DKDS4 Certifikačná politika poskytovania dôveryhodnej služby uchovávania kvalifikovaných elektronických podpisov a pečatí

Názov dokumentu:	DKDS4 Certifikačná politika poskytovania dôveryhodnej služby uchovávania kvalifikovaných elektronických podpisov a pečatí		
Označenie dokumentu:	cp_archive_snca.pdf		
Verzia:	1.3	Status:	*Finálna verzia*
Dátum vytvorenia:	6.12.2023	Platný do:	

História dokumentu

História revízií dokumentu

Verzia	Dátum	Popis zmeny	Autor / Autor zmien
0.9	18.11.2020	Úvodná verzia	Ing. Marián Štefánek
1.0	30.11.2020	Finálna verzia	Tibor Berešík
1.1	03.05.2021	Doplnenie SNCA4, formálne úpravy	Štefan Szilva
1.2	20.05.2021	Formálne úpravy	Štefan Szilva
1.3	06.12.2023	Zmena adresy detašovaného pracoviska a webového sídla. Aktualizácia informácií o podporovaných formátoch	Štefan Szilva

Schválenia

Verzia	Funkcia	V zastúpení	Schválil dňa	Podpis
1.0	GR NASES		30.11.2020	
1.3	GR NASES		06.12.2023	

Referencie na legislatívne a normatívne dokumenty

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

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

[3] ETSI SR 019 510 v.1.1.1 - Electronic Signatures and Infrastructures (ESI); Scoping study and framework for standardization of long-term data preservation services, including preservation of/with digital signatures.
ETSI SR 019 510 v.1.1.1

[4] 6737/2016/IBEP/OA-003. Disig QES Signer 4 - Deklarácia výrobcu aplikácie pre kvalifikovaný elektronický podpis/pečať (QES), NBÚ SR.
Disig QES Signer 4 - Deklarácia výrobcu

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

[6] ETSI TS 103 172 v.2.2.2 - Electronic Signatures and Infrastructures (ESI); PAdES Baseline Profile.
ETSI TS 103 172 v.2.2.2

[7] ETSI TS 103 171 v.2.1.1 - Electronic Signatures and Infrastructures (ESI); XAdES Baseline Profile.
ETSI TS 103 171 v.2.1.1

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

[9] ISO 32000-1:2008 - Document management - Portable document format.
ISO 32000-1:2008 Document management - Portable document format

[10] 05968/2019/ORD-001 - Schéma dohľadu kvalifikovaných dôveryhodných služieb definovaná orgánom dohľadu, Verzia 1.4, NBÚ SR (ďalej aj „schéma dohľadu“).
Schéma dohľadu KDS definovaná orgánom dohľadu

[11] ETSI EN 319 401 v.2.2.1 - Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.
ETSI EN 319 401 v.2.2.1

[12] ETSI TS 119 312 v.1.3.1 - Electronic Signatures and Infrastructures (ESI); Cryptographic Suites.
ETSI TS 119 312 v.1.3.1

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

[14] ETSI EN 319 411-1 v.1.2.2 - Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.
ETSI EN 319 411-1 v.1.2.2

[15] RFC 3647 - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.
RFC 3647

[16] ETSI TS 102 853 v.1.1.1 - Electronic Signatures and Infrastructures (ESI); Signature verification procedures and policies.
ETSI TS 102 853 v.1.1.1

[17] ETSI EN 319 102-1 v.1.0.0 - Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation.
ETSI EN 319 102-1 v.1.0.0.E (Draft)

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

Zoznam tabuliek

Použité definície a skratky

Tabuľka 1 Použité definície

Definícia	Vysvetlenie definície
Univerzálny koordinovaný čas	Časová škála, založená na sekunde podľa definície v Recommendation ITU-R TF.460-6, „svetový čas“.
Autorita časovej pečiatky	TSP poskytujúci služby vyhotovovania časovej pečiatky použitím jednej alebo viacerých TSU.
Jednotka archivačnej služby	Sústava technických a programových prostriedkov, ktorá je spravovaná ako jednotka.
Poskytovateľ dôveryhodnej služby	Entita, ktorá poskytuje jednu alebo viac dôveryhodných služieb.

Tabuľka 2 Použité skratky

Skratka	Vysvetlenie skratky
CA	Certifikačná autorita.
CP	Certifikačná politika.
IT	Informačné technológie.
LTA	Long Term with Archive time-stamps.
Nariadenie eIDAS	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.
NASES	Národná agentúra pre sieťové a elektronické služby.
NBÚ	Národný bezpečnostný úrad.
PKI	Infraštruktúra verejného kľúča (Public Key Infrastructure).
PMA	Autorita pre riadenie politík (Policy Management Authority).
PSU	Samostatná jednotka archivačnej služby (Preservation Service Unit).
SCVA	Aplikácia na vyhotovovanie a overovanie podpisu/pečate (Signature/ Seal Creation & Verification Application).
SNCA	Slovenská národná certifikačná autorita.
SR	Slovenská republika.
SW	Softvér (Software).

TSA	Autorita časovej pečiatky, vydavateľ časovej pečiatky (Time-Stamping Authority).
TSP	Poskytovateľ dôveryhodnej služby (Trust Service Provider).
TWS	Dôveryhodný systém (Trustworthy System).

Obsah

1 Úvod

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

Poskytovateľom tejto dôveryhodnej služby je Národná agentúra pre sieťové a elektronické služby so sídlom Kollárova 8, 917 02 Trnava, Detašované pracovisko: Tower 115, Pribinova 25, 811 09 Bratislava, IČO: 42 156 424 (ďalej aj „Poskytovateľ“ alebo „NASES“), prostredníctvom svojho systému archivačnej služby (ďalej aj „AS SNCA“).

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

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

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

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

1.1 Prehľad

Táto certifikačná politika sa týka poskytovania dôveryhodnej služby:

- uchovávanie kvalifikovaných elektronických podpisov a kvalifikovaných elektronických pečatí

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

2 Názov dokumentu a jeho identifikácia

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

1.3.158.42156424.0.1.7

kde jednotlivé zložky OID majú nasledovný význam:

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

2.1 Účastníci PKI

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

2.1.1 Jednotka archivačnej služby

Jednotka archivačnej služby (PSU):

- je entita, ktorá poskytuje kvalifikovanú dôveryhodnú službu uchovávania kvalifikovaných elektronických podpisov a kvalifikovaných elektronických pečatí pre používateľov (Odberatelia, Spoliehajúce sa strany),
- má celkovú zodpovednosť za poskytovanie kvalifikovanej dôveryhodnej služby, špecifikovanej v odstavci 1.1,
- zaručuje, že všetky aspekty jej služieb, operácií a infraštruktúry, zviazanej so správami z archivácie, vydanými podľa tejto politiky, sú vykonávané v súlade s jej požiadavkami a ustanoveniami a v súlade s pravidlami na výkon certifikačných činností Poskytovateľa.

2.1.2 Odberateľ

Odberateľom sa rozumie orgán verejnej moci, ktorému Poskytovateľ poskytuje archivačnú službu a ten, na koho sa viažu záväzky odberateľa.

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

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

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

2.1.3 Spoliehajúca sa strana

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

2.1.4 Iní účastníci

PMA je zložka Poskytovateľa, ustanovená za účelom:

- dohľadu nad vytváraním a aktualizáciou certifikačnej politiky, vrátane vyhodnocovania zmien a plánov na implementovanie ľubovoľných prijatých zmien ,
- revízie výsledkov auditov, aby sa určilo, či Poskytovateľ zodpovedne dodržiava ustanovenia, vydané certifikačnou politikou,
- vydávania odporúčaní pre Poskytovateľa, týkajúcich sa nápravných a iných vhodných opatrení,
- riadenia a usmerňovania činnosti Poskytovateľa a registračných autorít,
- vydávania technologických certifikátov pre vnútornú potrebu SNCA,
- zrušovania certifikátov SNCA a ďalších certifikátov, vydávaných SNCA.

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

2.2 Použiteľnosť správy z archivácie

Uchované dokumenty, resp. uchované kvalifikované elektronické podpisy, resp. kvalifikované elektronické pečate k nim prislúchajúce, sú použiteľné všade tam, kde sa vyžaduje platný kvalifikovaný elektronický podpis, resp. kvalifikovaná elektronická pečať.

2.3 Správa politiky

2.3.1 Organizácia zodpovedná za správu dokumentu

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

Kontaktná adresa:

Národná agentúra pre sieťové a elektronické služby

Detašované pracovisko:

Tower 115,

Pribinova 25,

811 09 Bratislava,

Slovenská republika,

https://snca.gov.sk

2.3.2 Kontaktná osoba

Bezpečnostný správca SNCA.

Národná agentúra pre sieťové a elektronické služby

Detašované pracovisko:

Tower 115,

Pribinova 25,

811 09 Bratislava,

Slovenská republika,

Telefón: +421 2 3278 0700

e-mail: info@nases.gov.sk

2.3.3 Osoba rozhodujúca o súlade CPS s CP

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

Vo všetkých záležitostiach a aspektoch, týkajúcich sa Poskytovateľa a jeho činností, s konečnou platnosťou rozhoduje riaditeľ organizačného útvaru, ktorý prevádzkuje SNCA.

2.3.4 Postupy schvaľovania CP

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

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

3 Zverejňovanie informácií a úložiská

3.1 Úložiská

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

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

https://snca.gov.sk

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

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

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

3.2 Zverejňovanie informácií o archivačnej službe

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

- túto certifikačnú politiku,
- certifikáty služieb časových pečiatok, ktoré sú využívané v rámci archivačnej služby,
- ďalšie dokumenty súvisiace s poskytovaním archivačnej služby v zmysle tejto CP.

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

https://snca.gov.sk

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

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

3.3 Frekvencia zverejňovania informácií

Informácie o zrušenom certifikáte PSU musia byť dostupné na webovom sídle SNCA, ktoré slúži ako jeho úložisko.

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

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

3.4 Kontroly prístupu

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

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

4 Všeobecné ustanovenia

4.1 Všeobecné ustanovenia politiky

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

Očakáva sa, že odberatelia a spoliehajúce sa strany budú konzultovať podrobnosti spôsobu poskytovania archivačnej služby priamo s poskytujúcou PSU Poskytovateľa.

4.2 Služby súvisiace s archivačnou službou

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

- Poskytovanie archivačnej služby – táto služba plní samotnú funkcionalitu uchovávania kvalifikovaných elektronických podpisov a kvalifikovaných elektronických pečatí pre Odberateľa.
- Manažment archivačnej služby – táto služba monitoruje a riadi procesy archivačnej služby, aby sa zaistilo, že služba je poskytovaná v súlade s touto certifikačnou politikou. Súčasťou tohto manažmentu je proces aktivácie resp. de-aktivácie archivačnej služby.

4.3 Poskytovateľ archivačnej služby

Poskytovateľ archivačnej služby pre potreby Odberateľov v zmysle tejto certifikačnej politiky je agentúra NASES .

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

4.4 Používateľ archivačnej služby

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

5 Úvod do politiky archivačnej služby a plnenie všeobecných požiadaviek

5.1 Všeobecne

Tento dokument definuje certifikačnú politiku poskytovania dôveryhodnej služby uchovávania kvalifikovaných elektronických podpisov a kvalifikovaných elektronických pečatí Poskytovateľom, ktorá uchováva platnosť kvalifikovaných podpisov a kvalifikovaných elektronických pečatí počas dlhšej doby ako je platnosť ich kvalifikovaných certifikátov.

Táto politika pokrýva odporúčania o dlhodobej politike uchovávania z klauzuly 4.8 dokumentu ETSI SR 019 510 v1.1.1 [3].

5.2 Cieľoví používatelia a použitie

5.2.1 Správna prax uplatňovania politiky archivačnej služby

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

5.3 Zmena politiky archivačnej služby

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

Typicky je zmena vyvolaná doplnením štandardov a legislatívnymi zmenami.

6 Politiky a pravidlá

6.1 Ohodnotenie rizík

Pozri kapitolu 5 dokumentu [2].

6.2 Pravidlá pre praktický výkon dôveryhodných služieb

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

6.3 Všeobecné podmienky

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

6.4 Politika informačnej bezpečnosti

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

6.5 Záväzky Poskytovateľa

6.5.1 Všeobecne

Poskytovateľ archivačnej služby sa zaväzuje:

- realizovať všetky požiadavky, kladené na Poskytovateľa v zmysle kapitoly 7 a 8;
- používať bezpečné systémy a zaisťovať dostatočnú bezpečnosť postupov, ktoré tieto systémy podporujú vrátane dostatočnej kryptografickej bezpečnosti týchto systémov;
- používať bezpečné systémy pre uchovávanie záznamov;
- zabezpečiť, aby prax prevádzky archivačnej služby zodpovedala procedúram popísaným v tejto certifikačnej politike .

6.5.2 Záväzky Poskytovateľa k Odberateľovi

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

6.6 Informácie pre spoliehajúce sa strany

Všeobecné podmienky, dostupné pre spoliehajúce sa strany (pozri odstavec 6.3) v prípade, že sa spoliehajú na uchovávané kvalifikované elektronické podpisy a kvalifikované elektronické pečate, musia zahŕňať nasledovné:

- Povinnosť uchovávať prístupové údaje k archivačnej službe na bezpečnom mieste, neprístupnom pre tretie strany.
- Všetky obmedzenia pre použitie archivačnej služby podľa tejto certifikačnej politiky.
- Všetky ďalšie obmedzenia, uvedené v dohodách alebo kdekoľvek inde.

7 Manažment a prevádzka archivačnej služby Poskytovateľa

7.1 Úvod

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

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

7.2 Vnútorná organizácia

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

Poskytovateľ:

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

7.3 Personálna bezpečnosť

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

7.4 Správa aktív

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

7.5 Riadenie prístupu

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

7.6 Kryptografické opatrenia

7.6.1 Kryptografické kľúče

Archivačná služba nepracuje so žiadnymi kryptografickými kľúčmi. Spolieha sa na dôveryhodnú službu kvalifikovanej časovej pečiatky.

7.6.2 Algoritmy a ich sila

Prevádzkovateľ služby garantuje sledovanie aktuálnych štandardov a životnosti kryptografických algoritmov a garantuje aktualizáciu aplikácií tak, aby podporovali a používali vždy aktuálne platné bezpečné algoritmy.

7.7 Uchovanie kvalifikovaného podpisu alebo pečate

7.7.1 Vymedzenie služby

Služba je realizovaná ako webová služba, prostredníctvom ktorej je možné zaradiť dokument do procesu archivácie (ďalej Notifikačný servis) a služba (servis) zabezpečujúca samotný proces archivácie. Zaradenie dokumentu predstavuje operáciu, prostredníctvom ktorej sú archivačnej službe poskytnuté iba meta-informácie o dokumente, určeného na archiváciu.

Samotné dokumenty sú fyzicky uchovávané na strane Odberateľa služby, prípadne na Spoliehajúcej sa strane. Tieto subjekty sprístupňujú archivačnej službe rozhranie (ďalej aj „DMSWS“), prostredníctvom ktorého si archivačná služba dokument stiahne na nevyhnutný čas na vykonanie archivačného procesu. Po rozšírení dokumentu (resp. podpisov dokumentu) do LTA formy, vráti archivačná služba takto obohatený dokument prostredníctvom rozhrania DMSWS naspäť Odberateľovi, prípadne Spoliehajúcej sa strane.

Archivačná služba publikuje Notifikačný servis, na ktorý sa Odberateľ integruje podľa príslušnej integračnej dokumentácie.

Odberateľ je povinný publikovať službu (implementovanú podľa integračnej dokumentácie k Archivačnej službe), prostredníctvom ktorej sprístupní dokumenty, určené na archiváciu archivačnej službe.

Archivačná služba realizuje schému uchovávania kvalifikovaných podpisov a pečatí typu „Dlhodobé uchovávanie AdES podpisov pomocou rozširovania podpisov s úložiskom“ podľa klauzuly 5.3 špeciálneho reportu ETSI SR 019 510 v1.1.1 [3]. Kontajner s dokumentami a podpismi, je prijatý Notifikačným servisom a je akciou, definovanou v bode 7.7.3 tejto certifika4nej politiky, zaradený do archivačného procesu. Kontajnery, zaradené do archivačného procesu, sú archivačnými mechanizmami rozširované do LTA formy a ďalej v tejto forme udržiavané až do vyradenia z archivačného procesu.

Keďže dokumenty, určené na archiváciu, sú uchovávané u klienta (Odberateľ/Spoliehajúca sa strana), používatelia môžu kedykoľvek dokument podať tretej strane na validáciu.

Všetky údaje, potrebné pre overenie, a teda aj dôkaz o uchovávaní, všetkých obsiahnutých podpisov/pečatí v danom kontajneri, sú uložené vo vnútri kontajneru, resp. v jeho podpisoch/pečatiach. Tretia strana musí byť schopná, pre overenie dôkazu o uchovávaní, validovať LTA formy AdES podpisov, obsiahnutých v kontajneri.

Archivačná služba musí vyhovovať technickým požiadavkám, ktoré sú definované v 5.1.

Certifikačná politika archivačnej služby, podľa ktorej sa archivačná služba riadi, je publikovaná na webovej stránke služby. Všetky dokumenty služby sa spracúvajú mechanizmom definovaným v tejto politike.

7.7.2 Spracovanie dát dokumentov zo vstupných kontajnerov

Používateľ pri práci s archivačnou službou odosiela archivačnej službe meta-informácie o dokumente, určenom na archiváciu. Archivačná služba na základe týchto meta-informácií dokument získa prostredníctvom DMSWS. Z charakteru tejto operácie vyplýva, že meta-informácie o dokumente sa od ich zaslania archivačnej službe prostredníctvom Notifikačného servisu, nesmú zmeniť. Rovnako dokument, ktorý archivačná služba spracuje do LTA formy, by nemal byť externými entitami menený.

Odstránenie, prípadne vyradenie dokumentu z procesu archivácie je možné vykonať tiež prostredníctvom Notifikačného servisu. Notifikačný servis ďalej umožňuje používateľovi služby zistiť, či daný dokument už je zaradený do procesu archivácie.

Dokumenty sa navyše krátkodobo, na nevyhnutnú dobu, nachádzajú aj v dočasnom úložisku SCVA aplikácie, ktorá s nimi narába vo vymedzených časových intervaloch, aby vykonala potrebné úkony s podpismi/pečaťami, časovými pečiatkami, resp. pri explicitnom vyvolaní vizualizácie dokumentu.

Archivačná služba spracúva dáta dokumentov v kontajneroch výlučne:

- iba v nevyhnutnej miere na výkon archivačnej služby (počítanie odtlačkov kryptografickými funkciami a pod.),
- na extrakciu/stiahnutie samotného dokumentu PMA, prípadne povereným pracovníkom.

Prístup k dokumentom má výhradne Používateľ a autorizovaný obslužný personál služby, ktorý sa riadi pravidlami z odstavca 6.5.

7.7.3 Akcia zaradenia do archivačnej služby

Notifikačný servis, po prijatí informácií o dokumente, určenom na archiváciu, zapíše tieto informácie do internej databázy, čím zaradí dokument do archivačnej služby. Pokiaľ je dokument v očakávanom formáte (viď 7.7.5.1), archivačná služba ho bude spracovávať.

Po zaradení súboru (archívu) do archivačnej služby, sú automaticky identifikované dokumenty a podpisy. Následne, prebieha automatizovaný proces uchovávania platnosti podpisov bez ďalšej interakcie používateľa.

Autorizovaný obslužný personál služby následne monitoruje a rieši akékoľvek problémy so službou.

7.7.4 Postupy uchovávania AdES podpisov a pečatí

Archivačná služba využíva pre uchovávanie kvalifikovaných podpisov a pečatí Poskytovateľa, certifikovaný TWS softvérový produkt Disig eArchive, ktorý využíva pre rozširovanie podpisových štruktúr overený komponent, certifikovaný NBÚ SR - Disig QES Signer 4 [4].

Tento produkt implementuje štandardy podpisových štruktúr:

- CAdES ETSI TS 103173 v.2.2.1 [5],
- PAdES ETSI TS 103172 v.2.2.2 [6],
- XAdES ETSI TS 103171 v.2.1.1 [7],
- kontajnera ASiC ETSI TS 103174 v.2.2.1 [8].

S podpisovými štruktúrami dokáže zrealizovať komplexné operácie validácie a pridávania časových pečiatok a rozširovať ich z jednoduchej formy B/BES/EPES až po ich LTA formy. Disig eArchive postupne rozširuje podpisové štruktúry, popísané v kapitole 4.7.2 dokumentu ETSI SR 019 510 v1.1.1 [3], obsiahnuté vo vstupných kontajneroch, technikou postupného rozširovania podpisov, popísanou v kapitole 5.3 dokumentu ETSI SR 019 510 v1.1.1 [3].

7.7.5 Obmedzenia služby

7.7.5.1 Podporované formáty súborov

Archivačná služba akceptuje nasledovné typy vstupných súborov:

- PDF – dokument podľa špecifikácie PDF ISO-32000 [9], ktorý je zároveň aj kontajnerom,
- ASICS – ASiC kontajner podľa ETSI TS 103174 [8],
- ASICE – ASiC kontajner podľa ETSI TS 103174 [8],
- SCS – ASiC kontajner podľa ETSI TS 103174 [8],
- SCE – ASiC kontajner podľa ETSI TS 103174 [8],
- ZIP – ASiC kontajner podľa ETSI TS 103174 [8],
- p7m – CMS kontajner obsahujúci dokument a CAdES podpis podľa ETSI TS 103 173,
- p7s – CMS kontajner obsahujúci iba CAdES podpis podľa ETSI TS 103 173, pričom podpísaný dokument je mimo CMS kontajnera,

- XML - XML kontajner obsahujúci dáta a XAdES podpis podľa ETSI TS 103 171
- ZEPf – ZIP formát súboru pre ZEP podľa dokumentu NBÚ SR s názvom "Formáty zaručených elektronických podpisov",
- xZEP/ZEPx – XML kontajner s elektronickým podpisom XAdES_ZEP na báze XAdES,
-

Služba predpokladá, že sa jedná o kontajnery podľa ich špecifikácií.

7.7.5.2 Maximálna veľkosť dokumentu

Maximálna veľkosť akceptovaného súboru pre zaradenie do archivačnej služby je 50MB.

7.7.5.3 Vnorené kontajnery

Archivačná služba nepodporuje uchovávanie vnorených kontajnerov, t. j. kontajnerov, ktoré obsahujú ďalšie kontajnery. Na vnorené kontajnery je nahliadané ako na binárne súbory a ich vnútorné podpisy/pečate nebudú uchovávané v zmysle predlžovania ich platnosti.

7.7.6 Dôveryhodný zdroj času

Poskytovateľ zabezpečí, že systémy archivačnej služby budú pripojené na dôveryhodný zdroj času s odchýlkou času nie väčšou ako 1000 milisekúnd.

7.8 Fyzická a objektová bezpečnosť

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

- Na správu archivačnej služby musia byť aplikované nasledovné dodatočné opatrenia:
  - Technické prostriedky služby musia byť prevádzkované v prostredí, ktoré fyzicky a logicky chráni služby pred kompromitáciou, ktorá môže byť spôsobená neautorizovaným prístupom k systémom alebo údajom.
  - Každý vstup do fyzicky bezpečnej oblasti musí podliehať nezávislému dohľadu a neautorizovaná osoba musí byť sprevádzaná autorizovanou osobou pokiaľ je v bezpečnej oblasti. Každý vstup a prítomnosť musí byť zaznamenaná.
  - Fyzická ochrana musí byť dosiahnutá vytvorením jasne definovanej bezpečnostnej hranice (perimetrom, fyzickou bariérou) okolo správy technických prostriedkov služby. Akékoľvek časti objektu zdieľané s inými organizáciami musia byť mimo tohto perimetra.
  - Fyzické a objektové bezpečnostné opatrenia musia chrániť objekty, kde sú umiestnené systémy, samotné systémové zdroje a objekty použité na podporu ich prevádzky. Bezpečnostné opatrenia týkajúce sa fyzickej a objektovej bezpečnosti Poskytovateľa musia pokrývať minimálne fyzické riadenie prístupu, ochranu pred prírodnými katastrofami, ochranu pred požiarom, výpadok podporných rozvodov

(napr. elektrina, telekomunikácie), zrútenie štruktúry, úniky z potrubí, ochranu proti odcudzeniu, vlámaniu, a obnovu po pohrome.

- Prijaté opatrenia musia chrániť zariadenia, informácie, médiá a softvér týkajúcich sa archivačných služieb pred vynesením bez autorizácie.

7.9 Prevádzková bezpečnosť

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

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

7.10 Sieťová bezpečnosť

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

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

7.11 Riadenie bezpečnostných incidentov

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

7.12 Zber dôkazov

Pre zber dôkazov platia ustanovenia, uvedené v dokumente [2], odstavec 5.10.

7.13 Riadenie kontinuity činnosti organizácie

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

- V prípade kompromitácie alebo podozrenia z kompromitácie pri prevádzkovaní archivačnej služby, musí Poskytovateľ sprístupniť všetkým odberateľom a spoliehajúcim sa stranám popis kompromitácie, ktorá nastala.
- V prípade významnej kompromitácie prevádzky Poskytovateľa, musí Poskytovateľ sprístupniť všetkým odberateľom a spoliehajúcim sa stranám informáciu, ktorá môže byť použitá na identifikáciu súborov z ich osobného priestoru, ktoré mohli byť ovplyvnené, pokiaľ tým neporuší súkromie používateľov Poskytovateľa alebo bezpečnosť služieb Poskytovateľa.

7.14 Ukončenie činnosti Poskytovateľa a plány ukončenia činnosti

Pre ukončenie činnosti Poskytovateľa platia ustanovenia, uvedené v dokumente [2], odstavec 5.12.

7.15 Zhoda

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

8 Plnenie požiadaviek pre kvalifikovanú archivačnú službu podľa Nariadenia eIDAS

8.1 Požiadavky

Keďže v čase publikácie tohto dokumentu ešte neboli publikované vykonávacie akty k požiadavkám Nariadenia eIDAS [1], platné požiadavky na poskytovanie kvalifikovanej dôveryhodnej služby uchovávania kvalifikovaných elektronických podpisov a kvalifikovaných elektronických pečatí sú definované v dokumente Schéma dohľadu, vydanom NBÚ SR [10].

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

- 5.1 - spoločné požiadavky na poskytovateľov kvalifikovaných dôveryhodných služieb,
- 5.4 - požiadavky na kvalifikovanú dôveryhodnú službu uchovávania kvalifikovaných elektronických podpisov a kvalifikovaných elektronických pečatí.

V kapitole 5.4 Schémy dohľadu sú okrem základných požiadaviek a odporúčaní Nariadenia eIDAS [1] pre archivačnú službu, slúžiacich k dosiahnutiu porovnateľnej úrovne bezpečnosti pri poskytovaní kvalifikovaných dôveryhodných služieb v celej Únii, uvedené a doplnené aj technické požiadavky pre jednotlivé body, záväzné pre Poskytovateľov kvalifikovaných dôveryhodných služieb pri prevádzke archivačnej služby na území SR.

8.2 Plnenie požiadaviek

8.2.1 Plnenie požiadaviek z kapitoly 5.1 Schémy dohľadu

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

8.2.2 Plnenie požiadaviek z kapitoly 5.4 Schémy dohľadu

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

Archivačná služba, jej fungovanie a spôsob tvorby a udržiavania dôkazu o evidencii, sú popísané v bode 7.7.1 tohto dokumentu. Z požiadaviek, uvedených v kapitole 5.4 Schémy dohľadu, vyplývajú procesy a postupy, ktoré sú ekvivalentné s procesmi a postupmi, implementovanými v softvérových produktoch Disig eArchive a Disig QES Signer 4 (viď bod 7.7.4 tohto dokumentu), zabezpečujúcich prevádzku systému archivačnej služby.

8.3 Služba časovej pečiatky

Kvalifikovaná elektronická časová pečiatka, využívaná v archivačnej službe, je poskytovaná vlastnou TSA službou Poskytovateľa.