti

Politika informačnej bezpečnosti je popísaná v dokumente Politika informačnej bezpečnosti vo verzii 1.1 a tvorí súčasť dokumentácie ISMS.

## 8.4 Záväzky Poskytovateľa

### *8.4.1 Všeobecne*

Poskytovateľ kvalifikovanej validačnej služby sa zaväzuje:

- realizovať všetky požiadavky, kladené na Poskytovateľa v zmysle kapitoly 5, 6, 7,
- používať bezpečné systémy pre uchovávanie záznamov,
- zabezpečiť, aby prax vytvárania výsledných správ z procesu validácie zodpovedala procedúram popísaným v tejto CP.

### *8.4.2 Záväzky Poskytovateľa k Zákazníkovi*

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

## 8.5 Informácie pre spoliehajúce sa strany

VP dostupné pre Spoliehajúce sa strany (pozri kapitolu 8.2) v prípade, že sa spoliehajú na výslednú správu z validačného procesu, musia zahŕňať:

- povinnosť overenia platnosti podpisu výslednej správy z validačného procesu v zmysle príslušných štandardov,
- všetky obmedzenia pre použitie validačnej služby podľa tejto CP,
- všetky ďalšie obmedzenia, uvedené v zmluvách, dohodách alebo platnej legislatíve SR.

# 9 Riadenie, prevádzka a fyzická bezpečnosť

Riadenie bezpečnosti musí byť zamerané predovšetkým na:

- systémy, ktoré prevádzkujú službu kvalifikovanej validácie,
- všetky ostatné procesy, ktoré podporujú službu kvalifikovanej validácie.

Oblasti riadenia prevádzkovej a fyzickej bezpečnosti musia byť zahrnuté a riešené v základných dokumentoch popisujúcich bezpečnostné politiky poskytovania dôveryhodných služieb, plánov obnovy a upresňujúcich interných dokumentoch. Tieto dokumenty reflektujú výsledky analýzy rizík.

Bezpečnosť Poskytovateľa musí byť založená na súhrne bezpečnostných opatrení v objektovej, personálnej, fyzickej a prevádzkovej oblasti bezpečnosti. Tieto bezpečnostné opatrenia musia byť navrhnuté, dokumentované a aplikované na základe bezpečnostných pravidiel. Tieto opatrenia musia byť schválené manažmentom Poskytovateľa.

Bezpečnostné opatrenia musia byť k dispozícii všetkým zodpovedným pracovníkom, ktorých sa týkajú, ako aj ostatným pracovníkom Poskytovateľa.

Poskytovateľ musí:

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

Bezpečnostná politika Poskytovateľa a súhrn aktív týkajúci sa bezpečnosti musia byť preskúmavané v pravidelných intervaloch. Bezpečnostná politika Poskytovateľa a súhrn aktív týkajúci sa bezpečnosti musia byť preskúmavaná v prípade významných zmien na zaistenie ich kontinuity, vhodnosti, dostatočnosti a účinnosti.

Manažmentom Poskytovateľa musia byť schválené všetky zmeny, ktoré môžu ovplyvniť úroveň bezpečnosti poskytovaných dôveryhodných služieb. Nastavenie systémov Poskytovateľa musí byť pravidelne preskúmavané na zmeny, ktoré ohrozujú bezpečnostnú politiku Poskytovateľa.

## 9.1 Fyzická bezpečnosť

### *9.1.1 Priestory*

Technologické priestory, v ktorých je umiestnená základná infraštruktúra Poskytovateľa musia byť v chránených priestoroch, ktoré sú prístupné len autorizovaným osobám. Tieto priestory musia byť od ostatných priestorov oddelené prostredníctvom primeraných bezpečnostných prvkov (bezpečnostné dvere, mreže, pevné múry a pod.). Vybavenie Poskytovateľa má pozostávať len z vybavenia vyhradeného na poskytovanie dôveryhodných služieb a kvalifikovaných dôveryhodných služieb, nemá slúžiť na žiadne účely, ktoré sa netýkajú týchto služieb.

### *9.1.2 Fyzický prístup*

Mechanizmy riadenia prístupu do chránených priestorov Poskytovateľa t. j. do priestorov zóny s najvyššou bezpečnosťou musia byť zabezpečené v čo najväčšej možnej miere. Priestory musia byť chránené bezpečnostným alarmom a vstup do nich môže byť umožnený len osobám, ktoré vlastnia bezpečnostný token a sú uvedené na zozname oprávnených osôb na vstup do chránených priestorov Poskytovateľa. Vybavenie Poskytovateľa musí byť neprestajne chránené pred neautorizovaným prístupom a to aj pred neautorizovaným fyzickým prístupom. Každý vstup iných osôb musí byť vždy zaznamenaný a môže byť povolený len v sprievode oprávnenej osoby.

#### *9.1.3 Napájanie a klimatizácia*

Priestory, v ktorých je umiestnené vybavenie Poskytovateľa, musia byť postačujúco zásobované elektrickou energiou, ako aj vybavené klimatizáciou na vytvorenie spoľahlivého operačného prostredia.

#### *9.1.4 Ochrana pred vodou*

Priestory, v ktorých je umiestnené vybavenie Poskytovateľa, musia byť umiestnené tak, aby nemohlo dôjsť k ich ohrozeniu a poškodeniu vodou z akýchkoľvek zdrojov. V prípade, že to nie je úplne možné musia byť prijaté opatrenia, ktoré minimalizujú riziko ohrozenia priestorov vodou na minimum.

#### *9.1.5 Prevencia a ochrana proti požiaru*

Priestory, v ktorých je umiestnené vybavenie Poskytovateľa musia byť spoľahlivo chránené od zdrojov priameho ohňa resp. tepla, čo by mohlo spôsobiť požiar v zabezpečených priestoroch.

#### *9.1.6 Úložisko médií*

Médiá musia byť uskladnené v priestoroch, ktoré sú chránené pred náhodným, neúmyselným poškodením (vodou, ohňom, elektromagnetickým žiarením). Médiá, ktoré obsahujú informácie týkajúce sa bezpečnostného auditu, archív alebo zálohované informácie musia byť uložené v lokalite oddelenej od vybavenia Poskytovateľa.

#### *9.1.7 Likvidácia odpadu*

S odpadom vznikajúcim v súvislosti s prevádzkou Poskytovateľa musí byť nakladané tak, aby v žiadnom prípade nedošlo k znečisťovaniu životného prostredia.

#### *9.1.8 Zálohovanie mimo hlavnú lokalitu*

Pre prípad nenávratného poškodenia priestorov hlavnej lokality, v ktorých je umiestnená infraštruktúra Poskytovateľa je potrebné mať k dispozícii minimálne kópie najdôležitejších aktív Poskytovateľa zálohované mimo túto hlavnú lokalitu.

#### *9.1.9 Delenie povinností*

Poskytovateľ musí zabezpečiť dostatočný počet zamestnancov pre dostatočné rozdelenie povinností podľa jednotlivých úsekov a v súlade s organizačným poriadkom.

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

### 9.2 Procesná bezpečnosť, ľudské zdroje

#### *9.2.1 Dôveryhodné role*

Poskytovateľ musí mať definované dôveryhodné role zodpovedné za jednotlivé postupy a procesy poskytovaných dôveryhodných služieb ako napr. systémový administrátor, bezpečnostný manažér, interný audítor, PMA a pod.), ktoré formujú základ dôvery v celú PKI a službu kvalifikovanej validácie.

Zároveň musia byť definované zodpovednosti jednotlivých rolí. Osoby vybrané na zastávanie rolí, ktoré si vyžadujú dôveryhodnosť, musia byť dôveryhodné a zodpovedné. Všetky osoby v dôveryhodných roliach musia byť bez konfliktu záujmov na zabezpečenie nestrannosti poskytovaných dôveryhodných služieb Poskytovateľom.

#### *9.2.2 Počet osôb požadovaných pre zaistenie jednotlivých činností*

Pre každú úlohu musí byť identifikovaný počet jednotlivcov, ktorí sú určení na vykonávanie jednotlivých úloh (pravidlo K z N). Počty jednotlivcov na jednotlivých pozíciách odpovedajú potrebe

a miere oddelenia zodpovednosti a zastupiteľnosti. Činnosti súvisiace so službou kvalifikovanej validácie nevyžadujú aby boli vykonávané za účasti viac než jednej osoby.

#### *9.2.3 Identifikácia a autentifikácia pre každú rolu*

Každá rola musí mať definovaný spôsob autentifikácie a identifikácie pri prístupe k IS Poskytovateľa.

Každá rola sa musí pri prístupe k prostriedkom poskytovanej validačnej služby identifikovať a autentifikovať. Každý z používateľov má pridelenú jednoznačnú identifikáciu vo všetkých systémoch ku ktorým má prístup.

#### *9.2.4 Role vyžadujúce rozdelenie zodpovednosti*

Každá rola musí mať stanovené kritériá, ktoré zohľadňujú potrebu oddelenia funkcií z hľadiska samotnej roly t. j. model pre správu a poskytovanie služby musí byť nastavený tak, aby uvedené roly, nemohli byť vykonávané rovnakými jednotlivcami a nedochádzalo ku kumulácií právomoci a strete záujmov.

### 9.3 Personálne bezpečnostné opatrenia

Pracovníci Poskytovateľa musia byť menovaní do dôveryhodných rolí výkonným manažmentom zodpovedným za bezpečnosť. Do rolí spojených so správou a poskytovaním služby môžu byť menovaní iba pracovníci Poskytovateľa, ak nie je zmluvne dohodnuté inak.

#### *9.3.1 Požiadavky na kvalifikáciu, skúsenosti a previerky*

Pre každého pracovníka, ktorý bude zaradený do role správy alebo dohľadu pri poskytovaní kvalifikovanej validačnej služby musí byť preskúmaná jeho spôsobilosť pre vykonávanie povinností vyplývajúcich z tejto role. Zamestnanci v dôveryhodných rolách musia spĺňať kvalifikačné požiadavky, požiadavky na odbornú prax a mali by mať bezpečnostné previerky stanovenej úrovne (ak si to situácia vyžaduje).

Osoby v manažérskych funkciách by mali:

- mať príslušné skúsenosti alebo školenia v oblasti dôveryhodných služieb, ktoré Poskytovateľ poskytuje,
- byť oboznámené s bezpečnostnými opatreniami pre roly zodpovedné za bezpečnosť,
- mať skúsenosti s informačnou bezpečnosťou a odhadom rizika v rozsahu potrebnom na výkon manažérskej funkcie.

V rámci posudzovania vhodnosti pracovníka pre konkrétnu rolu môže vzniknúť požiadavka na preukázanie bezúhonnosti. Takáto požiadavka môže byť posudzovaná na základe výpisu z registra trestov. V súlade so zavedenými postupmi pre prijímanie zamestnancov, každý pracovník poskytuje tieto informácie počas vstupného osobného pohovoru. Pre doplnenie informácií, ich overenie a kvôli ich aktualizácii môže byť vykonaný ďalší pohovor so zodpovednými pracovníkmi Poskytovateľa.

Pracovníci, ktorí sú vymenovaní do rolí bezpečnostných správcov poskytovaných dôveryhodných služieb môžu byť vyberaní iba z vysoko spoľahlivých a dôveryhodných zamestnancov Poskytovateľa.

#### *9.3.2 Požiadavky previerky*

Pred obsadením pracovníka do kľúčovej roly správy validačnej služby musí byť posúdená jeho spôsobilosť. Zdrojom informácií pre toto posúdenie nie je samotný pracovník, ale osoba s ktorou pracoval a jeho nadriadeným. Ďalším dôležitým zdrojom informácií sú verejne prístupné informačné zdroje.

Je odporúčané, aby zamestnanec, ktorý má byť zaradený do dôveryhodnej roly Poskytovateľa mal bezpečnostnú previerku stanovenej úrovne resp. je v procese žiadania o takýto typ previerky. Personálne bezpečnostné opatrenia môžu byť zabezpečované internými mechanizmami Poskytovateľa.

#### *9.3.3 Požiadavky na školenie*

Pre niektoré dôveryhodné roly Poskytovateľa môžu byť špecifikované niektoré špeciálne požiadavky na školenia, ktoré by mali absolvovať pred zaradením prípadne v priebehu zaradenia do role. Témy majú obsahovať fungovanie softvéru a hardvéru, bezpečnostné a prevádzkové postupy, ustanovenia tejto CP a príslušných CPS a pod.

#### *9.3.4 Frekvencia obnovy školení*

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

#### *9.3.5 Frekvencia rotácie rolí*

Rotácia rolí medzi jednotlivými pozíciami nie je vykonávaná. Zo strany Poskytovateľa je potrebné zabezpečiť podporu pre získavanie vedomostí pre výkon rôznych dôveryhodných rolí z dôvodu zastupiteľnosti a pre prípad krízových situácií.

#### *9.3.6 Sankcie za neoprávnené konanie*

Zlyhanie akéhokoľvek zamestnanca Poskytovateľa, ktorého výsledok môže byť stav, ktorý nie je v súlade s ustanoveniami tejto CP resp. prijatých CPS, či už sa jedná o zlý úmysel alebo nedbanlivosť, musí byť predmetom zodpovedajúcich disciplinárnych a administratívnych konaní, ktoré môžu viesť až k ukončeniu pracovného pomeru, prípadne občianskym resp. trestnoprávnym postihom.

Akékoľvek nevhodné alebo neoprávnené konanie zamestnanca v dôveryhodnej roly označené vedením Poskytovateľa musí viesť k bezodkladnému odvolaniu z dôveryhodnej roly a to až do ukončenia prebiehajúceho preskúmania manažmentom. Následne po preskúmaní manažmentom a vzájomnej diskusii alebo preskúmaní výsledkov vyšetrovania so zamestnancom, môže byť tento zamestnanec prepustený zo zamestnania, alebo podľa potreby znovu pridelený do dôveryhodnej roly.

#### *9.3.7 Požiadavky na externých dodávateľov*

Nezávislí dodávatelia, ktorí by mohli byť priradení na vykonávanie dôveryhodných rolí musia podliehať rovnakým povinnostiam a špecifickým požiadavkám na tieto roly v zmysle ustanovení bodu 9.3 a rovnako podliehajú sankciám uvedeným v bode 9.3.6.

#### *9.3.8 Dokumentácia poskytnutá zamestnancom*

Zamestnanci v dôveryhodných rolách musia mať k dispozícii dokumenty potrebné pre výkon funkcie, na ktorú sú priradení, vrátane kópie tejto CP resp. CPS a všetky technické a prevádzkové dokumenty potrebné k zachovaniu integrity operácií Poskytovateľa. Tieto informácie musia zahŕňať aj bezpečnostnú dokumentáciu a dokumentáciu interného systému, postupy a politiky overovania identity ako aj ďalšie informácie pripravené Poskytovateľom a dokumenty tretích strán resp. dokumenty dostupné prostredníctvom internetu.

### 9.4 Kryptografické riadiace prvky

#### *9.4.1 Všeobecne*

Všetky vhodné bezpečnostné opatrenia, ktoré musia byť aplikované na riadenie akýchkoľvek kryptografických kľúčov a kryptografických zariadení počas ich životnosti, sú popísané v politike

informačnej bezpečnosti a dokumentácii pre prácu s takýmito zariadeniami a Poskytovateľ ich musí dodržiavať.

### *9.4.2 Generovanie kľúčov pre VSU*

Generovanie kľúčov pre jednotlivé VSU musí spĺňať nasledovné:

- musí byť vykonávané vo fyzicky bezpečnom prostredí osobami, zaradenými v dôveryhodných rolách, za účasti minimálne dvoch oprávnených osôb,
- generovanie VSU autorizačného kľúča/kľúčov 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 výsledných správ z validačného procesu.

### *9.4.3 Ochrana súkromného kľúča VSU*

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

- súkromný autorizačný kľúč VSU musí byť uložený a používaný v bezpečnom hardvérovom zariadení,
- súkromný kľúč VSU musí byť 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 bezpečnostným pravidlám obsiahnutým v bezpečnostných politikách,
- akékoľvek záložné kópie súkromného autorizačného kľúča nachádzajúce sa mimo VSU musia byť chránené tak, aby bola zabezpečená ich integrita a dôvernosť.

### *9.4.4 Certifikát verejného kľúča VSU*

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

- verejný kľúč VSU, ktorý slúži na overenie autorizácie, musí byť dostupný spoliehajúcim sa stranám v certifikáte verejného kľúča,
- certifikát verejného kľúča VSU pre overenie autorizácie, musí byť vydaný kvalifikovaným poskytovateľom dôveryhodnej služby vyhotovovania a overovania kvalifikovaných certifikátov pre podpis/pečať,
- VSU nemôže vytvoriť výslednú správu z validačného procesu pred tým ako jej certifikát verejného kľúča pre overenie autorizácie je načítaný v kryptografickom zariadení VSU.

### *9.4.5 Prepísanie kľúča VSU*

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

### *9.4.6 Riadenie životného cyklu podpisového kryptografického hardvéru*

Pre riadenie životného cyklu podpisového kryptografického hardvéru musia byť aplikované nasledovné požiadavky:

- do kryptografického hardvéru, kde sú uložené kryptografické kľúče, určené na autorizáciu výslednej správy z validačného procesu, 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 hardvéry musí byť vykonávaná iba osobami v dôveryhodných rolách, s minimálne dvojitou kontrolou a vo fyzicky bezpečnom prostredí,
- súkromné autorizačné kľúče VSU, uložené v kryptografickom module VSU, musia byť v prípade vyradenia modulu vymazané takým spôsobom, že je prakticky nemožné ich obnovenie.

#### *9.4.7 Ukončenie životného cyklu kľúča VSU*

Dátum exspirácie kľúčov VSU musí byť viazaný na koniec platnosti pridruženého certifikátu verejného kľúča, ktorý musí zohľadňovať životnosť, definovanú v „odporúčaných veľkostiach kľúča vzhľadom na čas“ zo štandardu ETSI TS 119 312.

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 výslednej správy z procesu validácie, nový certifikát, s novou platnosťou, ktorý bude následne zaradený do národného dôveryhodného zoznamu.

### 9.5 Prevádzková bezpečnosť

Pre účely prevádzkovej bezpečnosti platia ustanovenia, uvedené v politike informačnej bezpečnosti, pričom najviac 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.

### 9.6 Sieťová bezpečnosť

Pre sieťovú bezpečnosť platia pre Poskytovateľa ustanovenia, uvedené v politike informačnej bezpečnosti, pričom je najviac potrebné zabezpečiť nasledovné:

- poskytovateľ musí udržiavať a chrániť všetky VSU v bezpečnej zóne,
- všetky systémy VSU musia byť nakonfigurované tak, aby mali 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.

### 9.7 Riadenie bezpečnostných incidentov

Pre riadenie bezpečnostných incidentov platia ustanovenia, uvedené v politike informačnej bezpečnosti a internej smernici pre zabezpečenie kontinuity.

### 9.8 Postupy získavania auditných záznamov (logov)

Poskytovateľ musí zaznamenávať a mať k dispozícii počas nevyhnutnej doby, aj po ukončení činnosti, všetky dôležité informácie týkajúce sa činnosti spojených s poskytovaním kvalifikovanej validačnej služby pre potreby kontroly a dokazovania.

Poskytovateľ musí v systéme na poskytovanie dôveryhodných služieb zaznamenávať presný čas. Čas zaznamenávaný pri jednotlivých udalostiach musí byť synchronizovaný s UTC minimálne každých 24 hodín.

### *9.8.1 Typy zaznamenaných udalostí*

Systém validačnej služby zaznamenáva informácie o všetkých operáciách vykonávaných správcom, informácie o stave a prevádzke systému validačnej služby a o periodicky vykonávaných automatických operáciách. Zaznamenávané musia byť aj všetky ostatné operácie a činnosti, ktoré sú požadované platnou legislatívou na území SR. Okrem toho musia byť zaznamenávané všetky udalosti, ktoré sa týkajú riadenia životného cyklu kľúčov VSU a riadenia životného cyklu certifikátov VSU.

Všetky auditné záznamy musia byť v nutnej miere zaznamenávané, uchovávané a spracované so zachovaním preukázateľnosti pôvodu, integrity, dostupnosti, dôvernosti a časovej autentickosti.

Systém auditovania musí byť navrhnutý a prevádzkovaný takým spôsobom, ktorý zaručuje udržiavanie auditných záznamov, dostatočný priestor pre ich uchovávanie, automatické prepisovanie auditného súboru, prezentáciu auditných záznamov pre používateľa vhodným spôsobom a s obmedzeným prístupom iba pre definovaného používateľa/ov.

### *9.8.2 Frekvencia spracovania auditných záznamov*

Administrátori Poskytovateľa sú povinný priebežne sledovať zasielané systémové logy, tak aby včas odhalili potenciálne nebezpečenstvo ohrozenia poskytovania služieb Poskytovateľa.

Auditné záznamy (logy) musia byť spracovávané pri podozrení alebo po bezpečnostnom incidente. Auditné záznamy musia byť kontrolované osobami, ktoré sú v zodpovedajúcej roly a sú poverene vykonávať túto činnosť. Kontrola auditných záznamov musí podliehať internej aj externej kontrole.

### *9.8.3 Lehota uchovania protokolu auditu*

Poskytovateľ musí v súlade s požiadavkami aktuálne platnej legislatívy SR uchovávať auditné logy. Auditné logy musia byť zároveň uchovávané minimálne do času ukončenia nasledovného pravidelného externého auditu svojich služieb.

### *9.8.4 Ochrana auditných záznamov*

Auditné záznamy musia byť chránené a uchovávané tak, aby nedošlo k ich znehodnoteniu a to najlepšie vo viacerých kópiách umiestnených v rozdielnych priestoroch. Auditné záznamy sú ukladané tak, aby boli ochránené proti krádeži, modifikácii a zničeniu, či už úmyselnému alebo neúmyselnému.

### *9.8.5 Postupy zálohovania protokolu auditu*

Auditné záznamy v písomnej forme vo všeobecnosti nie sú zálohované, sú iba archivované (ak nejaké existujú). Žiadne iné ustanovenia.

### *9.8.6 Systém zhromažďovania auditov (interný vs. externý)*

Auditné záznamy sú interne zhromažďované v rámci jednotlivých častí systémov poskytovaných služieb podľa interných pravidiel. Žiadne iné ustanovenia.

### *9.8.7 Oznámenie subjektu iniciujúceho audit*

Žiadne ustanovenia.

### *9.8.8 Posúdenie zraniteľnosti*

Všetky závažné porušenia bezpečnosti musia byť bezodkladne posunuté zodpovednej osobe alebo organizačnej zložke. Pozri bod 9.8.2.

## 9.9 Uchovávanie informácií a dokumentácie

Použité mechanizmy a procesné opatrenia sú všeobecne predmetom interných predpisov, ktoré upravujú problematiku dokumentácie.

### *9.9.1 Typy uchovávaných informácií a dokumentácie*

V rámci poskytovania validačnej služby musia byť archivované informácie pre účely auditu, výsledky vykonaných auditov, dokumentácia registračného procesu a programového vybavenia, informácie a údaje spojené s výsledkami validačného procesu spolu so všetkými podkladovými údajmi a súvisiacimi zmluvnými dokumentmi pre prístup k validačnej službe.

Dokumenty poskytované validačnej službe k vykonávaniu overovania platnosti elektronických podpisov/pečatí nemusia byť uchovávané.

### *9.9.2 Lehota uchovania uchovávaných informácií a dokumentácie*

Programové vybavenie, informácie a údaje, auditné záznamy a dokumenty sa musia archivovať po dobu najmenej 10 rokov.

### *9.9.3 Ochrana úložiska uchovávaných informácií a dokumentácie*

Archívne záznamy Poskytovateľa musia byť chránené a uložené na bezpečnom mieste mimo prevádzkových priestorov a musia byť udržiavané spôsobom, ktorý zabraňuje ich neoprávnenej modifikácii, zničeniu alebo nahradenia. Ochrana archívnych záznamov musí byť zabezpečená spôsobom, ktorý zodpovedá ich bezpečnostnej citlivosti a významu.

### *9.9.4 Postupy zálohovania uchovávaných informácií a dokumentácie*

Žiadne ustanovenia.

### *9.9.5 Požiadavky na používanie časových pečiatok pri uchovávaní informácií a dokumentácie*

Pokiaľ sú v rámci poskytovania validačnej služby využívané časové pečiatky, jedná sa o kvalifikované elektronické časové pečiatky vydané zvoleným QTSP.

### *9.9.6 Postupy na získanie a overenie uchovávaných informácií a dokumentácie*

Správca validačnej služby musí overovať neporušenosť a celistvosť archívu najmenej 1 (raz) ročne v rámci pravidelného interného auditu. Prístup k archívu musí mať výlučne správca validačnej služby a členovia nezávislého tímu audítorov, ktorých určuje Poskytovateľ podľa interných pravidiel.

Správca služby môže určiť povereného pracovníka dohľadu, aby priebežne vykonával pravidelné kontroly archívu.

## 9.10 Obnova po kompromitácií a katastrofe

Pre riadenie kontinuity činnosti organizácie platia ustanovenia uvedené v dokumentoch Poskytovateľa, a to politika informačnej bezpečnosti na základe štandardu ISO 27001 a v politikách systému riadenia kontinuity podnikania na základe štandardu ISO 22301. Najviac je potrebné aby Poskytovateľ zabezpečil nasledovné:

- plán obnovy po katastrofe sa musí zaoberať kompromitáciou, prípadne podozrením z kompromitácie súkromného kľúča VSU,
- v prípade kompromitácie alebo podozrenia z kompromitácie pri vytváraní výslednej správy z validačného procesu, musí Poskytovateľ sprístupniť všetkým zákazníkom a spoliehajúcim sa stranám popis kompromitácie jej zverejnením v úložisku Poskytovateľa,

- v prípade kompromitácie prevádzky VSU alebo podozrenia z kompromitácie, Poskytovateľ nesmie vytvárať výsledné správy z validačného procesu, pokiaľ nebudú vykonávané 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 výslednej správy z validačného procesu, ktoré mohli byť ovplyvnené, pokiaľ tým neporuší súkromie používateľov alebo bezpečnosť služieb poskytovateľa.

### *9.10.1 Postupy pri riešení kompromitácie a katastrof*

Na zabezpečenie integrity služieb musí Poskytovateľ implementovať postupy zálohovania údajov a ich obnovy. Poskytovateľ musí mať vypracované plány obnovy a havarijné postupy pre poskytovanie dôveryhodných služieb.

Postupy riešenia incidentov spojených s kompromitáciou a katastrofou sú popísané v politikách pre systém riadenia kontinuity podnikania podľa štandardu ISO 22301.

Postupy v prípade havárie a obnovy musia byť pravidelne testované a preskúmavané (minimálne na ročnej báze) a mali by byť aktualizované a revidované podľa potreby.

### *9.10.2 Poškodenie výpočtových prostriedkov, softvéru alebo dát*

V prípade poškodenia alebo podozrenia z poškodenia hardvéru, softvéru alebo údajov musí Poskytovateľ použiť postupy určené k obnove poškodených aktív. Postupy musia zahŕňať aktivity, ktoré zabezpečia kompletnú obnovu prostredia.

### *9.10.3 Zachovanie kontinuity činnosti po katastrofe*

Poskytovateľ musí mať prijaté postupy na zabezpečenie kontinuity činnosti v prípade havárie v dôsledku napr. prírodnej katastrofy, ktoré zabezpečia jej schopnosť obnoviť svoju činnosť. Postupy musia zahŕňať miesto obnovy, postupy na ochranu aktív v mieste havárie resp. prírodnej katastrofy a podobne.

## 9.11 Ukončenie činnosti CA alebo RA

V prípade ukončenia činnosti Poskytovateľa je najviac potrebné zabezpečiť aby:

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

Pre ukončenie kvalifikovaného poskytovateľa dôveryhodných služieb platia nasledujúce pravidlá:

- ukončenie činnosti kvalifikovaného poskytovateľa dôveryhodných služieb musí byť písomne oznámené orgánu dohľadu a všetkým subjektom, ktoré majú uzatvorenú zmluvu na využívanie kvalifikovanej validačnej služby,
- ukončenie činnosti poskytovateľa dôveryhodnej služby musí byť zverejnené na internetovej adrese podľa kapitoly 3.2,
- ukončenie činnosti musí byť riadený proces prebiehajúci podľa dopredu pripraveného plánu, ktorého súčasťou musí byť popis postupu uchovávania a sprístupňovania informácií pre poskytovanie dôkazov v súdnom procese a pre účely zaistenia kontinuity služieb.

Poskytovateľ sa zaväzuje poskytovať kvalifikovanú validačnú službu ešte po dobu 6 mesiacov odo dňa oznámenia o ukončení činnosti. V prípade odobratia štatútu kvalifikovaného poskytovateľa dôveryhodných služieb podľa platnej legislatívy:

- informácia o odobratí štatútu musí byť písomne alebo elektronicky oznámená všetkým subjektom, ktoré majú uzatvorenú zmluvu na využívanie kvalifikovanej validačnej služby,
- informácia o odobratí štatútu musí byť zverejnená v súlade s kapitolou 3.2 tejto CP,
- o ďalšom postupe rozhodne CEO spoločnosti brainit.sk na základe rozhodnutí orgánu dohľadu.

## 9.12 Zhoda a právne požiadavky

Pre zhodu a právne požiadavky platia ustanovenia, uvedené v politike pre poskytovanie dôveryhodných služieb a naviac Poskytovateľ musí poskytovať svoje služby nasledovne:

- poskytovateľ musí prijať vhodné technické a organizačné opatrenia proti neautorizovanému alebo protiprávnemu spracovávaniu osobných údajov a proti strate, zničeniu alebo poškodeniu osobných údajov,
- poskytovateľ validačnej služby neuchováva validovaný dokument po jeho spracovaní a overení,
- poskytovateľ nesie celkovú zodpovednosť za splnenie požiadaviek definovaných v kapitolách 6 až 9, a to aj keď niektoré alebo všetky jeho funkcie sú využívané subdodávateľmi.

# 10 Technické bezpečnostné opatrenia

Technická časť infraštruktúry Poskytovateľa (hardvér a softvér) musí pozostávať len z legálneho softvéru a bezpečných systémov. Architektúra infraštruktúry Poskytovateľa musí byť navrhnutá s použitím komponentov, ktoré vyhovujú bezpečnostným štandardom na úrovni súčasných poznatkov. V tejto kapitole sú ďalej definované bezpečnostné požiadavky na jednotlivé oblasti pre zaistenie kvality poskytovanej kvalifikovanej validačnej služby podľa tejto CP.

## 10.1 Bezpečnosť životného cyklu

### *10.1.1 Riadenie vývoja softvéru*

Pri vývoji softvéru sa musí postupovať v súlade s internou dokumentáciou a best practice postupov pre vývoj softvéru.

### *10.1.2 Kontroly riadenia bezpečnosti*

Súlad voči všetkým štandardom, ktoré Poskytovateľ deklaruje musí byť overovaný pravidelnými auditmi a kontrolami bezpečnostných zhôd.

### *10.1.3 Riadenie bezpečnosti životného cyklu*

Riadenie bezpečnosti životného cyklu musí byť v spoločnosti brainit.sk vykonávané procesným prístupom typu PDCA (Plan-Do-Act-Check), ktorý sa musí skladať z nasledujúcich procesov:

- vybudovanie – stanovenie rozsahu a hraníc, ktorých sa riadenie informačnej bezpečnosti týka, určenia bezpečnostnej politiky, určenie plánu a výber bezpečnostných opatrení v závislosti na vyhodnotených rizikách,
- implementácia – účelné a systematické presadenie vybraných bezpečnostných opatrení,
- monitorovanie a prehodnocovanie – zaistenie spätnej väzby, pravidelné sledovanie a hodnotenie úspešných aj neúspešných a nedostatočných stránok riadenia informačnej bezpečnosti, poskytovanie zistení vedeniu spoločnosti k posúdeniu,
- údržba a zlepšovanie – vykonávané opatrenia k náprave a zlepšovaniu, na základe rozhodnutí vedenia spoločnosti.

# 11 Audit súladu a ďalšie hodnotenia

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

## 11.1 Frekvencia alebo okolnosti posudzovania

Pre zaistenie definovanej úrovne bezpečnosti infraštruktúry a tým aj vysokej kvality poskytovaných služieb, musí byť vykonávaná pravidelná kontrola zhody. Táto kontrola je vykonávaná minimálne raz za 12 mesiacov formou interného bezpečnostného auditu.

Ďalšie pravidelné audity dané nariadením eIDAS a vykonávané k tomu určeným akreditovaným posudzovateľom zhody musia byť vykonávané vždy v intervale kratšom ako 24 mesiacov.

## 11.2 Totožnosť a kvalifikácia posudzovateľa

Orgán posudzovania zhody a nim poverené osoby na výkon auditu musí spĺňať požiadavky ETSI EN 319 403 „Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers“ minimálne vo verzii 2.2.2 v súlade s certifikačnou schémou NBÚ, ktorá upravuje požiadavky tejto normy.

## 11.3 Vzťah hodnotiteľa k hodnotenému subjektu

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

Pravidelná kontrola poskytovania služby musí byť vykonávaná internými zamestnancami Poskytovateľa.

V prípade externého posudzovateľa platí, že sa jedná o nestranný subjekt a nedochádza k stretu záujmov.

## 11.4 Hodnotené oblasti

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

## 11.5 Opatrenia prijaté v dôsledku nedostatku

Keď audítor zistí rozpor medzi prevádzkou Poskytovateľa a platnými požiadavkami alebo ustanoveniami CP a vydaných CPS, musia sa uskutočniť nasledujúce akcie:

- audítor musí upovedomiť o rozpore subjekty definované v časti 11.6,
- rozpor musí byť zaznamenaný,
- PMA musí určiť vhodné opatrenie na nápravu.

## 11.6 Postup v prípade zistených nedostatkov

Všetky zistené nedostatky musia byť komunikované v rámci auditnej správy. Podľa charakteru nedostatku sú naplánované a vykonané činnosti technologického (konfiguračné zmeny, implementácia ďalších technologických opatrení atď.) charakteru a/alebo doplnená a aktualizovaná relevantná dokumentácia tak, aby bol nedostatok odstránený.

### 11.7 Oznámenie výsledkov

Orgán posudzovania zhody musí výsledky auditu predložiť v písomnej alebo elektronickej forme auditovanému subjektu, ktorý na ich základe musí vykonať a prijať potrebné nápravné opatrenia. Vykonanie opatrení na nápravu musí byť dané na vedomie orgánu posudzovania zhody.

V lehote troch pracovných dní od jej doručenia je Poskytovateľ povinný predložiť výslednú správu o posúdení zhody orgánu dohľadu.

## 12 Plnenie požiadaviek pre kvalifikovanú validačnú službu kvalifikovaných elektronických podpisov a pečatí podľa nariadenia eIDAS

### 12.1 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.

### 12.2 Plnenie požiadaviek eIDAS

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

#### *12.2.1 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 politike poskytovania dôveryhodných služieb, ktorý popisuje všeobecné pravidlá pri poskytovaní dôveryhodných služieb.

#### *12.2.2 Plnenie požiadaviek 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 validačného procesu je realizovaná pomocou webového portálu NFQES pomocou webového portálu https://zone.nfqes.com, 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 v2.1.1,
- 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.

Výsledná správa z validačného procesu, 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 5.2.4 Schémy dohľadu NBÚ SR.

Výsledná správa z validačného procesu je vytvorená z týchto rozšírených dát. Správa môže byť vytvorená vo formátoch uvedených v kapitole 6.7.

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

## 12.3 Certifikát verejného kľúča VSU a zdroj kvalifikovaných pečiatok

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

# 13 Odkazy

- 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
- Bezpečnostná Politika poskytovania dôveryhodných služieb spoločnosti brainit.sk
- Nariadenie Európskeho Parlamentu a Rady (EÚ) 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov
- 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. 18/2018 Z. z. o ochrane osobných údajov
- Informácia o spracúvaní osobných údajov
- Všeobecné podmienky poskytovania a používania dôveryhodnej služby vyhotovovania a overovania certifikátov brainit.sk, s.r.o.
- SD Schéma dohľadu kvalifikovaných dôveryhodných služieb definovaná orgánom dohľadu
- ETSI EN 319 411-2 V2.1.1 (2016-02) 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 319 411-1 V1.1.1 (2016-02) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
- Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework (RFC3647)
- Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (RFC5280)
- X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP (RFC6960)
- OCRA: OATH Challenge-Response Algorithm (RFC6287)

**Príloha A**

Spoločné obmedzenia overovania podpisov pre politiku overovania **QES** (1.3.158.52577465.0.0.0.1.7.1.1):

- **FAIL** - ak nie je splnené obmedzenie, validácia zobrazí chybu,
- **WARN** – ak obmedzenie nie je splnené, validácia zobrazí varovanie
- **IGNORE** – obmedzenie sa ignoruje

| Obmedzenie | Indikátor |
| --- | --- |
| **Obmedzenie kontajnerov** | |
| Akceptované typy kontajnerov:<br>ASiC-S<br>ASiC-E | FAIL |
| Je prítomný súbor MimeType | FAIL |
| Prijateľný obsah súboru MimeType:<br>application/vnd.etsi.asic-s+zip<br>application/vnd.etsi.asic-e+zip | WARN |
| Je prítomný súbor Manifest | FAIL |
| Všetky súbory sú podpísané | WARN |
| **Obmedzenia podpisu** | |
| Prijateľné politiky:<br>ANY_POLICY<br>NO_POLICY | FAIL |
| Politiky sú k dispozícii | FAIL |
| Zhodujú sa hashe politík | FAIL |
| Existujú referenčné údaje | FAIL |
| Referenčné údaje sú neporušené | FAIL |
| Existuje manifest vstupný objekt | WARN |
| Podpis je neporušený | FAIL |
| Potenciálny reťazec certifikátov | FAIL |
| Rozpoznanie podpisového certifikátu | FAIL |
| Podpisový certifikát podpisu | FAIL |
| Kvalifikácia podpisového certifikátu | FAIL |
| Podpisový certifikát podporuje QSCD | FAIL |
| Platnosť podpisového certifikátu neskončila | WARN |
| Existuje prístup k informáciám o podpisovej certifikačnej autorite | WARN |
| Existuje prístup k informáciám o zrušení podpisu certifikátu | WARN |
| K dispozícii sú údaje o zrušení podpisového certifikátu | FAIL |
| Je prítomná ďalšia aktualizácia podpisového certifikátu | WARN |
| Podpisovanie aktuálnosti údajov o zrušení certifikátu | WARN |
| Použitie kľúča podpisového certifikátu obsahuje „nonRepudiation“ | WARN |
| Je uvedené sériové číslo podpisového certifikátu | WARN |
| Podpisový certifikát nie je zrušený | FAIL |
| Podpisový certifikát nie je pozastavený | FAIL |
| Podpisový certifikát nie je vlastnoručne podpísaný | WARN |
| Certifikačný podpis certifikačnej autority | FAIL |
| Platnosť certifikátu certifikačnej autority neskončila | WARN |
| Údaje o zrušení certifikátu certifikačnej autority sú k dispozícii | FAIL |
| K dispozícii sú údaje o zrušení certifikátu certifikačnej autority pri ďalšej aktualizácii | WARN |
| Aktuálnosť údajov o zrušení certifikátu certifikačnej autority | WARN |

| | |
|---|---|
| Certifikát certifikačnej autority nie je zrušený | FAIL |
| Certifikát certifikačnej autority nie je pozastavený | FAIL |
| Podpísané atribúty obsahujú podpisový certifikát | FAIL |
| Podpísané atribúty obsahujú súhrn podpisového certifikátu | FAIL |
| Súhrn podpisového certifikátu v zhode podpísaných atribútov | FAIL |
| Sériový súhrn vydavateľa v zhode podpísaných atribútov | WARN |
| Podpísané atribúty obsahujú čas podpisu | FAIL |
| Podpísané atribúty obsahujú súhrn správy alebo podpísané vlastnosti | FAIL |
| **Obmedzenia časovej pečiatky** | |
| Čas revokácie je proti najlepšiemu času podpisu | FAIL |
| Najlepší čas podpisu je pred dátumom vydania politiky podpisu certifikátu | FAIL |
| Súdržnosť | WARN |
| Existujú referenčné dáta | FAIL |
| Referenčné dáta sú neporušené | FAIL |
| Podpis je neporušený | FAIL |
| Potenciálny reťazec certifikátov | FAIL |
| Rozpoznanie podpisového certifikátu | FAIL |
| Podpisový certifikát podpisu | FAIL |
| Platnosť podpisového certifikátu neskončila | WARN |
| Sú k dispozícii údaje o zrušení podpisového certifikátu | FAIL |
| Je prítomná ďalšia aktualizácia podpisového certifikátu | WARN |
| Podpisovanie aktuálnosti údajov o zrušení certifikátu | WARN |
| Použitie kľúča podpisového certifikátu obsahuje „časovú pečiatku“ | WARN |
| Podpisový certifikát nie je zrušený | FAIL |
| Podpisový certifikát nie je pozastavený | FAIL |
| Podpisový certifikát nie je vlastnoručne podpísaný | WARN |
| Certifikačný podpis certifikačnej autority | FAIL |
| Platnosť certifikátu certifikačnej autority neskončila | WARN |
| Údaje o zrušení certifikátu certifikačnej autority sú k dispozícii | WARN |
| K dispozícii sú údaje o zrušení certifikátu certifikačnej autority pri ďalšej aktualizácii | WARN |
| Aktuálnosť údajov o zrušení certifikátu certifikačnej autority | WARN |
| Certifikát certifikačnej autority nie je zrušený | FAIL |
| Certifikát certifikačnej autority nie je pozastavený | FAIL |
| **Obmedzenia odvolania (revocation)** | |
| Existujú referenčné dáta | FAIL |
| Referenčné údaje sú neporušené | FAIL |
| Podpis je neporušený | FAIL |
| Potenciálny reťazec certifikátov | WARN |
| Rozpoznanie podpisového certifikátu | FAIL |
| Podpisový certifikát podpisu | FAIL |
| Platnosť podpisového certifikátu neskončila | WARN |
| K dispozícii sú údaje o zrušení podpisového certifikátu | IGNORE |
| Je prítomná ďalšia aktualizácia podpisového certifikátu | IGNORE |
| Podpisovanie aktuálnosti údajov o zrušení certifikátu | IGNORE |
| Podpisový certifikát nie je zrušený | IGNORE |
| Podpisový certifikát nie je pozastavený | IGNORE |
| Certifikačný podpis certifikačnej autority | FAIL |
| Platnosť certifikátu certifikačnej autority neskončila | IGNORE |
| Údaje o zrušení certifikátu certifikačnej autority sú k dispozícii | IGNORE |
| K dispozícii sú údaje o zrušení certifikátu certifikačnej autority pri ďalšej aktualizácii | IGNORE |

| | |
|---|---|
| Aktuálnosť údajov o zrušení certifikátu certifikačnej autority | IGNORE |
| Certifikát certifikačnej autority nie je zrušený | IGNORE |
| Certifikát certifikačnej autority nie je pozastavený | IGNORE |
| **Obmedzenia dôveryhodného listu** | |
| Aktuálnosť zoznamu dôveryhodných informácií (6 hodín) | WARN |
| Platnosť dôveryhodného zoznamu ešte nevypršala | WARN |
| Dôveryhodný zoznam je dobre podpísaný | FAIL |
| Verzia dôveryhodného zoznamu 5 | FAIL |
| Konzistencia dôveryhodného zoznamu | FAIL |
| **Kryptografické obmedzenia** | |
| Prijateľné šifrovacie algoritmy:<br>RSA – (minimálna veľkosť kľúča 1024)<br>DSA – (minimálna veľkosť kľúča 160)<br>ECDSA – (minimálna veľkosť kľúča 160)<br>PLAIN-ECDSA – (minimálna veľkosť kľúča 160) | FAIL |
| Prijateľné algoritmy spracovania: SHA1, SHA224, SHA256, SHA384, SHA512, SHA3-224, SHA3-256, SHA3-384, SHA3-512, RIPEMD160, WHIRLPOOL | FAIL |
| Dátum vypršania platnosti algoritmu:<br>SHA1 – 2009<br>SHA224 – 2023<br>SHA256 – 2026<br>SHA384 – 2026<br>SHA512 – 2026<br>SHA3-224 – 2026<br>SHA3-256 – 2026<br>SHA3-384 – 2026<br>SHA3-512 – 2026<br>RIPEMD160 - 2011<br>WHIRLPOOL – 2015<br>DSA 160 – 2013<br>DSA 192 – 2013<br>DSA 224 – 2023<br>DSA 256 – 2026<br>RSA 1024 – 2009<br>RSA 1536 – 2016<br>RSA 2048 – 2023<br>RSA 3072 – 2026<br>RSA 4096 – 2026<br>ECDSA 160 – 2013<br>ECDSA 192 - 2013<br>ECDSA 224 – 2016<br>ECDSA 256 – 2026<br>ECDSA 384 – 2026<br>ECDSA 512 – 2026<br>PLAIN-ECDSA 160 – 2013<br>PLAIN-ECDSA 192 – 2013<br>PLAIN-ECDSA 224 – 2016<br>PLAIN-ECDSA 256 – 2026<br>PLAIN-ECDSA 384 – 2026<br>PLAIN-ECDSA 512 – 2026 | FAIL |

## Príloha B

Spoločné obmedzenia overovania podpisov pre politiku overovania AdES (1.3.158.52577465.0.0.0.1.7.1.2):

- **FAIL -** ak nie je splnené obmedzenie, validácia zobrazí chybu,
- **WARN –** ak obmedzenie nie je splnené, validácia zobrazí varovanie,
- **IGNORE –** obmedzenie sa ignoruje.

| Obmedzenie | Indikátor |
| --- | --- |
| **Obmedzenie kontajnerov** | |
| Akceptované typy kontajnerov:<br>ASiC-S<br>ASiC-E | FAIL |
| Je prítomný súbor MimeType | FAIL |
| Prijateľný obsah súboru MimeType:<br>application/vnd.etsi.asic-s+zip<br>application/vnd.etsi.asic-e+zip | WARN |
| Je prítomný súbor Manifest | FAIL |
| Všetky súbory sú podpísané | WARN |
| **Obmedzenia podpisu** | |
| Prijateľné politiky:<br>ANY_POLICY<br>NO_POLICY | FAIL |
| Politiky sú k dispozícii | FAIL |
| Zhodujú sa hashe politík | IGNORE |
| Existujú referenčné údaje | IGNORE |
| Referenčné údaje sú neporušené | FAIL |
| Existuje manifest vstupný objekt | WARN |
| Podpis je neporušený | WARN |
| Potenciálny reťazec certifikátov | FAIL |
| Rozpoznanie podpisového certifikátu | WARN |
| Podpisový certifikát podpisu | WARN |
| Kvalifikácia podpisového certifikátu | WARN |
| Podpisový certifikát podporuje QSCD | WARN |
| Platnosť podpisového certifikátu neskončila | FAIL |
| Existuje prístup k informáciám o podpisovej certifikačnej autorite | FAIL |
| Existuje prístup k informáciám o zrušení podpisu certifikátu | WARN |
| K dispozícii sú údaje o zrušení podpisového certifikátu | FAIL |
| Je prítomná ďalšia aktualizácia podpisového certifikátu | WARN |
| Podpisovanie aktuálnosti údajov o zrušení certifikátu | WARN |
| Použitie kľúča podpisového certifikátu obsahuje „nonRepudiation“ | WARN |
| Je uvedené sériové číslo podpisového certifikátu | WARN |
| Podpisový certifikát nie je zrušený | FAIL |
| Podpisový certifikát nie je pozastavený | FAIL |
| Podpisový certifikát nie je vlastnoručne podpísaný | WARN |
| Certifikačný podpis certifikačnej autority | FAIL |
| Platnosť certifikátu certifikačnej autority neskončila | WARN |
| Údaje o zrušení certifikátu certifikačnej autority sú k dispozícii | FAIL |
| K dispozícii sú údaje o zrušení certifikátu certifikačnej autority pri ďalšej aktualizácii | WARN |
| Aktuálnosť údajov o zrušení certifikátu certifikačnej autority | WARN |

| | |
|---|---|
| Certifikát certifikačnej autority nie je zrušený | FAIL |
| Certifikát certifikačnej autority nie je pozastavený | FAIL |
| Podpísané atribúty obsahujú podpisový certifikát | FAIL |
| Podpísané atribúty obsahujú súhrn podpisového certifikátu | FAIL |
| Súhrn podpisového certifikátu v zhode podpísaných atribútov | FAIL |
| Sériový súhrn vydavateľa v zhode podpísaných atribútov | WARN |
| Podpísané atribúty obsahujú čas podpisu | FAIL |
| Podpísané atribúty obsahujú súhrn správy alebo podpísané vlastnosti | FAIL |
| **Obmedzenia časovej pečiatky** | |
| Čas revokácie je proti najlepšiemu času podpisu | FAIL |
| Najlepší čas podpisu je pred dátumom vydania politiky podpisu certifikátu | FAIL |
| Súdržnosť | WARN |
| Existujú referenčné dáta | FAIL |
| Referenčné dáta sú neporušené | FAIL |
| Podpis je neporušený | FAIL |
| Potenciálny reťazec certifikátov | FAIL |
| Rozpoznanie podpisového certifikátu | FAIL |
| Podpisový certifikát podpisu | FAIL |
| Platnosť podpisového certifikátu neskončila | WARN |
| Sú k dispozícii údaje o zrušení podpisového certifikátu | FAIL |
| Je prítomná ďalšia aktualizácia podpisového certifikátu | WARN |
| Podpisovanie aktuálnosti údajov o zrušení certifikátu | WARN |
| Použitie kľúča podpisového certifikátu obsahuje „časovú pečiatku“ | WARN |
| Podpisový certifikát nie je zrušený | FAIL |
| Podpisový certifikát nie je pozastavený | FAIL |
| Podpisový certifikát nie je vlastnoručne podpísaný | WARN |
| Certifikačný podpis certifikačnej autority | FAIL |
| Platnosť certifikátu certifikačnej autority neskončila | WARN |
| Údaje o zrušení certifikátu certifikačnej autority sú k dispozícii | WARN |
| K dispozícii sú údaje o zrušení certifikátu certifikačnej autority pri ďalšej aktualizácii | WARN |
| Aktuálnosť údajov o zrušení certifikátu certifikačnej autority | WARN |
| Certifikát certifikačnej autority nie je zrušený | FAIL |
| Certifikát certifikačnej autority nie je pozastavený | FAIL |
| **Obmedzenia odvolania (revocation)** | |
| Existujú referenčné dáta | FAIL |
| Referenčné údaje sú neporušené | FAIL |
| Podpis je neporušený | FAIL |
| Potenciálny reťazec certifikátov | WARN |
| Rozpoznanie podpisového certifikátu | FAIL |
| Podpisový certifikát podpisu | FAIL |
| Platnosť podpisového certifikátu neskončila | WARN |
| K dispozícii sú údaje o zrušení podpisového certifikátu | IGNORE |
| Je prítomná ďalšia aktualizácia podpisového certifikátu | IGNORE |
| Podpisovanie aktuálnosti údajov o zrušení certifikátu | IGNORE |
| Podpisový certifikát nie je zrušený | IGNORE |
| Podpisový certifikát nie je pozastavený | IGNORE |
| Certifikačný podpis certifikačnej autority | FAIL |
| Platnosť certifikátu certifikačnej autority neskončila | IGNORE |
| Údaje o zrušení certifikátu certifikačnej autority sú k dispozícii | IGNORE |
| K dispozícii sú údaje o zrušení certifikátu certifikačnej autority pri ďalšej aktualizácii | IGNORE |

| | |
|---|---|
| Aktuálnosť údajov o zrušení certifikátu certifikačnej autority | IGNORE |
| Certifikát certifikačnej autority nie je zrušený | IGNORE |
| Certifikát certifikačnej autority nie je pozastavený | IGNORE |
| **Obmedzenia dôveryhodného listu** | |
| Aktuálnosť zoznamu dôveryhodných informácií (6 hodín) | WARN |
| Platnosť dôveryhodného zoznamu ešte nevypršala | WARN |
| Dôveryhodný zoznam je dobre podpísaný | FAIL |
| Verzia dôveryhodného zoznamu 5 | FAIL |
| Konzistencia dôveryhodného zoznamu | FAIL |
| **Kryptografické obmedzenia** | |
| Prijateľné šifrovacie algoritmy:<br>RSA – (minimálna veľkosť kľúča 1024)<br>DSA – (minimálna veľkosť kľúča 160)<br>ECDSA – (minimálna veľkosť kľúča 160)<br>PLAIN-ECDSA – (minimálna veľkosť kľúča 160) | FAIL |
| Prijateľné algoritmy spracovania: SHA1, SHA224, SHA256, SHA384, SHA512, SHA3-224, SHA3-256, SHA3-384, SHA3-512, RIPEMD160, WHIRLPOOL | FAIL |
| Dátum vypršania platnosti algoritmu:<br>SHA1 – 2009<br>SHA224 – 2023<br>SHA256 – 2026<br>SHA384 – 2026<br>SHA512 – 2026<br>SHA3-224 – 2026<br>SHA3-256 – 2026<br>SHA3-384 – 2026<br>SHA3-512 – 2026<br>RIPEMD160 - 2011<br>WHIRLPOOL – 2015<br>DSA 160 – 2013<br>DSA 192 – 2013<br>DSA 224 – 2023<br>DSA 256 – 2026<br>RSA 1024 – 2009<br>RSA 1536 – 2016<br>RSA 2048 – 2023<br>RSA 3072 – 2026<br>RSA 4096 – 2026<br>ECDSA 160 – 2013<br>ECDSA 192 - 2013<br>ECDSA 224 – 2016<br>ECDSA 256 – 2026<br>ECDSA 384 – 2026<br>ECDSA 512 – 2026<br><br>PLAIN-ECDSA 160 – 2013<br>PLAIN-ECDSA 192 – 2013<br>PLAIN-ECDSA 224 – 2016<br>PLAIN-ECDSA 256 – 2026<br>PLAIN-ECDSA 384 – 2026<br>PLAIN-ECDSA 512 – 2026 | FAIL |