Č. p.:

DKDS2 Certifikačná politika pre kvalifikovanú dôveryhodnú službu vyhotovovania a overovania kvalifikovaných certifikátov pre elektronický podpis, ktorej kvalifikovaný štatút udelil NBÚ

Názov dokumentu:	DKDS2 Certifikačná politika pre kvalifikovanú dôveryhodnú službu vyhotovovania a overovania kvalifikovaných certifikátov pre elektronický podpis, ktorej kvalifikovaný štatút udelil NBÚ		
Označenie dokumentu:	DKDS2 Certifikačná politika vyhotovovania a overovania kvalifikovaných certifikátov SNCA.docx		
Verzia:	0.9	Status:	*Návrh*
Dátum vytvorenia:	18.11.2020	Platný do:	31.12.2021

História dokumentu

História revízií dokumentu

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

Schválenia

Verzia	Funkcia	V zastúpení	Schválil dňa	Podpis

Distribúcia

Verzia	Spoločnosť	Meno	Počet výtlačkov

Referencie na legislatívne a normatívne dokumenty

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

[2] Recommendation ITU-T X.509 | ISO/IEC 9594-8 Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks.
ITU-T X.509 | ISO/IEC 9594-8

[3] 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

[4] 05968/2019/ORD-001 - Schéma dohľadu kvalifikovaných dôveryhodných služieb definovaná orgánom dohľadu, Verzia 1.4, NBÚ SR.
Schéma dohľadu KDS definovaná orgánom dohľadu

[5] 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 319 411-2 V2.1.1 (2016-02)

[6] 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.
ETSI EN 319 411-1 V1.1.1 (2016-02)

[7] ETSI EN 319 403 - Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers.
ETSI EN 319 403 V2.2.2 (2015-08)

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

[9] Zákon č. 122/2013 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov (do 24.5.2018).
Zákon č. 122/2013 Z. z. o ochrane osobných údajov – účinný do 24.05.2018

[10] Zákon č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov (od 25.5.2018).
Zákon č. 18/2018 Z. z. o ochrane osobných údajov – účinný od 25.05.2018

[11] RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.
RFC 5280

[12] Pravidlá na výkon certifikačných činností (CPS) SNCA.
DKDS9 Pravidlá na výkon certifikačných činností (CPS) SNCA

Zoznam tabuliek

Použité definície a skratky

Tabuľka 1 Použité definície

Definícia	Vysvetlenie definície
Certifikát	Elektronický dokument, ktorým vydavateľ certifikátu (certifikačná autorita) potvrdzuje, že v certifikáte uvedený verejný kľúč patrí Držiteľovi, ktorému je certifikát vydaný.
Dôveryhodná služba	Elektronická služba, ktorá sa spravidla poskytuje za odplatu a spočíva: a) vo vyhotovovaní, overovaní a validácii: ■ elektronických podpisov, elektronických pečatí alebo elektronických časových pečiatok, elektronických doručovacích služieb pre registrované zásielky a certifikátov, ktoré s týmito službami súvisia, ■ certifikátov pre autentifikáciu webových sídiel, b) v uchovávaní elektronických podpisov, elektronic. pečatí alebo certifikátov, ktoré s týmito službami súvisia.
Držiteľ	Entita, identifikovaná v certifikáte ako Držiteľ súkromného kľúča, prislúchajúceho k verejnému kľúču, obsiahnutému v certifikáte.
Elektronický podpis	Údaje v elektronickej forme, ktoré sú pripojené alebo logicky pridružené k iným údajom v elektronickej forme a ktoré podpisovateľ používa na podpisovanie.
Elektronická pečať	Údaje v elektronickej forme, ktoré sú pripojené alebo logicky pridružené k iným údajom v elektronickej forme s cieľom zabezpečiť pôvod a integritu týchto pridružených údajov.
Hashovacia funkcia (hash, message digest, fingerprint)	Rýchlo spočítateľná funkcia, ktorá dostane na vstupe dokument ľubovoľnej dĺžky a zostrojí z neho pomerne krátku (napr. 256 bitov) charakteristiku, nazývanú hashovacia hodnota (tiež hašovacia hodnota, hash). V súčasnosti patria v kryptografii medzi najpoužívanejšie hašovacie funkcie SHA1 a SHA2 (SHA224, SHA256, SHA384; SHA512).
Kľúčový pár	Predstavuje súčasť PKI systému, ktorá využíva asymetrickú kryptografiu. Kľúčový pár pozostáva z verejného a k nemu prislúchajúceho súkromného kľúča.

Kvalifikovaná dôveryhodná služba	Dôveryhodná služba, ktorá spĺňa uplatniteľné požiadavky, stanovené v nariadení eIDAS.
Kvalifikovaná elektronická pečať	Zdokonalená elektronická pečať, vyhotovená pomocou kvalifikovaného zariadenia na vyhotovenie elektronickej pečate a založená na kvalifikovanom certifikáte pre elektronickú pečať.
Kvalifikované zariadenie na vyhotovenie elektronického podpisu	Zariadenie na vyhotovenie elektronického podpisu, ktoré spĺňa požiadavky stanovené v prílohe II nariadenia eIDAS.
Kvalifikované zariadenie na vyhotovenie elektronickej pečate	Zariadenie na vyhotovenie elektronickej pečate, ktoré primerane spĺňa požiadavky stanovené v prílohe II nariadenia eIDAS.
Kvalifikované zariadenie	Spoločné označenie pre kvalifikované zariadenie na vyhotovovanie elektronického podpisu a kvalifikované zariadenie na vyhotovovanie elektronickej pečate.
Kvalifikovaný certifikát pre autentifikáciu webového sídla	Certifikát v zmysle čl. 3, bod 39 nariadenia eIDAS, ktorý vyhotovuje kvalifikovaný poskytovateľ dôveryhodných služieb a ktorý spĺňa požiadavky stanovené v prílohe IV nariadenia eIDAS.
Kvalifikovaný certifikát pre elektronickú pečať	Certifikát v zmysle čl. 3, bod 30 nariadenia eIDAS, ktorý vyhotovuje kvalifikovaný poskytovateľ dôveryhodných služieb a ktorý spĺňa požiadavky stanovené v prílohe III nariadenia eIDAS.
Kvalifikovaný certifikát pre elektronický podpis	Certifikát v zmysle čl. 3, bod 15 nariadenia eIDAS, ktorý vyhotovuje kvalifikovaný poskytovateľ dôveryhodných služieb a ktorý spĺňa požiadavky stanovené v prílohe I nariadenia eIDAS.
Kvalifikovaný elektronický podpis	Zdokonalený elektronický podpis, vyhotovený s použitím kvalifikovaného zariadenia na vyhotovenie elektronického podpisu a založený na kvalifikovanom certifikáte pre elektronické podpisy.
Kvalifikovaný poskytovateľ dôveryhodných služieb	Poskytovateľ dôveryhodných služieb, ktorý poskytuje jednu alebo viacero kvalifikovaných dôveryhodných služieb a ktorému orgán dohľadu udelil kvalifikovaný štatút.
Mandátny certifikát	Certifikát v zmysle §8 zákona č. 272/2016 Z. z..
Odberateľ	Fyzická osoba, resp. právnická osoba, ktorá je oprávnená žiadať o KC v mene entity, ktorej meno sa objaví ako subjekt v atribúte KC – Držiteľ certifikátu.

Poskytovateľ	Národná agentúra pre sieťové a elektronické služby.
Pracovník Poskytovateľa	Zamestnanec NASES.
Pracovník RA	Zamestnanec NASES, registračný operátor, vykonávajúci vybrané činnosti pri poskytovaní dôveryhodných služieb.
Prevádzkovateľ	Organizačný útvar, ktorý na základe rozhodnutia Poskytovateľa prevádzkuje IS KDS.
Pravidlá na výkon certifikačných činností	Postupy, ktoré SNCA používa pri vyhotovovaní certifikátov.
RFC	Postup vytvárania štandardu na Internete a zároveň označenie takto vzniknutého štandardu.
Spoliehajúca sa strana	Fyzická osoba alebo právnická osoba, ktorá sa pri svojom konaní spolieha na dôveryhodné služby SNCA.
Zákon o OOÚ	Zákon č. 122/2013 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov (do 24.5.2018). Zákon č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov (od 25.5.2018).
Zdokonalený elektronický podpis	Elektronický podpis, spĺňajúci požiadavky, stanovené v článku 26 nariadenia eIDAS.
X.509	Medzinárodný štandard, ktorý okrem iného definuje aj formát certifikátu verejného kľúča.

Tabuľka 2 Použité skratky

Skratka	Vysvetlenie skratky
CA	Certifikačná autorita (Certification Authority).
CP	Certifikačná politika (Certification Policy).
CPS	Pravidlá na výkon certifikačných činnosti (Certificate Practice Statement).
CRL	Zoznam zrušených certifikátov (Certificate Revocation List).
HSM	Kvalifikované zariadenie na vyhotovenie elektronického podpisu alebo vyhotovenie elektronickej pečate; kryptografický modul, hardvérový bezpečnostný modul (Hardware Security Modul).
HW	Hardvér (Hardware).
KC	Kvalifikovaný certifikát.
NASES	Národná agentúra pre sieťové a elektronické služby.
NBÚ	Národný bezpečnostný úrad.

OCSP	Protokol, určený spoliehajúcim sa stranám na potvrdenie existencie a platnosti certifikátu (OCSP - Online Certificate Status Protocol)
OVM	Orgán verejnej moci.
PKCS	Séria štandardov určená pre kryptografiu verejných kľúčov (Public Key Cryptography Standard).
PKI	Infraštruktúra verejných kľúčov (Public Key Infrastructure).
PMA	Autorita pre riadenie politík (Policy Management Authority).
QSCD	Kvalifikované zariadenie, určené na generovanie a uloženie páru kľúčov (súkromný, verejný) a na vyhotovovanie elektronického podpisu/ pečate (Qualified electronic Signature/Seal Creation Device).
RA	Registračná autorita (Registration Authority).
RFC	Žiadosť o vyjadrenie (Request For Comment).
URL	Internetový ekvivalent pre web adresu (Uniform Resource Locator).

Obsah

1 Úvod

Dokument „Certifikačná politika pre kvalifikovanú dôveryhodnú službu vyhotovovania a overovania kvalifikovaných certifikátov pre elektronický podpis, ktorej kvalifikovaný štatút udelil NBÚ“ (ďalej aj „CP“):

- definuje politiku poskytovania kvalifikovanej dôveryhodnej služby a bezpečnostné požiadavky, ktoré sa týkajú postupov riadenia a prevádzkovej praxe pri poskytovaní tejto služby,
- upravuje metodiku, záväzné postupy a povinnosti pri správe kvalifikovaných certifikátov verejných kľúčov (ďalej aj „KC“), vyhotovovaných certifikačnou autoritou SNCA.

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

Certifikačná politika predstavuje štandard pre definovanie zásad, procedúr a postupov, ktoré sú záväzné pre všetky zúčastnené strany v procese vyhotovovania kvalifikovaných certifikátov. Dodržiavanie týchto procedúr a postupov, zjednodušuje identifikáciu vydaných certifikátov v súlade s platnými právnymi predpismi SR.

Táto certifikačná politika nadväzuje na certifikačnú politiku pre koreňovú CA NBÚ, definovanú v dokumente „Certifikačná politika pre koreňovú CA a dôveryhodnú službu vyhotovovania kvalifikovaných certifikátov, ktorej kvalifikovaný štatút udelil Národný bezpečnostný úrad, verzia 4.0, č.: 5767/2016/IBEP/OA-008“, OID dokumentu: 1.3.158.36061701.0.0.0.1.2.2.

Pokiaľ sú v tejto certifikačnej politike definované povinnosti SNCA, ich právnym nositeľom je Prevádzkovateľ SNCA.

1.1 Prehľad

Táto certifikačná politika sa týka poskytovania kvalifikovaných dôveryhodných služieb vyhotovovania a overovania kvalifikovaných certifikátov v zmysle ustanovení Nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES (ďalej len „nariadenie eIDAS“).

Certifikačná politika je spracovaná v štruktúre, ktorá je odporúčaná v dokumentácii RFC 3647 „Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework“.

Pokiaľ sa v dokumente použije skratka „KC“ myslia sa tým všetky typy kvalifikovaných certifikátov, vyhotovované v zmysle tejto CP, ktoré sú uvedené v bode 1.3.1.

Ak sa niektoré ustanovenie týka len určitého typu kvalifikovaného certifikátu, táto skutočnosť je v texte zreteľne definovaná.

1.2 Názov dokumentu a jeho identifikácia

Politika poskytovania kvalifikovanej dôveryhodnej služby vyhotovovania a overovania kvalifikovaných certifikátov pre elektronický podpis, ktorej kvalifikovaný štatút udelil NBÚ, je identifikovaná nasledovným identifikátorom, odvodeným od objektového identifikátora NASES:

1.3.158.42156424.0.1.2

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
2	Certifikačná politika pre kvalifikované certifikáty (pre elektronický podpis, elektronickú pečať).

1.3 Účastníci PKI

V rámci poskytovania dôveryhodnej služby vyhotovovania a overovania KC, sú účastníkmi infraštruktúry verejného kľúča prevádzkovateľa entity, uvedené v tejto časti.

1.3.1 Certifikačné autority

Certifikačnou autoritou, sa v rámci tejto certifikačnej politiky rozumie SNCA, zriadená a prevádzkovaná podľa ustanovení nariadenia eIDAS a zákona č. 272/2016 Z. z. o dôveryhodných službách.

SNCA môže v mimoriadnych prípadoch, ak by prišlo k ohrozeniu bezpečnostných záujmov Slovenskej republiky (ďalej aj „SR“), vydať nový certifikát klientom zaniknutého kvalifikovaného poskytovateľa dôveryhodných služieb.

SNCA poskytuje kvalifikované dôveryhodné služby fyzickým osobám, právnickým osobám a orgánom verejnej moci (ďalej len „OVM“) na základe a v súlade so „Zmluvou o poskytovaní

kvalifikovaných dôveryhodných služieb“, ktorú je povinný uzatvoriť prevádzkovateľ SNCA s príslušnou fyzickou osobou, právnickou osobou alebo príslušnou organizačnou zložkou OVM.

Certifikačná autorita SNCA, poskytuje kvalifikovanú dôveryhodnú službu vyhotovovania nasledovných typov kvalifikovaných certifikátov:

- kvalifikovaný certifikát pre elektronický podpis (článok 3, bod 15 nariadenia eIDAS),
- kvalifikovaný certifikát pre elektronickú pečať (článok 3, bod 30 nariadenia eIDAS),
- kvalifikovaný certifikát pre autentifikáciu webového sídla (článok 3, bod 39 nariadenia eIDAS),
- mandátny certifikát (§8 zákona č. 272/2016 Z. z.).

1.3.2 Registračná autorita

Registračná autorita je entita, vykonávajúca činnosti, spojené s poskytovaním kvalifikovaných dôveryhodných služieb, v mene Poskytovateľa. RA musí vykonávať svoje aktivity v súlade so schválenou CP a „Pravidlami na výkon certifikačných činností“ (ďalej aj „CPS“) v aktuálnom znení. Tieto činnosti môže poskytovať interná, externá, prípadne mobilná registračná autorita (ďalej aj „RA SNCA“).

RA SNCA slúži na registráciu a overovanie žiadostí o vydanie kvalifikovaných certifikátov. RA SNCA zároveň zabezpečuje príjem žiadostí a podnetov o zrušenie kvalifikovaných certifikátov.

1.3.3 Odberateľ a Držiteľ kvalifikovaného certifikátu

Odberateľom KC, vydávaných SNCA, sú fyzické alebo právnické osoby, ktoré sú oprávnené požiadať o vydanie kvalifikovaného certifikátu v mene entity, ktorej meno bude uvedené v subjekte vyhotoveného kvalifikovaného certifikátu, v atribúte Držiteľ.

Držiteľom KC môže byť:

- fyzická osoba,
- fyzická osoba, identifikovaná v spojení s právnickou osobou,
- právnická osoba, ktorou môže byť organizácia alebo jej organizačná jednotka,
- fyzická osoba identifikovaná v spojení s orgánmi verejnej moci,
- orgán verejnej moci.

Táto CP definuje podmienky, ktoré musí splniť Odberateľ.

V prípade, že Odberateľom je fyzická osoba a ako subjekt sú uvedené len jej meno a priezvisko, tak Odberateľ a Držiteľ KC je tá istá fyzická osoba t. j. daná fyzická osoba je priamo zodpovedná v prípade neplnenia si povinností, kladených na Odberateľa a aj Držiteľa.

Formálnym Držiteľom KC sa rozumie fyzická osoba, ktorá sa zaviaže, že bude používať zodpovedajúci súkromný kľúč a KC v súlade s touto certifikačnou politikou.

1.3.4 Spoliehajúca sa strana

Spoliehajúcou sa stranou je fyzická alebo právnická osoba, ktorá sa pri svojom konaní spolieha na elektronickú identifikáciu alebo dôveryhodné služby Poskytovateľa.

1.3.5 Iní účastníci

1.3.5.1 Policy Management Authority

Autorita pre riadenie politík (ďalej len „PMA“), ktorá predstavuje zložku Poskytovateľa, ustanovenú 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 CPS,
- 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.

1.3.5.2 Poskytovatelia iných služieb

Medzi poskytovateľov iných služieb patria:

- autorita, poskytujúca služby vyhotovovania kvalifikovaných elektronických časových pečiatok,
- entita v podobe OCSP respondera, ktorá poskytuje služby súvisiace so štatútom platnosti KC.

1.4 Použiteľnosť KC

1.4.1 Korektné použitie certifikátu

Kvalifikované certifikáty, vyhotovené v zmysle tejto certifikačnej politiky, môžu byť použité len na identifikáciu držiteľa verejného kľúča pri overovaní:

- zdokonaleného elektronického podpisu fyzickej osoby, ktorý spĺňa požiadavky uvedené v článkoch 26 a 27 nariadenia eIDAS,
- zdokonalenej elektronickej pečate orgánu verejnej moci, ktorá spĺňa požiadavky uvedené v článkoch 36 a 37 nariadenia eIDAS,

- kvalifikovaného elektronického podpisu fyzickej osoby, ktorý spĺňa požiadavky uvedené v článku 3 bod 12 nariadenia eIDAS,
- kvalifikovanej elektronickej pečate orgánu verejnej moci, ktorá spĺňa požiadavky uvedené v článku 3 bod 27 nariadenia eIDAS,
- kvalifikovaného certifikátu pre autentifikácie webového sídla, ktorý spĺňa požiadavky uvedené v článku 3 bod 39 nariadenia eIDAS.

1.4.2 Nepovolené použitie certifikátu

Akékoľvek iné použitie KC, odlišné od spôsobov použitia uvedených v bode 1.4.1 tejto certifikačnej politiky, sa považuje za nepovolené (neoprávnené) použitie certifikátu.

1.5 Správa politiky

1.5.1 Organizácia zodpovedná za správu dokumentu

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

Kontaktná adresa:

Národná agentúra pre sieťové a elektronické služby

Detašované pracovisko:

BC Omnipolis,

Trnavská cesta 100/II,

821 01 Bratislava,

Slovenská republika,

http://www.nases.gov.sk

1.5.2 Kontaktná osoba

Kontaktnou osobou je pracovník NASES, menovaný do roly PMA SNCA.

Otázky, pripomienky a návrhy k tejto certifikačnej politike je možné zaslať na adresu:

Národná agentúra pre sieťové a elektronické služby

Detašované pracovisko:

BC Omnipolis,

Trnavská cesta 100/II,

821 01 Bratislava,

Slovenská republika,

Telefón: +421 2 3278 0700

e-mail: info@nases.gov.sk

1.5.3 Osoba rozhodujúca o súlade CPS s certifikačnou politikou

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

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

1.5.4 Postupy schvaľovania CP

Je nevyhnutné, aby pred uvedením do prevádzky, mal Poskytovateľ schválenú požadovanú dokumentáciu, svoju certifikačnú politiku dôveryhodnej služby vyhotovovania kvalifikovaných certifikátov a CPS a zároveň, aby spĺňal a dodržiaval všetky požiadavky, definované v týchto dokumentoch.

Obsah certifikačnej politiky dôveryhodnej služby vyhotovovania kvalifikovaných certifikátov a CPS schvaľuje riaditeľ sekcie Slovenskej národnej certifikačnej autority NASES.

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

2 Zverejňovanie informácií a úložiská

2.1 Úložiská

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

Úložiská sú prístupné Odberateľom a Spoliehajúcim sa stranám. Prevádzka úložísk je zabezpečená v súlade s celkovými bezpečnostnými požiadavkami platnej legislatívy SR a EÚ.

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

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

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

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

2.2 Zverejňovanie informácií o CA

SNCA zverejňuje alebo na požiadanie poskytuje informácie, súvisiace s poskytovaním dôveryhodných služieb (ďalej len „certifikačné informácie“) na týchto adresách:

- detašované pracovisko prevádzkovateľa SNCA:

  Národná agentúra pre sieťové a elektronické služby
  BC Omnipolis
  Trnavská cesta 100/II
  821 01 Bratislava
  Slovenská republika

- sídla registračných autorít SNCA / registračné miesta:
  - interná registračná autorita SNCA:

    Národná agentúra pre sieťové a elektronické služby
    BC Omnipolis,
    Trnavská cesta 100/II,
    821 01 Bratislava
    Slovenská republika
  - externá OVM registračná autorita SNCA:

    Národný bezpečnostný úrad
    Budatínska 30

851 06 Bratislava
Slovenská republika

- dedikované internetové stránky SNCA a webové sídlo agentúry NASES:

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

  https://www.nases.gov.sk/doveryhodne-sluzby/index.html

SNCA zverejňuje certifikačné informácie, určené na zverejnenie, v zmysle nariadenia eIDAS a zákona o dôveryhodných službách, minimálne v tomto rozsahu:

- certifikačná politika pre kvalifikovanú dôveryhodnú službu vyhotovovania a overovania kvalifikovaných certifikátov pre elektronický podpis, ktorej kvalifikovaný štatút udelil NBÚ,
- informácie o KC vydaných SNCA,
- archív zoznamov CRL vydaných SNCA,
- certifikát vydávajúcej SNCA.

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

2.3 Frekvencia zverejňovania informácií

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

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

Informácie o KC vydaných SNCA sa zverejňujú neodkladne po vydaní nového certifikátu.

Informácie o zrušených certifikátoch sa zverejňujú zvyčajne každé štyri hodiny, najmenej však raz za 24 hodín.

Informácie o certifikáte vydávajúcej SNCA sa zverejňujú neodkladne po každej zmene.

2.4 Kontroly prístupu

Certifikačné informácie podľa bodu 2.3 tejto certifikačnej politiky, zverejňuje prevádzkovateľ SNCA bez obmedzenia.

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

3 Identifikácia a autentifikácia

3.1 Mená

3.1.1 Typy mien

SNCA vydáva certifikáty, ktoré obsahujú rozlišovacie mená (ďalej len „DN“) vydavateľa (issuer) a držiteľa (subject) zadefinované v nasledujúcich dokumentoch:

ITU-T X.500 Information technology – Open Systems Interconnection – The Directory: Overview of concepts, models and services,

ITU-T X.501 – Information technology – Open Systems Interconnection – The Directory: Models,

ITU-T X.520 – Information technology – Open Systems Interconnection – The Directory: Selected attribute types.

3.1.2 Potreba zmysluplnosti mien

Prevádzkovateľ SNCA zodpovedá za zmysluplnosť mien v certifikátoch, vydávaných SNCA. Identifikačné údaje, uvedené v certifikáte, musia zmysluplne identifikovať vydavateľa certifikátu (SNCA) a držiteľa certifikátu.

3.1.3 Anonymita a používanie pseudonymov

SNCA uvádza pseudonymy, len v kvalifikovaných certifikátoch pre elektronické pečate, vydávaných pre správcov elektronických podateľní. Vyhotovenie KC pre anonymného držiteľa nie je podporované a povolené.

3.1.4 Pravidlá na interpretáciu rôznych foriem mien

Prevádzkovateľ SNCA, po prijatí žiadosti o vydanie certifikátu, skontroluje žiadosť v písomnej aj v elektronickej forme, podľa nasledujúcich pravidiel:

- skontrolovanie syntaxe mien,
- skontrolovanie vecnej správnosti mien (sémantika),
- skontrolovanie prítomnosti všetkých povinných položiek.

Pri interpretácii mien platí, že ak sú vyššie uvedené kontroly ukončené s kladným výsledkom, prevezmú sa zo žiadosti o vydanie certifikátu.

Interpretácia jednotlivých foriem mien v KC, vyhotovovaných SNCA, musí byť v súlade s profilmi KC, ktoré sú popísané v kapitole č. 7 tohoto dokumentu.

3.1.5 Jednoznačnosť mien

Prevádzkovateľ SNCA zodpovedá za jednoznačnosť mien v certifikátoch, vydávaných SNCA. Identifikačné údaje, uvedené v certifikáte, jednoznačne identifikujú vydavateľa certifikátu (SNCA) a držiteľa certifikátu.

Identifikačné údaje držiteľa kvalifikovaného certifikátu pre elektronický podpis typu mandátny certifikát, jednoznačne identifikujú fyzickú osobu v spojení s OVM, ktorej bol mandátny certifikát vydaný. Za týmto účelom sa do kvalifikovaného certifikátu pre elektronický podpis – mandátneho certifikátu, môže uviesť číslo pasu, číslo osobnej identifikačnej karty (OIK), osobné evidenčné číslo (OEČ) alebo číslo služobného preukazu a ako osobitný atribút, rodné číslo podpisovateľa, v súlade so znením §8 ods. 1, písm. a) zákona o dôveryhodných službách.

Identifikačné údaje držiteľa kvalifikovaného certifikátu pre elektronickú pečať, jednoznačne identifikujú právnickú osobu alebo orgán verejnej moci, ktorým bol kvalifikovaný certifikát pre elektronickú pečať vydaný. Za týmto účelom sa do kvalifikovaného certifikátu pre elektronickú pečať uvádza identifikačné číslo držiteľa.

3.1.6 Rozpoznanie, autentizácia a význam obchodných značiek

Ochranné známky nie sú v rámci poskytovania dôveryhodných služieb zo strany SNCA využívané. Poskytovateľ negarantuje žiadnej entite, že jej meno v KC bude obsahovať jej obchodnú značku (trademark) a to ani na jej výslovnú žiadosť.

3.2 Počiatočné overenie identity

V tejto časti dokumentu sú popísané postupy, ktoré je potrebné dodržiavať v procese identifikácie a autentifikácie jednotlivých subjektov, ktorým je poskytovaná dôveryhodná služba.

V prípade vyhlásenia mimoriadnej situácie, v zmysle zákona č. 42/1994 Z. z. o civilnej ochrane obyvateľstva, s pôsobnosťou na území Slovenskej republiky, môže osoba, menovaná do roly PMA SNCA, rozhodnúť o modifikácii spôsobu vydávania kvalifikovaných certifikátov uložených v QSCD a s tým spojeným generovaním kryptografických kľúčov a overovaním identity jednotlivých subjektov, ktorý sa bude odlišovať od tu uvedených postupov. Modifikovaný postup musí byť spracovaný v písomnej podobe a musí byť schválený osobu, menovanou do roly PMA SNCA. Modifikovaný postup je možné použiť len počas trvania mimoriadnej situácie. Po ukončení mimoriadnej situácie, je potrebné postupovať v zmysle tu uvedených postupov.

3.2.1 Preukazovanie vlastníctva súkromného kľúča

Kľúčový pár, na ktorý sa vyhotovuje KC pre elektronický podpis, určený na vyhotovovanie kvalifikovaného elektronického podpisu resp. KC pre elektronickú pečať, určený na vyhotovovanie kvalifikovanej elektronickej pečate, musí byť generovaný priamo

v kvalifikovanom zariadení na vyhotovenie elektronického podpisu, ktoré spĺňa požiadavky stanovené v prílohe II Nariadenia eIDAS (ďalej len „QSCD“).

Všetky žiadosti o vydanie KC, kde kľúčový pár nie je uložený v QSCD, musia byť vo formáte PKCS#10, čo znamená, že žiadosť o vydanie KC bude podpísaná s využitím súkromného kľúča, patriaceho k verejnému kľúču, nachádzajúcemu sa v danej žiadosti. Overením väzby medzi verejným kľúčom v žiadosti a súkromným kľúčom, využitým na jej podpísanie, sa preukazuje, že v čase podpisovania žiadosti Odberateľ vlastnil zodpovedajúci súkromný kľúč. Pokiaľ je KC vydávaný na kvalifikované zariadenie pre elektronický podpis/pečať, potom je vlastníctvo kľúča Držiteľa preukázané tým, že kryptografický pár kľúčov je generovaný priamo v kvalifikovanom zariadení pracovníkom NASES za súčasnej prítomnosti Odberateľa.

3.2.2 Autentizácia identity právnickej osoby

Právnická osoba so sídlom v Slovenskej republike, musí preukázať svoju totožnosť výpisom z obchodného registra, príp. iného platného registra právnických osôb. Zo strany Poskytovateľa dôveryhodných služieb, musí byť vyžadovaný originál alebo úradne overená kópia originálu, nie staršie ako tri mesiace. Doklad musí obsahovať úplné obchodné meno alebo názov, identifikačný údaj (spravidla IČO), sídlo, meno/á osoby/osôb konajúcej/ich za právnickú osobu a spôsob konania a podpisovania za danú právnickú osobu.

V prípade, že právnická osoba nemá sídlo na území Slovenskej republiky, jej totožnosť sa musí overiť rovnakým spôsobom, ako je uvedené vyššie. Výpis z platného registra právnických osôb, musí byť úradne preložený do slovenského jazyka úradným prekladateľom – znalcom (okrem organizácií so sídlom v Českej republike).

V prípade, že právnická osoba nemôže preukázať svoju totožnosť výpisom z obchodného registra (platí pre nepodnikateľské subjekty ako sú napr. obec, cirkev, občianske združenie, nadácia, štátny orgán a podobne), musí takáto právnická osoba písomne preukázať okrem svojej totožnosti aj legálnosť, resp. „dôvod“ svojej existencie, s využitím a poukázaním na zákon alebo iný predpis, ktorý o subjekte daného typu pojednáva, zriaďovacou listinou a pod..

V prípade vydávania certifikátu, musí právnická osoba preukázať pravdivosť identifikačného údaja, uvedeného v žiadosti o certifikát, predložením k nahliadnutiu originálneho dokumentu, preukazujúceho túto skutočnosť.

Všetky doklady, predložené registračnému operátorovi RA SNCA klientami SNCA, musia byť originálom alebo úradne overenou kópiou originálu. Žiadny údaj v predložených dokladoch, nesmie byť doplňovaný, pozmeňovaný, prečiarknutý a podobne. Doklady, na ktorých je vyznačená doba ich platnosti, musia byť platné.

Pri poskytovaní dokladov sa vyžaduje, aby na registračné miesto RA SNCA boli poskytnuté originály týchto dokladov, slúžiace k nahliadnutiu a kópie originálov (nemusia byť overené), okrem osobných dokladov identifikujúcich totožnosť klienta SNCA, slúžiace na archiváciu pre potreby Poskytovateľa dôveryhodných služieb. Poskytnutie výpisu z obchodného registra, získaného z internetu zo strany klienta SNCA, nie je postačujúce, nakoľko tento výpis má len informatívny charakter a nie je použiteľný na právne úkony.

Existencia právnickej osoby a orgánu verejnej moci, je daná platnou legislatívou Slovenskej republiky, ktorá definuje právnické osoby a orgány verejnej moci, podľa úrovne pôsobnosti, napr. zákon č. 513/1991 Z. z. (Obchodný zákonník) v znení neskorších predpisov, obchodný register prípadne iný platný register právnických osôb, zákon č. 460/1992 Z. z. (Ústava Slovenskej republiky) v znení neskorších predpisov, zákon č. 575/2001 Z. z. o organizácii činnosti vlády a organizácii ústrednej štátnej správy v znení neskorších predpisov a o zmene a doplnení niektorých zákonov a pod..

Na žiadosť klienta SNCA alebo registračného operátora RA SNCA, budú prípadné sporné prípady pri preukazovaní totožnosti riešené postupom podľa časti 9.13.

3.2.3 Autentizácia identity fyzickej osoby

Poskytovateľ garantuje, že identita Držiteľa KC a jeho verejný kľúč sú zodpovedajúco previazané. Postupy na autentizáciu identity Držiteľa KC, špecifikuje Poskytovateľ vo vydaných CPS.

Dokumentácia o identifikácii musí obsahovať minimálne nasledovné údaje:

- identitu osoby, ktorá vykonáva identifikáciu,
- jednoznačné identifikačné údaje z dokladov, preukazujúcich identitu autentizovanej osoby,
- dátum vykonania identifikácie.

Overenie identity fyzickej osoby, pre ktorú má byť vydaný kvalifikovaný certifikát, sa vykoná na základe predloženia dvoch identifikačného dokladov, z ktorých kombináciou ich obsahu, budú k dispozícii minimálne tieto údaje:

- celé meno a priezvisko,
- rodné číslo (osoby, ktoré ho majú pridelené),
- dátum narodenia (osoby, ktoré nemajú pridelené rodné číslo),
- adresa trvalého bydliska,
- číslo predkladaného dokladu (platí pre obidva doklady).

Je vyžadované, že jeden z dvoch predkladaných identifikačných dokladov musí byť buď občiansky preukaz občana Slovenskej republiky, služobný preukaz alebo cestovný pas, vydaný Slovenskou republikou. Ďalšie údaje potrebné na overenie identity fyzickej osoby je možné získať z druhého dokladu, ktorý obsahuje potrebné údaje, napr. použiť vodičský preukaz, služobný preukaz, zbrojný preukaz, rodný list alebo preukaz poistenca verejného zdravotného poistenia.

Ak fyzická osoba zastupuje pri vydávaní KC inú fyzickú osobu, musí sa navyše preukázať úradne overenou plnou mocou, alebo inou úradne overenou listinou, z textu ktorej je jednoznačne jasné, že zastupujúca fyzická osoba bola splnomocnená splnomocňujúcou fyzickou osobou konať v danej veci v jej mene.

3.2.3.1 Preukazovanie oprávnenia alebo postavenia

Pokiaľ je vyhotovovaný mandátny certifikát, tak Odberateľ musí predložiť overiteľné doklady, preukazujúce oprávnenie v zmysle požiadaviek, uvedených v aktuálnej verzii zoznamu oprávnení v zmysle §9 ods. 2 písm. b) zákona č. 272/2016 Z. z..

Pokiaľ je vyhotovovaný mandátny certifikát (§8 zákona č. 272/2016 Z. z.) a týka sa konania za inú osobu alebo orgán verejnej moci, musí Odberateľ predložiť oprávnenie na konanie v mene zastupovanej osoby vo forme:

- dokladu preukazujúceho, že daná osoba je štatutárnym orgánom danej právnickej osoby alebo orgánu verejnej moci,
- poverenia, ak je daná fyzická osoba zamestnancom právnickej osoby, v mene ktorej koná a je s ňou v pracovnoprávnou vzťahu alebo obdobnom pracovnom vzťahu,
- notárom overenej plnej moci, ak daná fyzická osoba nie je s danou osobou v pracovnoprávnom vzťahu alebo obdobnom pracovnom vzťahu

Pokiaľ je vyhotovovaný mandátny certifikát (§8 zákona č. 272/2016 Z. z.) a týka sa vykonávania činnosti alebo vykonávania funkcie, musí Odberateľ hodnoverným spôsobom preukázať, že je orgánom verejnej moci, že vykonáva činnosť alebo funkciu podľa požiadaviek zákon č. 272/2016 Z. z. a v zmysle požiadaviek uvedených v zozname oprávnení, pre dané oprávnenie, ktoré je zverejnené na webovom sídle NBÚ.

Registračný operátor RA SNCA môže akceptovať, ako preukázanie oprávnenia, aj hromadný zoznam, podpísaný štatutárnym orgánom OVM, alebo inou oprávnenou osobou, ktorý bude obsahovať meno a priezvisko fyzickej osoby, ktorej má byť vydaný mandátny certifikát, číslo jej identifikačného dokladu a číslo oprávnenia v zmysle aktuálnej verzie zoznamu oprávnení, ktorý je zverejnený na webovom sídle NBÚ (§9, ods. 2, písm. a) zákona o dôveryhodných službách).

Poskytovateľ a jeho externé registračné autority majú právo, overiť si platnosť údajov z predloženého dokumentu pomocou iných verejne dostupných zdrojov napr. notárska komora, komora exekútorov, zoznam znalcov, tlmočníkov a prekladateľov a pod.

3.2.3.2 Autentizácia identity zariadenia alebo systému

Poskytovateľ garantuje, že identita webového sídla a jeho verejný kľúč, sú spoľahlivo previazané.

Z uvedeného dôvodu musí byť KC webového sídla priradený fyzickej osobe, konajúcej v mene právnickej osoby, ktorá má preukázateľnú kontrolu nad webovým sídlom, na ktoré je KC vyhotovený.

Daná fyzická osoba je povinná poskytnúť SNCA nasledovné údaje a informácie:

- identifikáciu zariadenia/systému v podobe presne stanoveného mena domény (Full Qualified Domain Name (FQDN)),
- žiadosť vo formáte PKCS#10, obsahujúcu verejné kľúče zariadenia/systému,

- kontaktné údaje pre prípadnú komunikáciu pracovníka RA SNCA s touto osobou.

Registračný operátor RA SNCA musí autentizovať správnosť ľubovoľnej autorizácie (hodnoty položky rozlišovacieho mena), ktorá má byť uvedená v KC a overí predložené údaje.

Spôsob vykonania autentizácie a kontroly údajov predstavujú nasledovné činnosti:

- overenie identity fyzickej osoby v súlade s požiadavkami bodu 3.2.3,
- overenie identity právnickej osoby, ktorej patrí daný komponent, v súlade s požiadavkami bodu 3.2.2,
- overenie oprávnenosti použitia údajov, ktoré majú byť uvedené v jednotlivých položkách kvalifikovaného certifikátu, s dôrazom na obsah položky commonName, kde najdôležitejšou položkou je presne stanovené meno domény (FQDN).

V prípade použitia FQDN je podmienkou, aby príslušná doména druhej a vyššej úrovne bola pod kontrolou Odberateľa, ktorý žiada o vydanie KC pre autentifikáciu webového sídla.

Overenie informácie, že Odberateľ je vlastníkom domény, resp. má kontrolu nad danou doménou, ktorej FQDN sa nachádza v položke CN žiadosti, resp. bude uvedené v položke Subject Alternative Name (SAN), pozostáva z nasledovných činností:

- Registračný operátor RA SNCA sa spoľahne na potvrdenie od oprávneného orgánu Odberateľa vo forme prehlásenia o vlastníctve domény. Prehlásenie o vlastníctve domény musí jasne preukazovať, že pochádza od Oprávneného kontaktu domény, ohláseného u oprávneného registrátora najvyššej úrovne (pre doménu „.sk“ je to Sk-NIC, a.s.), pričom registračný operátor RA SNCA je povinný overiť, že predložené potvrdenie o vlastníctve domény:
  - obsahuje dátum, ktorý je totožný alebo neskorší ako dátum kedy bola žiadosť podaná,
  - údaje vo WHOIS databáze oprávneného registrátora sa nezmenili pri porovnaní s údajmi, ktoré boli predložené v prehlásení o vlastníctve domény pri predchádzajúcom vyhotovovaní kvalifikovaného certifikátu pre dané FQDN.
- Pokiaľ sa nedá spoľahlivo zistiť, že Odberateľ má plnú kontrolu nad danou doménou, registračný operátor RA SNCA je povinný odmietnuť vydanie KC pre danú žiadosť.

Rovnaké pravidlá overovania platia aj pre „wildcard“ KC pre autentifikáciu webového sídla, ktoré obsahujú znak hviezdička (*) na tretej a vyššej pozícii úrovne domény.

3.2.4 Neoverované informácie o Držiteľovi

Neoverené informácie o žiadateľovi, ktorý predloží žiadosť o vydanie certifikátu, SNCA nebude spracovávať.

Registračným operátorom RA SNCA nie sú overované informácie týkajúce týchto položiek :

- názov organizačnej jednotky (položka OH).

3.2.5 Overovanie oprávnení

Platia rovnaké ustanovenia, ako v bode 3.2.5 dokumentu „Pravidlá na výkon certifikačných činností (CPS) SNCA“ [12].

3.2.6 Kritériá interoperability

Neuplatňuje sa.

3.3 Identifikácia a autentifikácia pri vyhotovovaní následného KC

Proces rutinného pregenerovania kľúčového materiálu, vždy pozostáva z vygenerovania nového asymetrického kľúčového páru a z vydania nového certifikátu. Identifikácia a autentizácia žiadateľa o pregenerovanie kľúčov prebieha podľa postupu, uvedeného v bodoch 3.2.2 a 3.2.3 tohto dokumentu.

3.4 Identifikácia a autentifikácia pri žiadaní o zrušenie KC

O zrušenie vydaného certifikátu môže požiadať:

- držiteľ certifikátu (fyzická osoba, fyzická osoba, identifikovaná v spojení s právnickou osobou, fyzická osoba, identifikovaná v spojení s OVM), s ktorou má prevádzkovateľ SNCA uzatvorenú „Zmluvu o poskytovaní kvalifikovaných dôveryhodných služieb“,
- štatutárny zástupca alebo ním poverená osoba príslušnej organizačnej zložky právnickej osoby alebo organizačnej zložky OVM, s ktorou má prevádzkovateľ SNCA uzatvorenú „Zmluvu o poskytovaní kvalifikovaných dôveryhodných služieb“,
- autorizovaný zástupca SNCA,
- tretia strana zo zákona (v súlade s platnými právnymi predpismi SR a EÚ, napr. súd).

Žiadosť o zrušenie KC môže byť autentizovaná použitím súkromného kľúča patriaceho ku KC, ktorý sa má zrušiť, bez ohľadu na to, či daný súkromný kľúč bol alebo nebol kompromitovaný.

Proces a postupy pri žiadaní o zrušenie KC sú záväzné pre každého žiadateľa o zrušenie certifikátu, vydaného SNCA a každý žiadateľ o zrušenie certifikátu je povinný ich dodržať. Proces a postupy pri žiadaní o zrušenie KC, sú bližšie popísané v bode 4.9 tohto dokumentu a riadia sa ustanoveniami, popísanými v bode 3.4 dokumentu „Pravidlá na výkon certifikačných činností (CPS) SNCA“ [12].

4 Požiadavky na životný cyklus certifikátu

V tejto kapitole je popísaný životný cyklus KC označovaný aj ako Certificate Management Life Cycle (CMLC).

Životný cyklus certifikátu pozostáva z primárnych a sekundárnych stavov. Každý vydaný KC prechádza všetkými stavmi.

Primárnymi stavmi sú:

a) žiadosť o vydanie certifikátu,

b) vyhotovenie certifikátu,

c) vydanie (odovzdanie) certifikátu držiteľovi,

d) aktivácia,

e) používanie,

f) exspirácia,

Sekundárnym stavom životného cyklu správy KC je zrušenie certifikátu pred ukončením jeho platnosti.

4.1 Žiadosť o vydanie KC

4.1.1 Kto môže žiadať o vydanie KC

NASES môžu požiadať o vydanie KC fyzické alebo právnické osoby (Odberatelia) a NASES môže vydať iba nasledovné typy certifikátov:

- KC pre elektronický podpis pre fyzickú osobu:
  - žiadateľom je fyzická osoba resp. fyzická osoba splnomocnená Držiteľom alebo konajúca na základe zákona alebo rozhodnutia príslušného orgánu,
  - žiadateľom je akákoľvek entita (Odberateľ), s ktorou je fyzická osoba spojená napr. jej zamestnávateľ (OVM), nezisková organizácia, ktorej je členom a pod..
- KC pre elektronickú pečať pre právnickú osobou a orgány verejnej moci:
  - žiadateľom je akákoľvek entita (Odberateľ), ktorá v zmysle platnej národnej legislatívy koná v mene danej právnickej osoby.
- KC pre autentifikáciu webového sídla:
  - žiadateľom je fyzická alebo právnická osoba, prevádzkujúca zariadenie resp. systém,
  - žiadateľom je akákoľvek entita (Odberateľ), ktorá v zmysle platnej národnej legislatívy koná v mene danej právnickej osoby.

- Mandátny certifikát:
  - žiadateľom je fyzická osoba, oprávnená zo zákona alebo na základe zákona konať za inú osobu alebo orgán verejnej moci, alebo v ich mene, alebo fyzická osoba, ktorá vykonáva činnosť podľa osobitného predpisu (§8 ods. 1 zákona č. 272/2016 Z. z.), alebo vykonáva funkciu podľa osobitného predpisu (§8 ods. 1 zákona č. 272/2016 Z. z.),
  - žiadateľom je akákoľvek entita (Odberateľ), s ktorou je fyzická osoba spojená napr. jej zamestnávateľ, nezisková organizácia, ktorej je členom a pod..

4.1.2 Registračný proces a zodpovednosti

Certifikáty vydáva NASES prostredníctvom svojej RA SNCA. Fyzická osoba alebo fyzická osoba v spojení s právnickou osobou alebo OVM, pre ktorú bude vydávaný niektorý KC, uvedený v časti 4.1.1, sa musí osobne dostaviť na registračné miesto RA SNCA, resp. môže splnomocniť/poveriť inú fyzickú na konanie vo svojom mene na registračnom mieste RA SNCA.

Pred samotným dostavením sa na registračné miesto RA SNCA, je táto osoba povinná oboznámiť sa s touto CP a podmienkami poskytovania dôveryhodných služieb NASES, pripraviť si hodnoty jednotlivých položiek, ktoré budú súčasťou žiadosti o vydanie KC, pripraviť si potrebné doklady na identifikáciu a autentifikáciu, prípadne ďalšie doklady, ktoré je povinná predložiť na registračnom mieste RA SNCA.

Registračný operátor RA SNCA musí pred samotným procesom vydania KC informovať prítomnú fyzickú osobu o podmienkach používania KC.

Po poučení musí registračný operátor RA SNCA vykonať autentifikáciu a identifikáciu fyzickej osoby alebo právnickej osoby ako budúceho držiteľa KC, resp. fyzickej osoby ktorá zastupuje inú fyzickú alebo právnickú osobu a zaznamenať všetky požadované identifikačné údaje (meno a priezvisko, rodné číslo, adresu trvalého bydliska, údaje o dokladoch totožnosti, na základe ktorých bola vykonaná identifikácia a autentifikácia) do svojho informačného systému.

Registračný operátor RA SNCA musí rovnako overiť aj ďalšie predložené doklady podľa stanovených postupov.

4.1.3 Generovanie žiadosti

V prípade žiadosti o vydanie KC pre elektronický podpis alebo elektronickú pečať, kedy sú kryptografické kľúče generované v kvalifikovanom zariadení na vydanie elektronického podpisu resp. pečate (QSCD) Odberateľa, musí Registračný operátor RA SNCA, po overení identity Odberateľa/ Držiteľa, vygenerovať kľúčový pár (verejný kľúč a súkromný kľúč) v QSCD Odberateľa a následne vytvorí elektronickú žiadosť na vydanie Certifikátu vo formáte PKCS#10.

V prípade žiadosti o vydanie KC pre elektronický podpis alebo elektronickú pečať, kedy kryptografické kľúče nie sú generované v QSCD Odberateľa, musí Registračný operátor RA

SNCA, pred overením identity Odberateľa/Držiteľa, skontrolovať doručenú elektronickú žiadosť na vydanie Certifikátu vo formáte PKCS#10.

V prípade žiadosti o vydanie KC pre autentifikáciu webového sídla, musí Registračný operátor RA SNCA, pred overením identity Odberateľa, skontrolovať doručenú elektronickú žiadosť na vydanie Certifikátu vo formáte PKCS#10.

V prípade žiadosti o vydanie KC pre autentifikáciu webového sídla je potrebné, aby si Odberateľ vygeneroval kryptografické kľúče odporúčanej veľkosti a následne si pripravil, vygeneroval elektronickú žiadosť o vydanie KC vo formáte PKCS#10. Pripravenú žiadosť o vydanie KC vo formáte PKCS#10, musí Odberateľ zaslať na kontrolu registračnému operátorovi RA SNCA vopred.

V prípade generovania kľúčového páru priamo u Odberateľa, musí byť zabezpečená dôvernosť takto generovaných údajov.

Registračný operátor RA SNCA musí vždy overiť, či zariadenie, v ktorom sú generované kľúče, či už priamo u Poskytovateľa alebo pod kontrolou Odberateľa, je certifikované QSCD.

Na verejný kľúč, na ktorý bol certifikačnou autoritou SNCA už raz vyhotovený kvalifikovaný certifikát, nie je možné opakovane vydať nový kvalifikovaný certifikát.

Žiadosť na vydanie kvalifikovaného certifikátu, musí generovať registračný operátor RA SNCA priamo v kvalifikovanom zariadení, prostredníctvom aplikačného softvéru (RA Client). Proces generovania kľúčového páru musí zabezpečiť dôvernosť takto generovaných údajov.

4.2 Spracovanie žiadosti o vydanie certifikátu

4.2.1 Vykonanie identifikácie a autentifikácie

Identifikácia fyzickej osoby, právnickej osoby, resp. fyzickej osoby konajúcej v mene alebo za inú fyzickú osobu, právnickú osobu alebo za orgán verejnej moci, sa vykoná v zmysle bodov 3.2.2. resp. 3.2.3 a pri vyhotovovaní následného certifikátu v zmysle bodu 3.3 tohto dokumentu.

Po vykonaní autentifikácie a identifikácie Držiteľa KC a zapísaní požadovaných osobných údajov do informačného systému Poskytovateľa, musí registračný operátor RA SNCA vykonať zadanie údajov žiadosti o vyhotovenie KC a v prípade použitia vopred zaslanej žiadosti, vykonať jej vizuálnu kontrolu.

Kontrola vyplnenia údajov (osobné údaje a údaje v žiadosti o KC), bude zároveň vykonaná aj samotnou aplikáciou - programovým vybavením, používaným registračným operátorom RA SNCA, ktoré neumožní pokračovať vo vyhotovovaní KC v prípade nevyplnenej položky, ktorá je povinná resp. v prípade nesprávne vyplnenej položky.

Komunikácia externých registračných autorít SNCA so systémom SNCA a IS certifikačnej autority CA SNCA, je realizovaná prostredníctvom zabezpečeného kanála a je umožnená iba registrovaným a autentifikovaným registračným operátorom RA SNCA.

4.2.2 Zaslanie žiadosti na vyhotovenie Certifikátu

Žiadosť na vyhotovenie certifikátu musí generovať registračný operátor RA SNCA priamo v kvalifikovanom zariadení prostredníctvom aplikačného softvéru (RA Client), ktorý zabezpečí dôveryhodné odoslanie žiadosti do IS certifikačnej autority CA SNCA.

V prípade žiadosti na vyhotovenie KC pre autentifikáciu webového sídla, musí registračný operátor RA SNCA pred overením identity Odberateľa, skontrolovať doručenú žiadosť o vydanie KC vo formáte PKCS#10.

4.2.3 Schválenie alebo zamietnutie žiadosti

Registračný operátor RA SNCA musí pred vydaním KC vykonať formálnu kontrolu všetkých osobných údajov fyzickej osoby, právnickej osoby, resp. fyzickej osoby konajúcej v mene alebo za inú fyzickú osobu, právnickú osobu alebo za orgán verejnej moci, poskytovaných do IS SNCA a rovnako údajov obsiahnutých v žiadosti. Overovanie stavu, či súkromný kľúč zodpovedá verejnému kľúču, obsiahnutému v žiadosti, musí byť vykonané aplikáciou na vyhotovovanie KC ešte pred samotným vydaním, rovnako ako formálna kontrola vyplnenia jednotlivých položiek žiadosti.

V prípade, že niektorá z kontrol skončí negatívne, musí registračný operátor RA SNCA ukončiť proces vyhotovovania KC a informovať o tejto skutočnosti prítomnú osobu, konajúcu v mene Odberateľa.

4.2.4 Čas spracovania žiadosti o KC

Po zaslaní žiadosti o vydanie KC do systému SNCA a po splnení všetkých podmienok na vydanie KC, bude KC pre Odberateľa vydaný v čo najkratšom možnom čase.

4.3 Vydanie KC

Vydanie kvalifikovaného certifikátu do kvalifikovaného zariadenia QSCD, musí byť bezpečne naviazané na proces generovania žiadosti v tomto kvalifikovanom zariadení.

4.3.1 Činnosť NASES pri vyhotovovaní KC

Po odoslaní žiadosti na vydanie KC z registračnej autority RA SNCA, systém SNCA pred samotným vydaním KC vykoná kontrolu, či žiadosť bola odoslaná oprávneným registračným operátorom RA SNCA a či zodpovedá predpísanému štandardu PKCS#10.

V prípade, že boli splnené všetky podmienky na vydanie KC, SNCA je povinná KC vyhotoviť.

Po vyhotovení, musí byť každý KC odovzdaný Odberateľovi dôveryhodným spôsobom.

Rozlišovacie meno vydávajúcej SNCA nesmie byť počas jej životnosti prenesené na inú entitu.

4.3.2 Informovanie Držiteľa o vydaní certifikátu

Registračný operátor RA SNCA musí vhodným spôsobom informovať Odberateľa/Držiteľa o vydaní KC.

4.4 Prevzatie vydaného certifikátu

4.4.1 Spôsob prevzatia certifikátu

Registračný operátor RA SNCA je povinný bezpečným spôsobom odovzdať vydaný KC jeho Držiteľovi.

4.4.2 Zverejnenie certifikátu

KC, ktoré obsahujú osobné údaje Držiteľa, nebudú zverejňované z dôvodu ochrany jeho osobných údajov.

4.4.3 Oznámenie o vydaní certifikátu iným stranám

NASES, v zmysle požiadaviek §6 ods. 2 zákona č. 272/2016 Z. z., informuje o vydaní kvalifikovaného certifikátu Národný bezpečnostný úrad.

4.5 Kľúčový pár a používanie certifikátu

V tejto časti sú popísané zodpovednosti, týkajúce sa používania kľúčov a KC.

4.5.1 Používanie súkromného kľúča a KC Držiteľom

Držiteľ KC má vo vzťahu k vygenerovanému súkromnému kľúču a vyhotovenému a vydanému KC nasledovné povinnosti:

- poskytnúť registračnému operátorovi RA SNCA v procese podania žiadosti o vydanie KC presné a úplné informácie,
- používať kľúčový pár iba na účely, pre ktoré bol vydaný a v súlade požiadavkami, ktoré sú dané v tejto certifikačnej politike,
- neustále chrániť svoje súkromné kľúče tak, aby boli výhradne pod jeho kontrolou,

- využívať súkromný kľúč až po vygenerovaní a odovzdaní KC k verejnému kľúču, s ktorým tvorí súkromný kľúč pár,
- v čase platnosti KC bezodkladne upovedomiť agentúru NASES o:
  - podozrení, že jeho súkromný kľúč bol kompromitovaný, odcudzený alebo stratený,
  - podozrení, že stratil kontrolu nad súkromným kľúčom kompromitáciou jeho aktivačných údajov (PIN),
  - nepresnostiach alebo zmenách v obsahu KC,
- okamžite ukončiť používanie súkromného kľúča po jeho kompromitácii (vrátane prípadu, že došlo ku kompromitácii samotného Poskytovateľa a Odberateľ/Držiteľ má o tom vedomosť),
- bezodkladne požiadať o zrušenie KC v prípade, že akýkoľvek údaj, uvedený v subjekte KC sa stal neplatným,
- ukončiť používanie súkromného kľúča po exspirácii, alebo zrušení KC verejného kľúča.

Povinnosti Držiteľa KC sa týkajú aj fyzickej osoby, ktorá prevzala KC pre autentifikáciu webového sídla.

4.5.2 Používanie verejného kľúča a KC Spoliehajúcou sa stranou

Spoliehajúce sa strany sú povinné:

- používať KC len na účel, pre ktorý bol vydaný,
- predtým, ako sa na KC spoľahnú, overovať každý KC na platnosť (tzn. overovať, že KC je v danom čase platný a že sa nenachádza na aktuálnom zozname zrušených KC, vydanom NASES),
- uchovávať originálne podpísané údaje, aplikácie potrebné na čítanie a spracovanie týchto údajov a kryptografické aplikácie, potrebné na overovanie kvalifikovaných elektronických podpisov týchto údajov, pokiaľ môže byť potrebné overovať podpis týchto údajov.

4.6 Obnova certifikátu

Služba obnovy certifikátu spočíva vo vyhotovení nového certifikátu na verejný kľúč, na ktorý už bol v minulosti SNCA vyhotovený KC.

SNCA v zmysle tejto CP nesmie vydať KC na takýto verejný kľúč. Takáto služba nie je agentúrou NASES poskytovaná.

4.7 Vydanie následného KC

Pod pojmom následný certifikát sa myslí vydanie nového KC rovnakého typu a s rovnakým obsahom položiek Subject a SubjectAlternativeName pre už existujúceho Držiteľa, ktorého osobné údaje sú zavedené v informačnom systéme SNCA.

4.7.1 Podmienky vydania následného KC

Následný KC môže byť vydaný len v prípade, že:

- skončila platnosť pôvodného KC resp. tento bol zrušený,
- položky žiadosti o vydanie sú zhodné s údajmi KC, ktorý je nahrádzaný,
- boli vygenerované nové kryptografické kľúče a pripravená a podpísaná nová žiadosť,
- bol vykonaný proces identifikácie a autentifikácie držiteľa v súlade s bodom 3.2.

4.7.2 Kto môže žiadať o vydanie následného KC.

O vydanie následného KC je oprávnený požadovať existujúci Držiteľ, ktorému bol agentúrou NASES v minulosti KC vydaný a ktorý splní požiadavky, uvedené v bode 4.7.1 tohto dokumentu.

4.7.3 Postup žiadania o vydanie následného KC

Následný KC musí byť vydaný rovnakým spôsobom ako bol vyhotovený pôvodný KC.

4.7.4 Oznámenie o vydaní následného KC

Registračný operátor RA SNCA je povinný vhodným spôsobom informovať Držiteľa KC o vydaní následného KC.

4.7.5 Spôsob prevzatia následného KC

Platia ustanovenia podľa bodu 4.4 tohoto dokumentu.

4.7.6 Zverejňovanie následného KC

Platia ustanovenia podľa bodu 4.4.2 tohto dokumentu.

4.7.7 Oznámenie o vydaní následného KC iným subjektom

Neuplatňuje sa.

4.8 Modifikácia KC

Vydanie nového KC, bez súčasnej zmeny kľúčového páru, z dôvodu zmien týkajúcich sa jeho obsahu NASES nepodporuje. U existujúceho Držiteľa je možné postupovať podobne, ako pri vyhotovení následného KC, kde sa pôvodný KC s nevyhovujúcim obsahom zruší.

4.9 Zrušenie KC

Žiadosť o zrušenie kvalifikovaného certifikátu je možné podať:

- na registračnom mieste RA SNCA,
- elektronickou formou,
- listovou zásielkou,
- telefonicky.

Na registračnom mieste RA SNCA, podáva Držiteľ KC žiadosť o zrušenie certifikátu písomnou formou, osobne. Žiadosť o zrušenie KC môže Držiteľ KC podať na každom registračnom mieste RA SNCA, počas pracovnej doby príslušného registračného miesta RA SNCA.

Elektronickú žiadosť o zrušenie certifikátu je potrebné podať na e-mailovú adresu registračného miesta RA SNCA, ktoré vydalo certifikát.

V prípade podania žiadosti o zrušenie certifikátu listovou zásielku je potrebné doručiť listovú zásielku na poštovú adresu registračného miesta RA SNCA, ktoré vydalo certifikát.

Telefonicky je možné podať žiadosť o zrušenie certifikátu na zverejnený telefonický kontakt registračného miesta RA SNCA, ktoré vydalo certifikát.

4.9.1 Podmienky zrušenia KC

Každý vyhotovený KC je nevyhnutné zrušiť v prípade, keď sa väzba medzi Držiteľom súkromného kľúča a verejným kľúčom, uvedeným v jeho kvalifikovanom certifikáte, už nepovažuje za platnú. Agentúra NASES, ako poskytovateľ KDS, je povinná zrušiť kvalifikovaný certifikát, ktorý spravuje, v týchto prípadoch:

- O zrušenie certifikátu požiada Držiteľ KC.
- NASES zistí, že:
  - došlo ku kompromitácii súkromného kľúča patriaceho k danému KC, napr. ak prístup k súkromnému kľúču, patriacemu k verejnému kľúču, uvedenému v KC pozná iná osoba, než Držiteľ uvedený v KC,
  - KC bol vydaný na základe nepravdivých údajov,
  - pri vydaní KC neboli splnené požiadavky Nariadenie eIDAS resp. zákona č. 272/2016 Z. z.,

- údaje uvedené v certifikáte sa stali neaktuálnymi,
- Držiteľ KC zomrel ak ide o fyzickú osobu resp. ak ide o právnickú osobu zanikol,
- Držiteľ KC sa stal nesvojprávnym na základe rozhodnutia súdu,

- Zrušenie KC nariadi SNCA svojím rozhodnutím súd.
- Držiteľ KC porušil svoje povinnosti, stanovené touto CP.
- Ak, v prípade vydaného mandátneho certifikátu, o zrušenie KC požiadal:
  - mandant,
  - mandatár,
  - orgán verejnej moci alebo osoba, u ktorej mandatár vykonáva činnosť alebo funkciu podľa osobitného predpisu (§ 8 ods. 1 zákona č. 272/2016 Z. z.),
- Došlo ku kompromitácii súkromného kľúča SNCA.

Zrušený KC musí byť zapísaný do zoznamu zrušených certifikátov (CRL), vydávaného v pravidelných intervaloch, čo najskôr po čase, kedy bol KC zrušený a musí sa v tomto zozname vyskytnúť minimálne do času jeho exspirácie, resp. informácia o jeho zrušení, musí byť dostupná prostredníctvom služby OCSP.

Zrušený KC nie je možné obnoviť za žiadnych okolností.

4.9.2 Kto môže žiadať o zrušenie KC

Držiteľ KC (alebo ním poverená fyzická alebo právnická osoba) môže kedykoľvek požiadať o zrušenie svojho vlastného KC spôsobom, stanoveným v tejto CP a to aj bez udania dôvodu v žiadosti o zrušenie.

O zrušenie certifikátu môže tiež požiadať:

- NASES, pričom príslušný zamestnanec agentúry je povinný písomne zdokumentovať túto skutočnosť, vrátane dôvodu svojho konania.
- súd, prostredníctvom svojho rozsudku alebo predbežného opatrenia, pričom k dokumentom o zrušení KC musí NASES priložiť kópiu príslušného súdneho rozhodnutia,
- subjekt (fyzická alebo právnická osoba) na základe dedičského konania, pričom k dokumentom o zrušení KC musí Poskytovateľ priložiť kópiu dokladov, z ktorých vyplýva právo daného subjektu žiadať o zrušenie KC,
- súdom poverená osoba, napr. poručník subjektu KC, ktorý sa má zrušiť, pričom k dokumentom o zrušení KC musí Poskytovateľ priložiť kópiu príslušného súdneho rozhodnutia,
- orgán verejnej moci alebo osoba, u ktorej mandatár vykonával činnosť alebo funkciu podľa osobitného predpisu (§ 8 ods. 1 zákona č. 272/2016 Z. z.), mandant resp. mandatár.

4.9.3 Postup žiadania o zrušenie KC

V prípade, že žiadosť o zrušenie KC podávaná osobne Držiteľ KC, v žiadosti je potrebné uviesť meno a priezvisko Držiteľa KC a sériové číslo KC, o ktorého zrušenie sa žiada. Držiteľ sa musí podrobiť obdobnému procesu identifikácie a autentifikácie, aký je požadovaný pri prvotnom vydaní KC, t. j. musí predložiť minimálne jeden identifikačný doklad, ktorý obsahuje jeho meno a priezvisko, fotku, rodné číslo alebo dátum narodenia (pozri odstavec 3.2), alebo sa musí preukázať dohodnutým heslom na zrušenie KC, ktoré Odberateľ/Držiteľ dostane po vydaní KC.

Držiteľa KC môže vo veci zrušenia KC zastupovať splnomocnená/poverená osoba. Zastupujúca osoba sa musí preukázať úradne overeným splnomocnením resp. poverením, alebo inou úradne overenou listinou, v texte ktorých je jednoznačne vyjadrená vôľa Držiteľa KC zrušiť ním vlastnený kvalifikovaný certifikát.

NASES môže odmietnuť zrušenie KC v prípade, že Držiteľ, resp. ním splnomocnená/poverená osoba dostatočným spôsobom nepreukážu svoju identitu a oprávnenosť, žiadať o zrušenie predmetného KC.

Registračný operátor RA SNCA je povinný preveriť platnosť certifikátu, ktorý sa má zrušiť. V prípade certifikátu, ktorý už nie je platný, musí odmietnuť žiadosť o jeho zrušenie, keďže nie je možné zrušiť certifikát, ktorého platnosť už vypršala, alebo ktorý už bol zrušený.

V prípade, že registračný operátor RA SNCA úspešne overení identitu Odberateľa/Držiteľa a posúdi žiadosť o zrušenie KC ako oprávnenú, musí daný KC bezodkladne zrušiť.

Žiadosť o zrušenie KC, môže byť doručená na registračné miesto RA SNCA aj nasledovnými formami:

- elektronickou poštou na kontaktnú e-mail-ovú adresu registračného miesta RA SNCA. Žiadosť musí obsahovať správu s jednoznačne vyjadrenou vôľou zrušiť KC, konkrétne vetu - "Žiadam týmto o zrušenie svojho KC so sériovým číslom „nnnnnn" a heslo na zrušenie je: xxxxxx“, kde za „nnnnnn“ a „xxxxxx“ vyplní Žiadateľ o zrušenie KC reálne údaje, platné pre KC, ktorý žiada zrušiť.
- písomne, na kontaktnú adresu registračného miesta RA SNCA.
  Odberateľ/Držiteľ musí v písomnej žiadosti uviesť sériové číslo KC, ktorého zrušenie žiada, pričom zrušenie je potrebné autentizovať pomocou platného hesla na zrušenie daného KC.

V prípade, že registračný operátor RA SNCA posúdi elektronicky doručenú žiadosť, resp. žiadosť doručenú listom ako oprávnenú, musí daný KC čo najskôr zrušiť.

Držiteľ, žiadajúci o zrušenie kvalifikovaného certifikátu elektronickou poštou, resp. písomne, musí byť o zrušení KC bezodkladne informovaný (e-mailom resp. písomne).

4.9.4 Čas na podanie žiadosti o zrušenie KC

V prípade hrozby kompromitácie súkromného kľúča, musí oprávnená osoba (v rozsahu bodu

4.9.2 tohto dokumentu) podať žiadosť o zrušenie KC ihneď, ako sa o danej skutočnosti dozvie. Osobne, je možné žiadať o zrušenie KC len v pracovnej dobe, určenej jednotlivými RA SNCA, ktorých zoznam a pracovná doba je zverejnená na webovom sídle agentúry NASES. Pri elektronickej žiadosti, je možné zaslať takúto žiadosť na jednotlivé RA kedykoľvek.

4.9.5 Čas na zrušenie KC

Na základe prijatej a platnej žiadosť o zrušenie KC, registračný operátor RA SNCA zabezpečí:

- zrušenie KC čo možno najskôr od momentu prijatia platnej žiadosti o zrušenie KC, najneskôr však do 24 hodín od momentu prijatia oprávnenej žiadosti,
- zverejnenie zrušeného KC v aktuálnom zozname zrušených KC a zabezpečí zverejnenie tohto zoznamu spoločne so všetkými predchádzajúcimi zoznamami zrušených certifikátov, v najkratšom možnom čase po zrušení KC tak, aby boli prístupné Odberateľom/Držiteľom a všetkým spoliehajúcim sa stranám,
- informovanie Odberateľa/Držiteľa KC o zrušení jeho KC, zaslaním správy na e-mailovú adresu, ktorú poskytol Držiteľ v priebehu registrácie na RA SNCA, pričom v zaslanej správe uvedie aj informáciu o dôvode zrušenia daného KC,
- kontrolu synchronizácie systémového času, vyžívaného ako zdroj pre údaj času zrušenia certifikátu, s UTC časom, minimálne v perióde každých 24 hodín,
- následnú archiváciu všetkých zoznamov zrušených KC (CRL), ktoré vydal.

Aktualizovaný zoznam CRL, musí byť publikovaný do úložiska SNCA v čo najkratšom čase po jeho vydaní.

4.9.6 Overovanie platnosti zo strany spoliehajúcej sa strany

Spoliehajúca sa strana je povinná pri spoľahnutí sa na KC overiť si jeho platnosť prostredníctvom dostupného zoznamu zrušených certifikátov (CRL), resp. prostredníctvom služby OCSP.

V čase, medzi podaním oprávnenej žiadosti o zrušenie KC a zverejnením zrušeného KC v CRL, nesie Odberateľ/Držiteľ certifikátu, všetku zodpovednosť za prípadné škody, spôsobené zneužitím jeho KC. Po zverejnení certifikátu v CRL, nesie všetku zodpovednosť za prípadné škody spôsobené použitím zrušeného KC strana, ktorá sa na daný zrušený KC spoľahla.

Neoverenie platnosti KC pomocou CRL je brané ako hrubé porušenie tejto certifikačnej politiky.

4.9.7 Frekvencia vydávania CRL

Zoznamy CRL sa vydávajú a zverejňujú minimálne raz za 24 hodín.

Zároveň je potrebné zabezpečiť, aby od prijatia žiadosti o zrušenie certifikátu do zverejnenia prvého zoznamu zrušených certifikátov, ktorý obsahuje číslo zrušeného KC, neuplynulo viac ako 24 hodín.

SNCA publikuje zoznamy CRL nasledovne:

SNCA

Prehľad zrušených certifikátov (HTTP):

http://ep.nbusr.sk/snca/crl2.html

http://ep.nbu.gov.sk/snca/crl3.html

Archív CRL (HTTP):

http://ep.nbusr.sk/snca/archive2/

http://ep.nbu.gov.sk/snca/archive3/

4.9.8 Doba publikovania CRL

NASES musí zabezpečiť, že čas od vydania zoznamu CRL do jeho publikovania v úložisku, uvedenom v bode 4.9.7, nepresiahne 300 sekúnd.

4.9.9 Dostupnosť služby OCSP

URI adresy OSCP služby Poskytovateľa, musia byť obsiahnuté v každom vydanom certifikáte v rozšírení Authority Information Access:

http://snca3-ocsp.nbu.gov.sk/ocsp/snca3

http://ocsp.nbu.gov.sk/ocsp/valid

Služba OCSP je v zmysle Nariadenia eIDAS, poskytovaná bezodplatne.

4.9.10 Požiadavky na OCSP overovanie

Tretie strany, ktoré majú záujem využívať službu OCSP, musia zaslať požiadavku na OCSP adresu, ktorá je uvedená vo vydanom certifikáte, ktorého platnosť požadujú overiť. Zaslaná žiadosť musí byť v súlade s požiadavkami RFC 6960.

4.9.11 Iné formy dostupnosti informácií o zrušení certifikátu

SNCA využíva na oznámenie o zrušení certifikátu mechanizmus publikovania zoznamov CRL v rozsahu bodu 4.9.7 tohto dokumentu, iné formy oznámenia o zrušení certifikátu nie sú podporované.

4.9.12 Špeciálne požiadavky na zmenu kľúčov po ich kompromitácii

SNCA nestanovuje špeciálne požiadavky na proces zrušenia certifikátu pre prípad kompromitácie súkromného kľúča.

4.9.13 Okolnosti pozastavenia platnosti certifikátu

SNCA nepodporuje inštitút pozastavenia platnosti certifikátu.

4.9.14 Suspendovanie certifikátu

Neuplatňuje sa.

4.10 Služby súvisiace so stavom certifikátu

4.10.1 Prevádzkové požiadavky

Aktuálny zoznam zrušených certifikátov, ktorého URI je uvedená v samotnom KC, musí byť dostupný prostredníctvom HTTP protokolu (port: 80) na tejto URI adrese.

Archív zoznamov zrušených certifikátov, musí byť dostupný na URL adrese, uvedenej v bode 4.9.7 a dostupný prostredníctvom HTTP protokolu na porte: 80.

Služba OCSP, musí byť dostupná na URL adrese, uvedenej vo vydanom certifikáte a žiadateľ o zistenie stavu certifikátu, musí zaslať žiadosť v zmysle bodu 4.9.10.

4.11 Ukončenie poskytovania služieb

Ukončenie poskytovania služieb môže nastať jedným z nasledovných spôsobov:

- vypovedanie „Zmluvy o poskytovaní kvalifikovaných dôveryhodných služieb“ medzi prevádzkovateľom SNCA a Odberateľom služieb,
- vypovedanie „Zmluvy o vydaní a používaní kvalifikovaného certifikátu“ s Držiteľom KC,
- zrušenie certifikátu.

V prípade, že sa Odberateľ/Držiteľ rozhodne ukončiť zmluvný vzťah s agentúrou NASES pred uplynutím doby platnosti vydaného KC, je povinný zároveň požiadať o zrušenie certifikátu.

4.12 Úschova a obnova kľúčov

SNCA takúto službu nepodporuje ani neposkytuje.

5 Fyzické, personálne a prevádzkové bezpečnostné opatrenia

Fyzická bezpečnosť SNCA je riešená v zmysle ustanovení vyhlášky NBÚ č. 336/2004 Z. z. o fyzickej bezpečnosti a o objektovej bezpečnosti v znení vyhlášky NBÚ č. 315/2006 Z. z. (ďalej aj „vyhláška NBÚ č. 336/2004 Z. z.“).

Bezpečnosť NASES, ako prevádzkovateľa SNCA, je založená na súhrne bezpečnostných opatrení v oblasti fyzickej, objektovej, personálnej a prevádzkovej bezpečnosti. Bezpečnostné opatrenia, aplikované v rámci zabezpečenia prevádzky SNCA a poskytovania kvalifikovaných dôveryhodných služieb sú navrhnuté, dokumentované a aplikované na základe bezpečnostnej politiky a bezpečnostných pravidiel NASES, ktoré sú schválené vedením agentúry NASES.

Bezpečnostné opatrenia sú k dispozícii všetkým pracovníkom, ktorých sa týkajú.

Agentúra NASES:

- preberá plnú zodpovednosť za súlad svojej činnosti s postupmi, definovanými v svojej bezpečnostnej politike, vrátane jej dodržiavania zo strany externých registračných autorít,
- definuje zodpovednosť externých registračných autorít a zaväzuje externé registračné autority dodržiavaním stanovených bezpečnostných opatrení,
- má spracovaný zoznam všetkých svojich aktív, s vyznačením ich klasifikácie v zmysle vykonaného posúdenia rizika.

Bezpečnostná politika SNCA a zoznam aktív, sú preskúmavané v pravidelných intervaloch, prípadne pri významných zmenách v prevádzke SNCA, z dôvodu zaistenia ich kontinuity, vhodnosti, dostatočnosti a účinnosti.

Všetky zmeny, ktoré môžu ovplyvniť úroveň poskytovanej bezpečnosti, musia byť schválené vedením agentúry NASES.

Konfigurácia a nastavenia systémov agentúry NASES, sú pravidelne prehodnocované v súvislosti so zmenami, ktoré ohrozujú bezpečnostnú politiku agentúry NASES.

5.1 Opatrenia týkajúce sa fyzickej bezpečnosti

5.1.1 Priestory

Technologické priestory, v ktorých je umiestnená základná infraštruktúra SNCA, sú chránenými priestormi, zabezpečujúcimi ochranu infraštruktúry SNCA pred živelnými pohromami a haváriami v inžinierskych sieťach. Technologické priestory sú prístupné iba autorizovaným osobám a od iných priestorov sú oddelené prostredníctvom primeraných bezpečnostných prvkov (bezpečnostné dvere, mreže, pevné múry a pod.).

Technologické vybavenie a komplexná infraštruktúra SNCA, slúžia výhradne na zabezpečenie prevádzky kvalifikovaných dôveryhodných služieb, poskytovaných agentúrou NASES.

5.1.2 Fyzický prístup

Chránený, technologický, prevádzkový priestor, v ktorom je umiestnená infraštruktúra SNCA a ktorý predstavuje zónu s najvyššou bezpečnosťou, je zabezpečený bezpečnostným alarmom a prístup do tohto priestoru je umožnený iba osobám, ktoré vlastnia bezpečnostný prístupový prvok a sú uvedené v zozname oprávnených osôb, ktorým je povolený prístup do chránených priestorov.

Prístup iných osôb do chránených priestorov SNCA, je umožnený iba v sprievode oprávnenej, zodpovednej osoby. Každý takýto prístup je zodpovednou osobou riadne zaznamenaný do príslušnej dokumentácie k chránenému priestoru.

Prístup do priestorov umiestnenia prevádzkovaného systému SNCA, je riadený prísnou bezpečnostnou politikou a pravidelne auditovanými procedúrami. Agentúra NASES má pripravené spôsoby a postupy na ochranu svojich počítačových systémov, údajov a archívov proti neoprávnenej manipulácii, krádeži a prezradeniu.

5.1.3 Zásobovanie elektrickou energiou a klimatizácia

Komponenty infraštruktúry SNCA sú chránené neprerušiteľnými zdrojmi elektrického napájania. Priestory, v ktorých sa nachádza infraštruktúra SNCA, sú vybavené klimatizáciou.

5.1.4 Ochrana pre vodou

Priestory umiestnenia infraštruktúry SNCA sú chránené proti nebezpečenstvu pôsobenia vody z akýchkoľvek zdrojov.

5.1.5 Ochrana pred ohňom

NASES využíva, na zabezpečenie ochrany priestorov, v ktorých je umiestnená infraštruktúra SNCA, dymové a požiarne detektory.

5.1.6 Úložisko médií

NASES uskladňuje všetky médiá SNCA, ako sú pásky a dokumenty, v bezpečnom prostredí.

Médiá sú uchovávané tak, aby boli bezpečne chránené pred možným poškodením (voda, oheň, elektromagnetické poškodenie). Médiá, obsahujúce záznamy pre audit, archívne alebo zálohované informácie, sú uchovávané v priestoroch, ktoré nie sú fyzicky spojené s prevádzkovými priestormi SNCA, v súlade s príslušnými internými smernicami agentúry a právnymi predpismi SR.

5.1.7 Nakladanie s odpadom

Nosiče informácií, obsahujúce citlivé informácie, sú likvidované v zmysle postupov, stanovených záväznými vnútornými predpismi agentúry NASES, kde je uvedená klasifikačná schéma citlivosti informácií.

S odpadom, vznikajúcim v súvislosti s prevádzkou SNCA, je nakladané spôsobom šetrným k životnému prostrediu, ktorý zároveň garantuje, že v žiadnom prípade nedochádza k znečisťovaniu životného prostredia.

5.1.8 Zálohovanie mimo hlavnú lokalitu

Okrem hlavných prevádzkových priestorov, disponuje NASES záložnými prevádzkovými priestormi, určenými na ukladanie pravidelných záložných kópií a archívnych dát.

5.2 Procedurálne bezpečnostné opatrenia

5.2.1 Dôveryhodné roly

Činnosti, vykonávané pracovníkmi, zodpovednými za správu a prevádzku SNCA, sú popísané formou definície prevádzkových postupov a procedúr. Prevádzkové postupy obsahujú definíciu nadväznosti jednotlivých procedúr, ktoré sú krokmi predmetného postupu. Prevádzkové procedúry sú špecifikáciou základných činností pri obsluhe komponentov SNCA a infraštruktúry CA. Špecifikácia prevádzkovej procedúry obsahuje popis činností pri obsluhe, pravidlá na bezpečnú realizáciu činností a identifikáciu roly pracovníka, ktorý môže dané činnosti vykonávať.

Spôsob a bezpečnosť vykonávania prevádzkových procedúr sú kontrolované interným auditom.

Na zabezpečenie činností, vykonávaných v prevádzke SNCA, boli pre jednotlivých pracovníkov prevádzky definované roly, ktoré definujú základ dôvery v celú hierarchiu PKI.

Definícia dôveryhodnej roly popisuje:

- rozsah činností, ktoré môže pracovník vykonávať,
- rozsah zodpovednosti pracovníka za vykonávané činnosti,
- počet osôb, potrebných na vykonávanie pridelených činností,
- pravidlá na obmedzenie fyzického prístupu do priestorov umiestnenia komponentov systému SNCA,
- spôsob autentifikácie pracovníka pri vykonávaní činností,
- požiadavky na znalosti a skúsenosti,
- zlučiteľnosť príslušnej roly s ďalšími rolami.

Pre prevádzku SNCA sú definované nasledujúce základné roly:

- bezpečnostný správca SNCA,
- interný audítor SNCA,
- manažér pre správu politík - PMA manažér SNCA,
- administrátor SNCA,
- systémový administrátor SNCA,
- operátor RA SNCA (registračný operátor),

Zamestnanci agentúry NASES, vybraní na zastávanie rolí, ktoré si vyžadujú dôveryhodnosť, sú zodpovední a dôveryhodní.

Každý zamestnanec, menovaný v dôveryhodných roliach, je bez konfliktu záujmov, čo garantuje nestrannosť služieb, poskytovaných agentúrou NASES.

5.2.2 Počet osôb v jednotlivých úlohách

Zabezpečené v zmysle organizačného poriadku agentúry. Pre každú úlohu je identifikovaný potrebný počet jednotlivcov, ktorí sú určení na vykonávanie jednotlivých úloh (pravidlo K z N).

5.2.3 Identifikácia a autentizácia pre každú rolu

Každá rola sa identifikuje a autentizuje bezpečným prostriedkom (čipová karta).

5.2.4 Roly vyžadujúce oddelenie zodpovedností

Zabezpečené v zmysle organizačného poriadku agentúry, pričom je zohľadnené a dodržané pravidlo, že každá rola má stanovené kritériá, ktoré zohľadňujú potrebu oddelenia funkcií z hľadiska samotnej roly.

5.3 Personálne bezpečnostné opatrenia

Každý pracovník prevádzky SNCA má vo svojej pracovnej náplni pridelenú prevádzkovú a bezpečnostnú rolu. Roly pracovníkov sú jednoznačne definované dokumentáciou SNCA. Každý pracovník je preukázateľne poučený o svojich povinnostiach, bezpečnostných a pracovných postupoch, požadovaných pri plnení úloh vyplývajúcich z jeho roly.

Pracovníci SNCA sú formálne menovaní do dôveryhodných rolí výkonným manažmentom agentúry NASES, zodpovedným za bezpečnosť.

Rotácia pracovníkov v jednotlivých rolách sa riadi vnútornými personálnymi opatreniami prevádzkovateľa SNCA.

5.3.1 Požiadavky na kvalifikáciu, skúsenosti a previerky

Pracovníci v dôveryhodných rolách musia spĺňať kvalifikačné požiadavky, požiadavky na odbornú prax a musia mať bezpečnostné previerky stanovenej úrovne, resp. musia byť v procese žiadania o bezpečnostnú previerku. Požiadavky na jednotlivé roly sú popísané v samostatných listoch, používaných pri výberových konaniach na nových pracovníkov.

Osoby v manažérskych funkciách musia:

- mať príslušné školenia alebo skúsenosti v oblasti dôveryhodných služieb, ktoré SNCA 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.

5.3.2 Požiadavky na previerky

Pracovníci, zabezpečujúci činnosti v prevádzke SNCA, sú preverovaní v zmysle vyhlášky Národného bezpečnostného úradu č. 134/2016 Z. z. o personálnej bezpečnosti.

Zamestnanec agentúry NASES môže byť zaradený do dôveryhodnej roly len v prípade, že má bezpečnostnú previerku stanovenej úrovne resp. je v procese žiadania o takýto typ previerky. Personálne bezpečnostné opatrenia sú zabezpečované internými mechanizmami agentúry NASES.

5.3.3 Požiadavky na školenia

Pracovníci, zabezpečujúci činnosti v prevádzke SNCA, sú pravidelne preškoľovaní z tém, špecifických pre prevádzku SNCA. Školenia sa uskutočňujú každých 6 mesiacov. Témy školení zahrňujú obsluhu technického a programového vybavenia informačného systému SNCA, prevádzkové predpisy SNCA a bezpečnostné predpisy SNCA. Rozsah školení pre jednotlivých pracovníkov je definovaný ich rolami.

5.3.4 Požiadavky na frekvenciu obnovy školení

Realizuje sa ako v bode 5.3.3, prípadne podľa potreby, na základe zmien v rámci prevádzkovaných IS a poskytovaných KDS.

5.3.5 Rotácia rolí

Neuplatňuje sa.

5.3.6 Postihy za neoprávnenú činnosť

Udeľovanie sankcií za neoprávnené činnosti s a riadi vnútorným poriadkom agentúry NASES a právnymi predpismi SR.

Akékoľvek neoprávnené alebo nevhodné konanie zamestnanca v dôveryhodnej role, označené manažmentom agentúry NASES, vedie k bezodkladnému odvolaniu tohto zamestnanca z dôveryhodnej roly až do doby ukončenia preskúmania takéhoto konania manažmentom agentúry NASES. Následne, po preskúmaní konania zamestnanca manažmentom agentúry NASES, po vzájomnej diskusii alebo preskúmaní výsledkov vyšetrovania so zamestnancom, môže byť tento zamestnanec podľa potreby znovu pridelený do dôveryhodnej roly, alebo prepustený zo zamestnania.

5.3.7 Požiadavky na externých dodávateľov

Externé organizácie, ktoré vystupujú ako zmluvní dodávatelia činností pre SNCA, musia spĺňať pravidlá, stanovené prevádzkovateľom SNCA, agentúrou NASES.

Externé organizácie a nezávislí dodávatelia, ktorí by mohli byť priradení na vykonávanie dôveryhodných rolí, podliehajú rovnakým povinnostiam a špecifickým požiadavkám na tieto roly, v zmysle ustanovení bodu 5.3 a rovnako podliehajú sankciám, uvedeným v bode 5.3.6.

5.3.8 Dokumentácia poskytovaná pracovníkom

Na definovanie povinností a procedúr pre každú rolu, je poskytnutá pracovníkom, vykonávajúcim túto rolu, dokumentácia v potrebnom rozsahu.

Pracovníci v dôveryhodných rolách, majú k dispozícii dokumenty, potrebné pre výkon funkcie, na ktorú sú priradení, vrátane kópie tejto CP resp. CPS a všetkých technických a prevádzkových dokumentov, potrebných k zachovaniu integrity operácií SNCA, vrátane dokumentácie interného systému a bezpečnostnej dokumentácie, politík a postupov overovania identity a dokumentov tretích strán resp. dokumentov, dostupných prostredníctvom internetu.

Pracovníci, zabezpečujúci činnosti v prevádzke SNCA, sú povinní používať dokumenty, ktoré im boli sprístupnené, len na účely, na ktoré sú tieto dokumenty určené. Každý pracovník je oboznámený s politikou ochrany osobných údajov a dát.

5.4 Postup získavania auditných záznamov

Na preukázanie činnosti SNCA, prevádzkovateľ SNCA vytvára a udržiava prevádzkové záznamy, ktoré zaznamenávajú požiadavky na činnosť SNCA, zachytávajú postupy vykonávania prevádzkových procedúr SNCA a uchovávajú záznamy o činnosti jednotlivých komponentov SNCA.

Prevádzkové záznamy a dokumenty sú uchovávané v papierovej alebo elektronickej forme, podľa toho v akej podobe vznikli.

Prevádzkové záznamy, vedené v elektronickej forme, musia byť zálohované tak, aby nedošlo k ich poškodeniu alebo strate.

Prevádzkové záznamy, vedené listinnou formou, musia byť spravované v režime ktorý zabezpečí, aby nemohlo dôjsť k ich poškodeniu alebo strate.

Prevádzkovateľ SNCA je povinný:

- zaznamenávať a mať k dispozícii počas nevyhnutnej doby, aj po ukončení činnosti, všetky dôležité informácie, týkajúce sa vydaných KC,
- zaznamenávať presný čas v systéme na poskytovanie dôveryhodných služieb. Minimálna perióda synchronizácie presného času s UTC je každých 24 hodín.

5.4.1 Typy zaznamenávaných udalostí

Počas prevádzky SNCA sú pravidelne zaznamenávané a vyhodnocované udalosti (záznamy), ktoré súvisia s procesmi a údajmi:

- životného cyklu kľúčov SNCA (generovanie, zálohovanie, obnova, likvidácia a pod.),
- prevádzky bezpečnostného HSM modulu,
- údajmi, získanými od Odberateľov/Držiteľov KC pri poskytovaní KDS,
- systémovými log-mi jednotlivých častí hardvérovej a softvérovej infraštruktúry SNCA.

5.4.2 Frekvencia spracovávania auditných záznamov

Prevádzkové záznamy sa spracovávajú v pravidelných denných, týždenných, mesačných a ročných intervaloch. Na vyhodnocovanie prevádzkových záznamov SNCA je vypracovaný systém pravidelného ako aj náhodného auditu v súlade s internými smernicami SNCA.

Administrátori SNCA sú povinní sledovať zasielané systémové logy priebežne tak, aby včas odhalili akékoľvek potenciálne nebezpečenstvo ohrozenia poskytovania kvalifikovaných dôveryhodných služieb. Všetky logy, zaznamenávané v elektronickej podobe, sú ukladané na záznamové médiá v pravidelných intervaloch, minimálne 1 krát mesačne, aby ich bolo možné predložiť audítorom pri realizácii auditu prevádzky SNCA. Rovnako, musia byť audítorom k dispozícii všetky písomné auditné záznamy z procesov, týkajúcich sa životného cyklu kľúčov certifikačných autorít SNCA a autorít časovej pečiatky TSA a OCSP reponderov.

5.4.3 Uchovávanie logov

Prevádzkové záznamy - auditné logy sú uchovávané v súlade s požiadavkami aktuálne platnej legislatívy. Všetky auditné logy sú zároveň uchovávané minimálne do času ukončenia nasledovného pravidelného externého auditu služieb SNCA.

5.4.4 Ochrana auditných záznamov

Auditné záznamy, vedené v elektronickej forme, sú zálohované tak, aby nemohlo dôjsť k ich poškodeniu alebo k ich strate. Integrita prevádzkových auditných záznamov, je zabezpečená prostredníctvom elektronického podpisu záznamov s použitím kľúča a certifikátu, ktoré boli generované výhradne pre tento účel. Súkromný kľúč, používaný pre podpisovanie auditných záznamov, nie je prístupný pre pracovníkov, ktorí majú oprávnenie prehliadať auditné záznamy.

Prevádzkové auditné záznamy sú zálohované vo viacerých kópiách, umiestnených v rozdielnych prevádzkových priestoroch agentúry NASES.

5.4.5 Postupy zálohovania auditných logov

Prevádzkovateľ SNCA, zabezpečuje zálohovanie prevádzkových záznamov - auditných logov v súlade s internou smernicou a platnými právnymi predpismi SR.

5.4.6 Systém zálohovania logov

Systém zberu elektronických prevádzkových záznamov je procesne zabezpečený kombináciou automatických činností, vykonávaných operačnými systémami a aplikáciami komponentov SNCA a manuálnych činností, vykonávaných pracovníkmi prevádzky.

Proces zberu elektronických prevádzkových záznamov je aktivovaný pri štarte systémov SNCA a uzavrie sa len pri vypnutí celého informačného systému SNCA.

V prípade prerušenia činnosti automatizovaného systému zberu prevádzkových záznamov, budú vykonané príslušné kroky na obnovu jeho činnosti, alebo budú využité náhradné možnosti, ktoré boli vopred odsúhlasené ako náhradné riešenie.

5.4.7 Notifikácia subjektu iniciujúceho log záznam

Neuplatňuje sa.

5.4.8 Posudzovanie zraniteľností

Platia ustanovenia podľa bodu 5.4.2 tohto dokumentu.

5.5 Uchovávanie záznamov

Na preukázanie činnosti SNCA, prevádzkovateľ SNCA vytvára a udržiava prevádzkové záznamy, ktoré zaznamenávajú požiadavky na činnosť SNCA, zachytávajú postupy vykonávania

prevádzkových procedúr SNCA a uchovávajú záznamy o činnosti jednotlivých komponentov SNCA.

Prevádzkové záznamy a dokumenty sú uchovávané v papierovej alebo elektronickej forme, podľa toho, v akej podobe vznikli.

Prevádzkové záznamy, vedené v elektronickej forme, musia byť zálohované tak, aby nemohlo dôjsť k ich poškodeniu alebo strate.

Prevádzkové záznamy, vedené listinnou formou, musia byť spravované v režime ktorý zabezpečí, aby nemohlo dôjsť k ich poškodeniu alebo strate.

5.5.1 Typy archivovaných záznamov

Archívne záznamy SNCA sú uchovávané v rozsahu, dostatočnom na zaručenie platnosti podpisu a správnej funkčnosti infraštruktúry správy a manažmentu certifikátov. Prevádzkovateľ SNCA musí zabezpečiť archiváciu informácií z prevádzky SNCA minimálne v nasledovnom rozsahu:

- Prevádzkové záznamy - auditné záznamy (logy), písomné záznamy z udalostí CA (generovanie kľúčov CA, vyhotovovanie TSA certifikátov a certifikátov pre OCSP respondery a pod.);
- Certifikáty, vydané SNCA;
- Zoznamy zrušených certifikátov;
- Oficiálna korešpondencia;
- Dokumentácia programového vybavenia SNCA;
- Bezpečnostná dokumentácia SNCA;
- Inštalačné média a popisy konfiguračných súborov programového vybavenia SNCA.

Všetky záznamy o vydaných KC ako aj samotné KC sú uchovávané v zmysle požiadaviek aktuálne platnej legislatívy po dobu, ktorá je stanovená v bode 5.5.2.

V prípade, že sú záznamy o vydaných KC uchovávané v papierovej forme, neoddeliteľnou súčasťou uchovávaných záznamov sú aj všetky dokumenty, ktoré musí Odberateľ/Držiteľ KC predložiť k tomu, aby mu bol vydaný požadovaný typ certifikátu (napr. výpis z obchodného registra, plná moc, potvrdenie o vlastníctve domény a pod.).

Každý archívny záznam je opatrený časovým údajom jeho vytvorenia.

5.5.2 Doba uchovávania záznamov

Doba uchovávania archivovaných údajov, mimo archívu vydaných kvalifikovaných certifikátov a archívu zoznamov zrušených kvalifikovaných certifikátov, je 10 rokov (v zmysle § 5 zákona o dôveryhodných službách).

Archív vydaných kvalifikovaných certifikátov a archív zoznamov zrušených kvalifikovaných certifikátov, vydaných SNCA, je uchovávaný agentúrou na dobu neurčitú.

5.5.3 Ochrana archívnych záznamov

Archívne záznamy sú chránené kombináciou fyzickej bezpečnosti, kryptografickej ochrany a režimových opatrení, zabraňujúcich ich neoprávnenej modifikácii, nahradeniu alebo zničeniu. Archivačné médiá sú chránené pred vplyvmi prostredia ako je teplota, vlhkosť a magnetizmus.

5.5.4 Zálohovanie archívnych záznamov

Procedúry zálohovania archívu sú navrhnuté tak, aby zaisťovali kompletné obnovenie služieb. Podrobnosti sú špecifikované v bezpečnostných a prevádzkových smerniciach SNCA.

5.5.5 Požiadavky na pridávanie časových pečiatok k záznamom

Neuplatňuje sa.

5.5.6 Archivačný systém

Neuplatňuje sa.

5.5.7 Postup získania a overenia archívnych informácií

Neuplatňuje sa.

5.6 Zmena kľúčov CA

K zmene kľúčov certifikačnej autority SNCA môže dôjsť z nasledovných dôvodov:

- Ukončenie doby platnosti (exspirácia) aktuálne používaných kľúčov SNCA.

  Jedná sa o normálny stav prevádzky SNCA, kedy dochádza k uplynutiu doby platnosti aktuálne používaných kľúčov SNCA.

  Prevádzkovateľ SNCA je v tomto prípade povinný:

  - minimálne 30 dní pred uplynutím doby platnosti doteraz používaného páru kľúčov SNCA, zverejniť na webovom sídle SNCA oznam o blížiacej sa zmene kľúčov SNCA,
  - vygenerovať nový kľúčový pár,
  - vyhotoviť nový certifikát pre SNCA, ktorý musí zverejniť na webovom sídle SNCA.

- Kompromitácia aktuálne používaných kľúčov SNCA počas doby ich platnosti.

  Jedná sa o havarijný stav prevádzky SNCA, kedy je potrebné vymeniť aktuálne používané kľúče SNCA z dôvodu ich kompromitácie.

  Prevádzkovateľ SNCA je v tomto prípade povinný bezodkladne:

  - informovať o vzniknutej situácii orgán dohľadu, všetkých držiteľov vydaných kvalifikovaných certifikátov a verejnosť,

- zrušiť kompromitovaný certifikát, ako aj všetky platné kvalifikované certifikáty, podpísané kompromitovaným kľúčom SNCA,
- upozorniť, prostredníctvom svojho webového sídla, držiteľov kvalifikovaných certifikátov, ktoré boli podpísané zrušeným certifikátom, ako aj spoliehajúce sa strany, že zrušený certifikát SNCA je potrebné odstrániť z každej aplikácie, ktorú používajú spoliehajúce sa strany. Oznámenie dotknutých strán zabezpečí SNCA vhodným spôsobom tak, aby uvedená informácia bola doručená v čo najkratšom čase (e-mailom, telefonicky).

- Zmena kľúčov koreňovej certifikačnej autority, ktorá vydala certifikát certifikačnej autorite SNCA.

Celý proces musí prebehnúť bez negatívneho vplyvu na úroveň zabezpečenia prevádzky SNCA.

5.7 Obnova po kompromitácii alebo havárii

5.7.1 Postupy riešenia incidentov a kompromitácie

Pre zabezpečenie integrity dôveryhodných služieb, poskytovaných SNCA, agentúra NASES:

- má vypracované havarijné postupy a plány obnovy pre poskytovanie dôveryhodných služieb,
- implementuje odporučené a štandardizované procesy a postupy, ktoré sú zamerané na zálohovanie údajov a zabezpečenie ich úspešnej obnovy po incidente.

Postupy, aplikované v prípade havárie a obnovy, sú pravidelne preskúmavané, testované (minimálne na ročnej báze), revidované a aktualizované v rozsahu a spôsobom, uvedeným v bezpečnostných a prevádzkových smerniciach SNCA.

Z dôvodu zabezpečenia integrity a maximálnej dostupnosť KDS pre Odberateľov, agentúra NASES prevádzkuje infraštruktúru SNCA v rámci dvoch, geograficky oddelených systémov certifikačných autorít CA, z ktorých je jeden systém vedený ako hlavný a druhý ako záložný systém, ktorý zabezpečí integritu a dostupnosť poskytovaných KDS v prípade zlyhania alebo havárie hlavného systému.

5.7.2 Poškodenie hardvéru, softvéru alebo údajov

Platia rovnaké ustanovenia, ako v bode 5.7.1 tohto dokumentu, s dôrazom na prevádzkové postupy SNCA, určené na obnovu poškodených aktív, umožňujúcich kompletnú obnovu prostredia SNCA.

5.7.3 Postupy pri kompromitácii kľúča SNCA

V prípade kompromitácie súkromného kľúča SNCA platia rovnaké ustanovenia, ako v bode 5.7.1 tohto dokumentu, s dôrazom na prevádzkové postupy SNCA, určené na obnovu

bezpečného prostredia SNCA, postup distribúcie verejného kľúča koncovým používateľom a obnovu a stanovenie procedúr, súvisiacich s procesom vyhotovovania nových KC jednotlivým koncovým používateľom.

5.7.4 Zachovanie kontinuity činnosti po havárii

V prípade havárie v dôsledku napr. prírodnej katastrofy, platia rovnaké ustanovenia, ako v bode 5.7.1 tohto dokumentu s dôrazom na prevádzkové postupy SNCA, zamerané na zabezpečenie obnovy a kontinuity činnosti v prípade havárie s ohľadom na miesto havárie a obnovy, postupy na ochranu aktív v mieste havárie resp. prírodnej katastrofy a pod.

5.8 Ukončenie činnosti CA resp. RA

Pri ukončení činnosti SNCA z iných dôvodov, ako sú udalosti spôsobené vyššou mocou (napr. prírodná katastrofa, vojnový stav, rozhodnutie štátnej moci a pod.), postupuje prevádzkovateľ SNCA v súlade s bodom 5.7 tohto dokumentu.

Pred ukončením poskytovania služieb SNCA, prevádzkovateľ SNCA zabezpečí vhodným spôsobom nasledovné činnosti:

- oznámi plánované ukončenie činnosti SNCA orgánu dohľadu, držiteľom všetkých vydaných platných KC, stranám spoliehajúcim sa na KC a verejnosti minimálne 6 mesiacov vopred,
- pokúsi sa uzavrieť zmluvu (ak je to možné) s iným poskytovateľom kvalifikovaných dôveryhodných služieb, ktorý by zabezpečil kontinuitu v poskytovaní jeho kvalifikovaných dôveryhodných služieb,
- pred ukončením činnosti zruší všetky platné KC, ak nezabezpečí kontinuitu v poskytovaní jeho služieb,
- sústredí a archivuje všetky dokumenty SNCA,
- vykoná kontroly dodržania zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov,
- vyradí z používania všetky súkromné kľúče, vrátane ich kópií takým spôsobom, že nebude možné vyradené súkromné kľúče žiadnym spôsobom obnoviť.

Po ukončení činnosti SNCA, agentúra NASES, ako prevádzkovateľ SNCA zabezpečí:

- znemožnenie vydávania kvalifikovaných certifikátov certifikačnou autoritou SNCA,
- preukázateľné znemožnenie opätovného použitia podpisových dát (súkromných kľúčov) SNCA.

Prevádzkovateľ SNCA musí disponovať dostatočnými finančnými prostriedkami, potrebnými na pokrytie všetkých nákladov, spojených so splnením minimálnych požiadaviek pri ukončení činnosti v prípade, kedy SNCA nebude schopná pokryť náklady vlastnými prostriedkami, a to v súlade s platnou legislatívou.

6 Technické bezpečnostné opatrenia

Technické bezpečnostné opatrenia, predstavujú opatrenia na ochranu kryptografických kľúčov a aktivačných údajov, počítačové bezpečnostné opatrenia (riadenie prístupu, audit, testovanie), bezpečnostné opatrenia na vývoj a riadenie bezpečnosti, sieťové bezpečnostné opatrenia a opatrenia pre kryptografické moduly.

Technická časť infraštruktúry SNCA (hardvér a softvér), pozostáva z bezpečných systémov a oficiálneho softvéru. Architektúra infraštruktúry SNCA je navrhnutá s použitím komponentov, ktoré vyhovujú bezpečnostným štandardom na úrovni súčasných poznatkov. Agentúra NASES používa na ochranu súkromného kľúča SNCA kombináciu fyzických, logických a procedurálnych opatrení, zaručujúcich jeho bezpečnosť.

Použitý kryptografický bezpečnostný modul (HSM modul), ktorý slúži na generovanie, úschovu a použitie súkromných kľúčov SNCA, a ktorý patrí k najcitlivejším aktívam agentúry NASES ako prevádzkovateľa SNCA a poskytovateľa KDS, je certifikovaný minimálne podľa štandardu FIPS 140-2, level 3.

V infraštruktúre SNCA sú implementované technologické zariadenia, zabezpečujúce nepretržitú detekciu, monitorovanie a signalizáciu neautorizovaných a neobvyklých pokusov o prieniky a prístup k jej prostriedkom.

Všetky aplikácie, súvisiace s informovaním o aktuálnom stave kvalifikovaného certifikátu v procese jeho vyhotovovania, sú zabezpečené proti akýmkoľvek neoprávneným pokusom o modifikovanie týchto informácií.

Komunikačná, LAN infraštruktúra SNCA a každá funkcionalita systému SNCA, pri ktorej je využívaná LAN infraštruktúra - počítačová sieť prevádzkovateľa SNCA, agentúry NASES, sú zabezpečené pred neautorizovaným prístupom a inými škodlivými činnosťami.

6.1 Generovanie a inštalácia páru kľúčov

Procedúra generovania a inštalácie kľúčového páru, je písomne zdokumentovaná. Jednotlivé činnosti uvedeného procesu zabezpečujú pracovníci, ustanovení v dôveryhodných rolách SNCA.

6.1.1 Generovanie a inštalácia páru kľúčov pre jednotlivé subjekty

6.1.1.1 Vydavateľ certifikátov

Generovanie a inštalácia kľúčového páru, priradeného k certifikátu SNCA, je vykonávaná štandardizovaným spôsobom, ktorý je podrobne popísaný v dokumentácii SNCA. Spôsob generovania zabezpečuje dostatočnú dôveru v postup generovania a celý proces je písomne

zaznamenaný. Generovanie kľúčov zabezpečujú pracovníci, ustanovení v dôveryhodných rolách SNCA, ktoré majú oprávnenie na účasť na uvedenom procese.

Súkromné kľúče, priradené k certifikátu SNCA, sú uložené v HSM module, ktorý je certifikovaný minimálne podľa štandardu FIPS 140-2 level 3.

6.1.1.2 Registračné autority

Generovanie kľúčových párov certifikátov pre registračné autority RA SNCA, je vykonávané pod kontrolou poverených pracovníkov agentúry NASES, pričom je vygenerovaný kľúčový pár uložený na bezpečnom QSCD zariadení.

6.1.1.3 Koncoví používatelia

Pre procedúry koncových používateľov Poskytovateľa platia rovnaké ustanovenia, ako v bode 4.1.3 tohto dokumentu a v bode 4.1.2 dokumentu „Pravidlá na výkon certifikačných činností (CPS) SNCA“ [12].

6.1.2 Doručenie súkromného kľúča Držiteľovi certifikátu

Vygenerovaný kľúčový pár, obsahujúci súkromný kľúč registračnej autority RA SNCA, je bezpečným spôsobom doručený príslušnému pracovníkovi RA SNCA.

Vygenerovaný kľúčový pár koncového Držiteľa KC, ktorý je uložený v bezpečnom zariadení pre elektronický podpis, je odovzdaný Držiteľovi KC osobne, ihneď po vyhotovení kvalifikovaného certifikátu na príslušnej registračnej autorite RA SNCA.

Pri vyhotovovaní KC pre elektronickú pečať, kde bol kľúčový pár generovaný v kvalifikovanom zariadení pre elektronickú pečať pod kontrolou Odberateľa, resp. kvalifikovaného dôveryhodného poskytovateľa služieb (napr. HSM modul), je koncovému používateľovi doručený iba vydaný kvalifikovaný certifikát.

Pri vyhotovovaní KC pre autentifikáciu webového sídla, je koncovému používateľovi doručený iba vydaný kvalifikovaný certifikát pre autentifikáciu webového sídla.

6.1.3 Doručenie verejného kľúča vydavateľovi certifikátu

Pokiaľ bol kľúčový pár, na ktorý je vydávaný KC, generovaný pod kontrolou Odberateľa, resp. iného kvalifikovaného poskytovateľa dôveryhodných služieb, musí byť verejný kľúč doručený certifikačnej autorite bezpečným spôsobom.

6.1.4 Poskytovanie verejných kľúčov SNCA Spoliehajúcim sa stranám

Pre Spoliehajúce sa strany musí SNCA bezpečným spôsobom poskytnúť verejné kľúče všetkých vydávajúcich certifikačných autorít CA SNCA, ktoré vyhotovujú KC.

6.1.5 Dĺžka kľúčového páru

Dĺžka kľúča pre KC, vyhotovovaný pre CA SNCA – RSA 4096 bit.

Dĺžka kľúča pre KC, vyhotovovaný pre koncových požívateľov – RSA minimálne 2048 bit.

6.1.6 Parametre a kvalita verejného kľúča

Kľúčový pár pre KC - verejný kľúč a k nemu prislúchajúci súkromný kľúč, sú generované spoločne. Parametre a kvalitu verejných kľúčov pre CA SNCA, definuje zodpovedná osoba SNCA, zaradená do dôveryhodnej role PMA. Počas procesu generovania kľúčového páru, musia byť dodržiavané všetky parametre kľúčového páru, stanovené PMA. SNCA využíva na generovanie a uchovávanie kľúčov pre vydávajúce certifikačné autority CA SNCA kryptografické hardvérové moduly, spĺňajúce požiadavky FIPS 140-2 Level 3, ktoré zabezpečujú náhodné generovanie RSA kľúčov veľkosti minimálne 4096 bitov.

Pre jednotlivé typy KC, vyhotovované pre koncových používateľov, má SNCA stanovené parametre a kvalitu verejného kľúča (dĺžka, typ) a pred samotným vydaním KC kontroluje ich dodržanie.

Pre proces generovania kľúčového páru platia rovnaké ustanovenia, ako v bode 6.1.5 dokumentu „Pravidlá na výkon certifikačných činností (CPS) SNCA“ [12].

6.1.7 Použitie kľúčov

Certifikáty certifikačných autorít CA SNCA obsahujú rozšírenia, ktoré určujú, k čomu môžu byť tieto certifikáty použité.

6.2 Ochrana súkromného kľúča a technické opatrenia pre kryptografický modul

6.2.1 Štandardy a opatrenia pre kryptografický modul

Súkromné kľúče všetkých vydávajúcich certifikačných autorít CA SNCA, sú chránené a uložené oddelene, v špeciálnom hardvérovom zariadení - kryptografickom bezpečnostnom module (HSM modul). Kryptografické bezpečnostné moduly, použité v infraštruktúre SNCA, sú odolné voči nedovolenej manipulácii a chránené pred neautorizovaným prístupom (aj fyzickým). Všetky použité HSM moduly sú certifikované podľa medzinárodného štandardu FIPS 140-2 na úroveň (level) 3. HSM moduly sú uložené v zabezpečených priestoroch, do ktorých majú prístup iba osoby, zaradené do dôveryhodných rolí SNCA. Infraštruktúra certifikačnej autority CA SNCA je nepretržite monitorovaná a chránená pred neautorizovanými prístupmi, realizovanými prostredníctvom komunikačnej infraštruktúry SNCA ako aj pred neautorizovaným fyzickým prístupom nepovolanou osobou. Bezpečnosť kryptografických bezpečnostných modulov je pravidelne monitorovaná a testovaná.

Súkromné kľúče vydávajúcich certifikačných autorít CA SNCA sú používané výlučne na podpisovanie kvalifikovaných certifikátov a CRL, vyhotovovaných SNCA.

6.2.2 Opatrenia (K z N) pre manipuláciu so súkromným kľúčom

Na vykonanie kritických činností na kryptografickom bezpečnostnom module (napr. záloha súkromného kľúča certifikačnej autority CA SNCA), je potrebná a nevyhnutná, súčasná autorizácia dvoch určených pracovníkov agentúry NASES, zaradených v dôveryhodných rolách SNCA.

Za účelom zálohovania (podľa bodu 6.2.4 tohto dokumentu), je súkromný kľúč certifikačnej autority CA SNCA exportovaný výhradne v zašifrovanej forme. Neexistuje žiadna možnosť, ako získať súkromný kľúč certifikačnej autority CA SNCA inými metódami (napr. Key escrow).

6.2.3 „Key escrow“ súkromného kľúča

Neuplatňuje sa.

6.2.4 Zálohovanie súkromného kľúča

Súkromné kľúče všetkých vydávajúcich certifikačných autorít CA SNCA, sú:

- generované a uchovávané vo vnútri hardvérových kryptografických bezpečnostných modulov,
- zálohované výhradne v zašifrovanej forme.

V prípade potreby ich prenosu pre proces zálohovania a obnovy, sú súkromné kľúče všetkých vydávajúcich certifikačných autorít CA SNCA prenášané výhradne a vždy v zašifrovanej podobe. Prenášanie súkromných kľúčov a ich obnova v inom hardvérovom kryptografickom module, je vykonaná iba pracovníkmi agentúry NASES, zaradenými v dôveryhodných rolách SNCA a v zmysle pravidiel uvedených v bode 6.2.2.

Po ukončení platnosti certifikátu vydávajúcej certifikačnej autority CA SNCA, ktorý je zviazaný s verejným kľúčom, prislúchajúcim k zálohovanému súkromnému kľúču, bude záloha súkromného kľúča zničená.

6.2.5 Archivácia súkromného kľúča

Neuplatňuje sa.

6.2.6 Prenos súkromných kľúčov z a do HSM modulu

Platia ustanovenia podľa bodu 6.2.4 tohto dokumentu.

6.2.7 Uchovávanie súkromných kľúčov v HSM module

Súkromný kľúč vydávajúcej certifikačnej autority CA SNCA, je generovaný priamo prostriedkami kryptografického modulu. Na vygenerovanie súkromného kľúča vydávajúcej certifikačnej autority CA SNCA, je potrebná súčasná autorizácia dvoch pracovníkov agentúry NASES, zaradených v dôveryhodných rolách SNCA.

Súkromné kľúče vydávajúcej certifikačnej autority CA SNCA, ktoré sú využívané pri vyhotovovaní vydaných KC pre koncových používateľov, môžu byť v samotnom HSM module uchovávané v čitateľnej forme. Funkčné, technické a bezpečnostné vlastnosti kryptografického modulu, na ktorom je uložený súkromný kľúč vydávajúcej certifikačnej autority CA SNCA, spĺňajú požiadavky nariadenia eIDAS a zákona č. 272/2016 Z. z. o dôveryhodných službách. Všetky HSM moduly infraštruktúry SNCA sú prevádzkované v zabezpečených priestoroch s režimovým prístupom.

6.2.8 Spôsob aktivácie súkromných kľúčov

Aktiváciu súkromného kľúča vydávajúcej certifikačnej autority CA SNCA, je možné zrealizovať iba v prítomnosti oprávnených osôb v zmysle bodu 6.2.2 tohto dokumentu. Pri aktivácii, musí každá oprávnená osoba z potrebného počtu oprávnených osôb, vložiť do HSM modulu svoju prístupovú čipovú kartu a následne zadať k svojej prístupovej čipovej karte heslo.

Po aktivácii, sú súkromné kľúče, uložené v HSM module aktívne až do doby, kým nedôjde k ich deaktivácii oprávnenou osobou, ktorou je administrátor SNCA, alebo výpadkom elektrického napájania HSM modulu.

Za ochranu súkromných kľúčov Držiteľov KC, ktorým bol SNCA vyhotovený a vydaný KC na príslušný verejný kľúč, sú výhradne zodpovední Držitelia KC.

6.2.9 Spôsob deaktivácie súkromného kľúča

Deaktiváciu súkromného kľúča v HSM module, môže vykonať len oprávnená osoba, ktorou je administrátor SNCA. K automatickej deaktivácii súkromného kľúča v HSM module dochádza pri výpadku relácie alebo pri výpadku elektrickej energie, ktorá napájania HSM modulu.

6.2.10 Spôsob zničenia súkromného kľúča

NASES, ako prevádzkovateľ SNCA a poskytovateľ KDS, prijatými technickými a organizačnými opatreniami zaručuje a zabezpečuje, že súkromné kľúče vydávajúcich certifikačných autorít CA SNCA, nie je možné po ukončení ich životného cyklu ďalej používať. O ukončení životného cyklu súkromného kľúča vydávajúcej certifikačnej autority CA SNCA a prijatých technických a organizačných opatreniach, je vyhotovený písomný záznam, podpísaný všetkými prítomnými, zodpovednými osobami.

6.2.11 Charakteristika HSM modulu

Platia ustanovenia podľa bodu 6.2.1 tohto dokumentu.

6.3 Ďalšie aspekty manažmentu páru kľúčov

6.3.1 Archivácia verejných kľúčov

NASES, ako prevádzkovateľ SNCA a poskytovateľ KDS, je povinný uchovávať, v zmysle bodu 5.5.2 tohto dokumentu, všetky verejné kľúče, na ktoré bol vydávajúcimi certifikačnými autoritami CA SNCA vydaný kvalifikovaný certifikát.

6.3.2 Dĺžka platnosti certifikátov a použiteľnosť kľúčového páru

Platnosť kvalifikovaných certifikátov SNCA, vyhotovovaných vydávajúcimi certifikačnými autoritami CA SNCA a použiteľnosť k nim prislúchajúcich šifrovacích kľúčových párov, generovaných registračnými autoritami RA SNCA, nesmie prekročiť hodnoty, uvedené v nasledujúcej tabuľke.

Tabuľka č. 1 Platnosť vyhotovovaných kvalifikovaných certifikátov SNCA

Typ certifikátu	Platnosť (maximálne)
KC pre koncového používateľa	3 roky
Certifikát pre TSA	5 rokov

6.4 Aktivačné údaje

6.4.1 Vytváranie a inštalácia aktivačných údajov

Aktivačné údaje Držiteľov KC (PIN a PUK), ktoré sa viažu ku konkrétnemu kvalifikovanému zariadeniu pre elektronický podpis resp. elektronickú pečať, sú odovzdané Držiteľovi KC pri osobnom stretnutí počas vyhotovovania KC. Držiteľ bude poučený o potrebe a spôsobe ich zmeny a o rizikách, pokiaľ uvedené zmeny nevykoná. Aktivačné údaje môžu byť v podobe PIN, hesla alebo hesla, rozdeleného na viacero častí na princípe K/N a pod..

Aktivačné údaje k používaným kryptografickým modulom vydávajúcich certifikačných autorít CA SNCA, sú vytvárané v zmysle ustanovení bodu 6.2.2 tohto dokumentu.

6.4.2 Ochrana aktivačných údajov

Za ochranu súkromných kľúčov Držiteľov KC sú zodpovední výhradne samotní Držitelia.

Pri vyhotovovaní KC je každý Držiteľ KC informovaný a upozornený registračným operátorom RA SNCA o potrebe chrániť vygenerovaný súkromný kľúč silným heslom, počas celej doby jeho používania, s cieľom zabrániť zneužitiu, resp. kompromitácii súkromného kľúča.

Kľúčový pár, určený pre vydávajúce certifikačné autority CA SNCA:

- bude generovaný v bezpečnostnom kryptografickom module, spĺňajúcom minimálne požiadavky štandardu FIPS 140-2 level 3,
- akákoľvek manipulácia so súkromným kľúčom bude umožnená iba za princípu viacnásobnej kontroly, pričom minimálny počet potrebných oprávnených osôb musí byť tri (3).

6.4.3 Ostatné aspekty aktivačných údajov

NASES, ako prevádzkovateľ SNCA a poskytovateľ KDS, je povinný zabezpečiť, nasledovné:

- súkromné kľúče vydávajúcich certifikačných autorít CA SNCA sa v nezašifrovanej forme nikdy nedostanú mimo HSM modul, v ktorom boli vygenerované a zostávajú uložené,
- prístup k súkromnému podpisovému kľúču má iba jeho Držiteľ, pričom žiadnej inej osobe tento prístup nie je umožnený,
- aktivačné dáta pre súkromné kľúče, patriace ku kvalifikovaným certifikátom, potvrdzujúcim individuálnu identitu Držiteľa KC, nie sú nikdy zdieľané,
- aktivačné dáta pre súkromné kľúče, patriace ku kvalifikovaným certifikátom, potvrdzujúcim identitu organizácie, sú známe iba osobám, ktoré sú v organizácii autorizované na použitie daných súkromných kľúčov.

6.5 Riadenie bezpečnosti počítačov

6.5.1 Špecifické požiadavky na bezpečnosť počítačov

Všetky počítačové komponenty, inštalované a implementované v rámci infraštruktúry SNCA, spĺňajú požiadavky na spoľahlivé a bezpečné prevádzkovanie dôveryhodných služieb.

NASES, ako prevádzkovateľ SNCA:

- vykonáva a poskytuje všetky funkcie kvalifikovaného poskytovateľa dôveryhodných služieb prostredníctvom dôveryhodného informačného a komunikačného systému, ktorý spĺňa požiadavky, definované v bezpečnostnom projekte IS SNCA.

- vykonáva a poskytuje všetky funkcie kvalifikovaného poskytovateľa dôveryhodných služieb v súlade s požiadavkami na bezpečnosť informácií, definovanými v štandarde ETSI EN 319411-2 " Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates.

Všetky počítačové komponenty a systémy infraštruktúry SNCA sú:

- pravidelne testované a preverované na prítomnosť škodlivého kódu,
- bezpečne chránené proti spyware a vírusom.

6.5.2 Hodnotenie bezpečnosti informácií

Neuplatňuje sa.

6.6 Opatrenia v životnom cykle

6.6.1 Opatrenia pri vývoji systémov

Na zabezpečovanie kvalifikovaných dôveryhodných služieb, používa agentúra NASES, ako prevádzkovateľ SNCA produkty na elektronický podpis s medzinárodne uznávanou certifikáciou ISO/IEC 15408 a NIST a špecializované programové vybavenie, ktoré bolo navrhnuté a vyvinuté v zmysle formálnej metodiky a je podporované nástrojmi pre riadenie konfigurácie.

Pri vývoji špecializovaného programového vybavenia, agentúra NASES:

- zohľadňuje zverejnené, aktuálne platné medzinárodné štandardy, zamerané na:
  - bezpečnosť vývojového prostredia,
  - personálnu bezpečnosť,
  - bezpečnosť riadenia konfigurácií pri údržbe systémov, v rámci technických postupov vývoja softvéru, metodológie vývoja softvéru a modularite a vrstvení softvéru,
- uplatňuje ustanovenia interných bezpečnostných smerníc, ktoré predpisujú zásady bezpečnosti vývoja programového vybavenia a riadenie bezpečnosti pri poskytovaní kvalifikovaných dôveryhodných služieb.

6.6.2 Opatrenia na riadenie bezpečnosti

NASES, ako poskytovateľ KDS, využíva pri prevádzke SNCA efektívne nástroje a postupy, umožňujúce identifikovať a v reálnom čase posúdiť a vyhodnotiť aktuálny stav a nastavenú úroveň zabezpečenia prevádzkovanej infraštruktúry, s dôrazom na operačné systémy, inštalované v rámci certifikačnej autority CA SNCA a sieťovú, komunikačnú infraštruktúru SNCA.

Použité nástroje a postupy, sú primárne zamerané na kontrolu:

- integrity bezpečnostného softvéru,
- aktuálnosti firmvéru prevádzkovaných hardvérových prostriedkov.

6.6.3 Bezpečnostné opatrenia v životnom cykle

Neuplatňuje sa.

6.7 Sieťové bezpečnostné opatrenia

Počítačové systémy SNCA, zabezpečujúce funkcie vydávania kvalifikovaných certifikátov a zoznamov zrušených certifikátov, sú oddelené od ďalších komponentov certifikačnej autority CA SNCA a nie sú priamo dostupné z verejnej siete Internet.

Prístup k systémom SNCA, ktoré sú dostupné z verejnej siete Internet, je zabezpečený a chránený prostredníctvom výkonných firewallov. Prevádzka týchto systémov je riadená a podlieha prijatým opatreniam na zabezpečenie sieťovej bezpečnosti, vrátane bezpečnosti firewalov.

6.8 Využívanie časovej pečiatky

Neuplatňuje sa.

7 Profily KC, CRL a OCSP

Všetky kvalifikované certifikáty sú vydávané v súlade s nariadením eIDAS, zákonom o dôveryhodných službách a normou X.509.

Formáty kvalifikovaných certifikátov sú definované v štandarde NBÚ „Formáty certifikátov a kvalifikovaných certifikátov“ verzia 4.0, ktorý vydala sekcia kybernetickej bezpečnosti Národného bezpečnostného úradu, Budatínska 30, 851 06 Bratislava.

Profily KC, profily zoznamov zrušených certifikátov (CRL) a odpoveď vo forme informácie o platnosti certifikátu, ktorá je poskytovaná prostredníctvom OCSP protokolu, musia byť stanovené centrálne, zodpovednou osobou SNCA, zaradenou do dôveryhodnej role PMA a ani osoby, zastávajúce služobné úrovne (roly), nemôžu svojvoľne meniť štruktúru týchto profilov resp. odpovedí.

Podľa čl. 28 ods. 3 a čl. 38 ods. 3 Nariadenia eIDAS, kvalifikované certifikáty pre elektronické podpisy (pečate), môžu obsahovať nepovinné dodatočné osobitné atribúty. Týmito atribútmi sa neovplyvní interoperabilita a uznávanie kvalifikovaných elektronických podpisov (pečatí). Rovnako, certifikát pre autentifikáciu webových sídiel, môže obsahovať nepovinné dodatočné osobitné atribúty, pokiaľ sa týmito atribútmi neovplyvní interoperabilita a uznávanie týchto kvalifikovaných certifikátov.

Štruktúra KC, vyhotovovaných SNCA, môže byť zmenená len na základe rozhodnutia osoby, zaradenej do dôveryhodnej role PMA.

7.1 Profil KC

7.1.1 Verzia

Táto CP povoľuje len profily KC, vyhovujúce štandardu X.509 verzie 3.

Profil kvalifikovaného certifikátu je uvedený v kapitole 10.2 CP KCA (OID 1.3.158.36061701.0.0.0.1.2.2) v odseku "Kapitola 6.6.1 ETSI EN 319 411-2 V2.1.1 (Certificate Profile)".

7.1.2 Obmedzenia týkajúce sa mien

Neuplatňuje sa.

7.1.3 Identifikátor certifikačnej politiky

Platia ustanovenia podľa bodu 1.2 tohto dokumentu.

7.1.4 Použitie rozšírení na obmedzenie politiky

Toto rozšírenie nie je používané.

7.1.5 Syntax a sémantika politiky

Každý KC, vydaný v zmysle tejto politiky, musí obsahovať jej identifikátor v podobe OID v rozšírení id-ce-certificatePolicies (2.5.29.32).

Každý KC, vydaný v zmysle tejto politiky, musí obsahovať identifikátor v podobe OID CP 1.3.158.36061701.0.0.0.1.2.2 v rozšírení id-ce-certificatePolicies (2.5.29.32), ktorým sa vyjadruje súlad požiadaviek Nariadenia eIDAS s národnou legislatívou.

7.1.6 Sémantika spracovania kritických certifikačných politík

Neuplatňuje sa.

7.2 Profily zoznamu zrušených certifikátov

Profil zoznamu zrušených certifikátov je definovaný v štandarde NBÚ „Formáty zoznamu zrušených certifikátov a potvrdzovania stavu a platnosti certifikátov“ verzia 3.0, ktoré vydala sekcia kybernetickej bezpečnosti Národného bezpečnostného úradu, Budatínska 30, 851 06 Bratislava.

7.2.1 Verzia

CRL, vydávané certifikačnou autoritou CA SNCA, musia byť CRL verzie 2.

CRL musia byť vydávané tou istou certifikačnou autoritou CA SNCA, ktorá vyhotovila a vydala kvalifikovaný certifikát.

Vydávané CRL musia byť v súlade s RFC 5280 „Internet X.509 Public Key Infrastructure Certificate and CRL Profile“.

7.2.2 Použité rozšírenia (CRL extensions) v CRL

Tabuľka č. 2 obsahuje zoznam rozšírení uvádzaných v CRL, vydávaných certifikačnou autoritou CA SNCA, povinnosť ich uvádzania a ich kritickosť.

Tabuľka č. 2 Rozšírenia vydávaného CRL

Názov rozšírenia	Vyžadované	Kritickosť
Authority Key Identifier (OID: 2.5.29.35)	ÁNO	NIE
CRL Number (OID: 2.5.29.20)	ÁNO	NIE
Issuing Distribution Point (OID: : 2.5.29.28)	ÁNO	ÁNO

7.3 Profil OCSP

7.3.1 Verzia

SNCA službu OCSP poskytuje. Vydávané OCSP odpovede sú v zmysle RFC 6960 „X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP“ a dokumentu Schéma dohľadu kvalifikovaných dôveryhodných služieb definovaná orgánom dohľadu. Ak budú OCSP odpovede pre jednotlivé vydávajúce certifikačné autority CA SNCA, vydávané samostatnými OCSP respondermi, ich podpisové certifikáty musia byť podpísané zodpovedajúcimi certifikačnými autoritami CA SNCA a zároveň musia obsahovať rozšírenie na použitie kľúča OCSP Signing (1.3.6.1.5.5.7.3.9).

7.3.2 OCSP rozšírenia

Tabuľka č. 3 obsahuje možné rozšírenia v OCSP odpovedi OCSP responderov Poskytovateľa, povinnosť ich uvádzania a ich kritickosť.

Tabuľka č. 3: Rozšírenia v OCSP odpovedi

Názov rozšírenia	Vyžadované	Kritickosť
id-commonpki-at-certHash (OID: 1.3.36.8.3.13)	ÁNO	NIE
id-pkix-ocsp-nonce (OID: 1.3.6.1.5.5.7.48.1.2)	NIE	NIE
id_pkix_ocsp_archive_cutoff (OID: 1.3.6.1.5.5.7.48. 1.6)	NIE	NIE

.

8 Audit zhody

Na zaistenie stabilného dohľadu nad bezpečnosťou prevádzky SNCA sa v prevádzke SNCA vykonáva bezpečnostný audit.

8.1 Témy pokrývané auditom zhody

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

8.2 Frekvencia auditu zhody

NASES, ako prevádzkovateľ SNCA a kvalifikovaný poskytovateľ dôveryhodných služieb sa musí na svoje náklady minimálne každých 24 mesiacov podrobiť posudzovaniu zhody - auditu ním poskytovaných kvalifikovaných dôveryhodných služieb zo strany orgánu posudzovania zhody, ktorý spĺňa požiadavky Nariadenia eIDAS.

8.3 Identita audítora a kvalifikačné požiadavky kladené na túto rolu

Orgán posudzovania zhody a ním poverené osoby na výkon auditu, musia spĺňať požiadavky ETSI EN 319 403, minimálne vo verzii 2.2.2.

8.4 Vzťah audítora k SNCA

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

8.5 Akcie vykonané na odstránenie nedostatkov

V prípade, že počas auditu zo stranu orgánu posudzovania zhody dôjde k zisteniu nedostatkov, zapríčinených rozporom medzi prevádzkou SNCA a platnými požiadavkami alebo ustanoveniami CP a vydaných CPS, je nevyhnutné zabezpečiť nasledovné činnosti:

- každý zistený nesúlad a rozpor musí byť audítorom riadne zdokumentovaný a zaznamenaný,
- audítor je povinný upovedomiť o rozpore všetky subjekty, uvedené v bode 8.6 tohto dokumentu,

- PMA je povinný zadefinovať, pripraviť a realizovať nápravné opatrenia na odstránenie zisteného nesúladu a rozporov a s realizovanými nápravnými opatreniami oboznámiť orgán posudzovania zhody.

8.6 Zaobchádzanie s výsledkami auditu

Orgán posudzovania zhody je povinný výsledky auditu predložiť auditovanému subjektu v písomnej forme, vypracovaním a odovzdaním tzv. správy audítora o vykonaní bezpečnostného auditu / auditu posúdenia zhody.

Auditovaný subjekt je povinný na základe predloženej správy:

- prijať a vykonať potrebné nápravné opatrenia,
- oznámiť orgánu posudzovania zhody navrhovaný termín realizácie a realizáciu prijatých nápravných opatrení.

NASES, ako prevádzkovateľ a poskytovateľ KDS, je povinný predložiť výslednú správu o posúdení zhody orgánu dohľadu v lehote troch pracovných dní od jej doručenia.

9 Iné obchodné a právne záležitosti

9.1 Poplatky

9.1.1 Poplatky za vydanie certifikátu

Poplatky za poskytované dôveryhodné služby a vydané certifikáty, musia byť každým klientom SNCA uhradené na základe dohodnutých podmienok s klientom SNCA - Odberateľom / Držiteľom certifikátu.

NASES, ako prevádzkovateľ SNCA a poskytovateľ kvalifikovaných dôveryhodných služieb, je povinný:

- zverejniť platný cenník svojich služieb na dedikovanej internetovej stránke SNCA a prostredníctvom webového sídla agentúry NASES,
- poskytovať všetky svoje dôveryhodné služby orgánom verejnej moci bezodplatne a za rovnakých podmienok.

Klienti SNCA sú povinní, zabezpečiť si certifikované QSCD produkty na vyhotovovanie kvalifikovaného elektronického podpisu / kvalifikovanej elektronickej pečate na vlastné náklady.

9.1.2 Poplatok za prístup k certifikátu

Neuplatňuje sa.

9.1.3 Poplatky za zrušenie alebo overenie statusu certifikátu

Neuplatňuje sa.

9.1.4 Poplatky za ostatné služby

Neuplatňuje sa.

9.1.5 Vrátenie poplatku

Neuplatňuje sa.

9.2 Finančná zodpovednosť

V súvislosti s rizikom zodpovednosti za škodu, je agentúra NASES, ako prevádzkovateľ SNCA, povinná udržiavať postačujúce finančné prostriedky a/alebo uzatvoriť vhodné poistenie zodpovednosti za škodu v súlade s platnými právnymi predpismi SR.

9.2.1 Poistenie

Poistenie prevádzkovateľa je určené platnými právnymi predpismi SR. Finančné krytie agentúry NASES, ako prevádzkovateľa SNCA, je zabezpečené zo štátneho rozpočtu.

9.2.2 Iné aktíva

Neuplatňuje sa.

9.2.3 Poistenie a záruky pre koncových používateľov

Neuplatňuje sa.

9.3 Dôvernosť

NASES, ako prevádzkovateľ SNCA, musí pristupovať k údajom získaným v súvislosti s poskytovanými kvalifikovanými dôveryhodnými službami v súlade s príslušnými právnymi predpismi, najmä so zákonom č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

9.3.1 Dôverné informácie

Dôvernými informáciami, podliehajúcimi zodpovedajúcej ochrane sú:

- súkromné kľúče vydávajúcich certifikačných autorít CA SNCA, využívané pri podpisovaní vyhotovovaných KC,
- súkromné kľúče autority časovej pečiatky, využívané pri podpisovaní vyhotovených elektronických časových pečiatok,
- súkromné kľúče OCSP respondera, používané na podpisovanie odpovedí na požiadavky na potvrdenie existencie a platnosti KC,
- súkromné kľúče, patriace k certifikátom zamestnancov NASES, zabezpečujúcich prevádzku kvalifikovaných dôveryhodných služieb SNCA (napr. certifikáty patriace registračným operátorom RA SNCA a pod.),
- interná infraštruktúra (napr. dokumenty, postupy, súbory, skripty, heslá, pass frázy a pod.), slúžiaca na prevádzku SNCA, vrátane registračných autorít RA SNCA,

- osobné údaje Držiteľov kvalifikovaných certifikátov, podliehajúce ochrane v zmysle zákona o ochrane osobných údajov,

a prípadne ďalšie technické, obchodné alebo výrobné údaje alebo iné informácie, ktoré nie sú verejne prístupné a ktoré sú označené SNCA alebo Odberateľom ako dôverné. Dôvernými informáciami môžu byť najmä, avšak nie výlučne, komerčné informácie, know-how, dáta, dokumentácie, špecifikácie, postupy a procesy, analýzy, informácie týkajúce sa klientov alebo obchodných partnerov, alebo iné informácie z informačného systému SNCA v akejkoľvek podobe.

So všetkými dôvernými informáciami, je nevyhnutné zaobchádzať ako s citlivými informáciami a prístup k nim je obmedzený len na osoby, ktoré tieto informácie nevyhnutne potrebujú na výkon svojich oficiálnych povinností.

9.3.2 Informácie nepovažované za dôverné

Dôvernými informáciami nie sú, prípadne prestávajú byť informácie, ktoré:

- sú v dobe ich prijatia druhou stranou verejne dostupnými alebo sa takými stanú následne bez toho, aby druhá strana porušila povinnosti podľa tejto CP, alebo
- boli druhej známe ich sprístupnením v súvislosti s poskytovanými dôveryhodnými službami, alebo
- boli druhou stranou preukázateľne získané od tretej osoby, ktorá je preukázateľne oprávnená šíriť takéto informácie, alebo
- boli druhou stranou nezávisle vyvinuté bez toho, aby došlo k neoprávnenej manipulácii s dôvernými informáciami alebo
- sú všeobecne známe aj napriek ich označeniu druhou stranou ako dôverné.

9.3.3 Zodpovednosť za ochranu dôverných informácií

Klienti SNCA ako aj NASES, ako prevádzkovateľ SNCA, sú povinní v prípade získania dôverných informácií alebo prístupu k nim tieto informácie chrániť pred ich prezradením a zdržať sa ich použitia alebo poskytnutia/prezradenia tretej strane.

V prípade, ak by mali byť tretej strane v rámci výkonu jej činnosti pre agentúru NASES, ako prevádzkovateľa SNCA, poskytnuté alebo sprístupnené dôverné informácie, agentúra NASES je povinná uzatvoriť s touto treťou stranou zmluvu o mlčanlivosti, resp. zmluvu o poskytnutí dôverných informácii, ktorej obsahom sú aj vyššie uvedené povinnosti.

NASES, ako prevádzkovateľ SNCA, môže za určitých okolností poskytnúť určité dôverné informácie tretej strane, najmä v prípade:

- povinného poskytnutia informácii orgánu dohľadu,
- povinného poskytnutia informácii v trestnom konaní, občianskom súdnom konaní alebo správnom konaní,

- poskytnutia informácii na požiadanie dotknutej osoby.

9.4 Ochrana osobných údajov

9.4.1 Politika ochrany osobných údajov

NASES, ako prevádzkovateľ SNCA, je povinný pri spracovaní osobných údajov:

- dodržiavať požiadavky zákona č. 18/2018 Z. z. o ochrane osobných údajov,
- prijať primerané technické a organizačné opatrenia pred neautorizovaným alebo nezákonným spracovaním osobných údajov a pred náhodnou stratou, zničením alebo poškodením osobných údajov,
- zdokumentovať rozsah a spôsob nakladania s poskytnutými osobnými údajmi v bezpečnostnom projekte,
- zabezpečiť dôvernosť a integritu osobných údajov, získaných v rámci procesu vyhotovovania kvalifikovaného certifikátu, a to aj v prípade ich prenosu medzi SNCA a Odberateľom či medzi jednotlivými komponentmi systému SNCA.

9.4.2 Informácie považované za súkromné

NASES, ako prevádzkovateľ SNCA, považuje za súkromné akékoľvek osobné údaje, týkajúce sa určenej alebo určiteľnej fyzickej osoby, pričom takouto osobou je osoba, ktorú možno určiť priamo alebo nepriamo, najmä na základe všeobecne použiteľného identifikátora, alebo na základe jednej či viacerých charakteristík alebo znakov, ktoré tvoria jej fyzickú, fyziologickú, psychickú, mentálnu, ekonomickú, kultúrnu alebo sociálnu identitu.

9.4.3 Informácie, ktoré nie sú považované za súkromné

NASES, ako prevádzkovateľ SNCA, môže:

- v súlade so zákonom č. 18/2018 Z. z. o ochrane osobných údajov definovať typy informácií, ktoré spracováva pri poskytovaní kvalifikovaných dôveryhodných služieb a nie sú považované za osobné údaje,
- na základe písomného súhlasu Držiteľa certifikátu na svojom webovom sídle zverejniť alebo sprístupniť informáciu o vydaní kvalifikovaného certifikátu s menom jeho Držiteľa.

9.4.4 Zodpovednosť za ochranu osobných údajov

NASES, ako prevádzkovateľ SNCA musí bezpečne uchovávať a ochraňovať osobné údaje, spracovávané v súvislosti s vyhotovovaním kvalifikovaného certifikátu. Tieto údaje je povinný chrániť prijatím vhodných bezpečnostných opatrení, a to najmä pred neautorizovaným prístupom, zmenou alebo prezradením.

9.4.5 Informačná povinnosť a súhlas

NASES, ako prevádzkovateľ SNCA je povinný pri plnení informačnej povinnosti voči dotknutým osobám a pri získavaní ich súhlasu so spracovaním osobných údajov, postupovať v súlade s požiadavkami zákona č. 18/2018 Z. z. o ochrane osobných údajov.

9.5 Ochrana práv duševného vlastníctva

NASES, ako prevádzkovateľ SNCA, je nositeľom autorských práv k všetkým dokumentom, databázam, postupom, politikám, poriadkom, pravidlám, certifikátom a súkromným kľúčom, ktoré sú súčasťou infraštruktúry SNCA a ktoré boli ním vytvorené.

9.6 Vyhlásenie a záruky

NASES, ako prevádzkovateľ SNCA prostredníctvom tejto CP a zmluvy o poskytovaní kvalifikovanej dôveryhodnej služby vyjadruje právne predpoklady používania vyhotovených kvalifikovaných certifikátov ich Držiteľmi a Spoliehajúcimi sa stranami.

9.6.1 Vyhlásenia a záruky SNCA

Pokiaľ ide o poskytované dôveryhodné služby, NASES, ako prevádzkovateľ SNCA neposkytuje žiadne vyhlásenia ani záruky s výnimkou prípadov, uvedených v tejto CP a nadväzujúcich CPS.

9.6.2 Vyhlásenia a záruky RA

Platia ustanovenia podľa bodu 9.6.1 tohto dokumentu.

9.6.3 Vyhlásenie a záruky Držiteľa

Ak nie je v tejto CP, alebo príslušnej zmluve s Odberateľom/Držiteľom KC uvedené inak, Držiteľ KC je výlučne zodpovedný za:

- poskytnutie správnych a presných informácií v komunikácii s SNCA,
- oboznámenie sa a súhlas so všetkými podmienkami, danými v tejto CP a s ňou spojenými politikami, ktoré sú dostupné na webovom sídle SNCA,
- generovanie kľúčového páru súkromný kľúč / verejný kľúč v prípade, že si kľúče k žiadosti na vydanie KC generuje vo vlastnej réžii,
- používanie vydaných KC len na právne účely a účely autorizácie v súlade s touto CP,
- ukončenie používania KC, pokiaľ sa ukáže, že akákoľvek informácia v KC je zavádzajúca, neaktuálna alebo nesprávna,

- vyvinutie maximálneho úsilia na zabránenie kompromitácie, straty, odtajnenie, modifikácie alebo akéhokoľvek neautorizovaného použitia súkromného kľúča, zodpovedajúceho verejnému kľúču, ktorý sa nachádza v KC vydanom SNCA.

9.6.4 Vyhlásenia a záruky Spoliehajúcej sa strany

Spoliehajúca sa strana akceptuje, že v prípade spoliehania sa na KC vydaný SNCA, musí:

- overiť platnosť vydaného KC prostredníctvom informácií na overenie stavu certifikátu (CRL),
- akceptovať KC len v prípade, že je platný a nebol zrušený alebo exspirovaný,
- dôverovať certifikátu vydávajúcej SNCA iba v prípade, že je platný a nebol zrušený alebo nie je exspirovaný,
- mať na pamäti akékoľvek obmedzenie použitia KC, či už je obsiahnuté v samotnom certifikáte alebo v tejto CP resp. publikovaných CPS,
- prijať akékoľvek iné kroky na minimalizáciu rizika pri spoľahnutí sa na elektronický podpis alebo elektronickú pečať vytvorenú prostredníctvom kľúčov, kde verejný kľúč je neplatný, zrušený, exspirovaný,
- vziať do úvahy akékoľvek iné indície dôveryhodnosti resp. nedôveryhodnosti, alebo iné fakty, s ktorými je Spoliehajúca sa strana oboznámená alebo bola na tieto upozornená.

9.6.5 Vyhlásenia a záruky iných strán

Neuplatňuje sa.

9.7 Odmietnutie poskytnutia záruky

NASES, ako prevádzkovateľ SNCA, zodpovedá v zmysle čl. 13 Nariadenia eIDAS výhradne za škodu, spôsobenú nesplnením svojich povinností podľa Nariadenia eIDAS.

9.8 Obmedzenie zodpovednosti

NASES, ako prevádzkovateľ SNCA, nezodpovedá za nepriame alebo podmienené straty alebo škody, ktoré Odberateľom alebo Spoliehajúcim sa stranám vznikli v súvislosti s používaním dôveryhodných služieb.

NASES, ako prevádzkovateľ SNCA, nezodpovedá za škodu, ktorá vznikla Odberateľovi/ Držiteľovi KC, Spoliehajúcej sa strane, príp. akýmkoľvek tretím stranám z dôvodu:

- porušenia povinností Odberateľom/Držiteľom certifikátu alebo Spoliehajúcou sa stranou, ktoré sú uvedené v právnych predpisoch, zmluve alebo v politikách SNCA, vrátane povinnosti vynaložiť primeranú starostlivosť pri používaní KC a pri spoliehaní sa na KC;
- neposkytnutia potrebnej súčinnosti zo strany Odberateľa/Držiteľa KC;
- nimi použitých softvérových alebo hardvérových prostriedkov a ich technickými vlastnosťami, konfiguráciou, nekompatibilitou, nevhodnosťou alebo inými vadami;
- používania, resp. spoliehania sa na KC, ktorého platnosť uplynula alebo ktorý bol zrušený;
- použitia KC Odberateľom/Držiteľom KC v rozpore so zmluvou alebo politikami SNCA;
- že KC bol použitý v rozpore s jeho účelom, určením alebo obmedzeniami uvedenými v KC resp. v politikách SNCA;
- omeškania alebo nedoručenia požiadaviek na overenie statusu KC SNCA, z dôvodov, ktoré nie sú na strane SNCA (najmä prípady nedostupnosti alebo preťaženosti siete internet alebo vady zariadenia alebo technického vybavenia používaného overovateľom);
- neposkytnutia niektorej z dôveryhodných služieb alebo jej nedostupnosti v priebehu plánovanej údržby alebo reorganizácie oznámenej na webovom sídle SNCA;
- pôsobenia vyššej moci.

Od okamihu, kedy zariadenie, na ktorom je uložený súkromný kľúč, ku ktorému patrí KC, nadobudne Odberateľ/Držiteľ KC, agentúra NASES, ako prevádzkovateľ SNCA nezodpovedá:

- za ochranu zariadenia, v ktorom je uchovaný KC a súkromný kľúč, resp. za ochranu prístupových kódov potrebných na jeho použitie,
- za to, že sa neoprávnená osoba zmocnila zariadenia alebo súkromného kľúča,
- za škody spôsobené použitím súkromného kľúča alebo KC, ak Odberateľ/Držiteľ KC nekoná v súlade so svojimi povinnosťami, najmä ak sa súkromného kľúča zmocní neautorizovaná osoba a Odberateľ/Držiteľ KC nepožiada o zrušenie KC, alebo ak SNCA neoznámi zmeny v údajoch.

9.9 Náhrada škody

Každý, kto poruší svoju povinnosť alebo akýkoľvek záväzok, vyplývajúci z tejto CP resp. zmluvy o poskytovaní kvalifikovanej dôveryhodnej služby, je povinný nahradiť škodu tým spôsobenú druhej strane, okrem prípadov, kde je vylúčená zodpovednosť daného subjektu za škody. Za škodu sa považuje skutočná škoda, ušlý zisk a náklady vzniknuté poškodenej strane v súvislosti so škodovou udalosťou.

Každý, kto poruší svoju povinnosť alebo akýkoľvek záväzok, vyplývajúci z tejto CP, resp. zmluvy o poskytovaní kvalifikovanej dôveryhodnej služby, môže byť zbavený zodpovednosti

na náhradu škody, jedine ak preukáže, že k porušeniu povinnosti alebo akéhokoľvek záväzku, došlo v dôsledku okolností vylučujúcich zodpovednosť – vyššej moci.

9.10 Doba platnosti, ukončenie platnosti

9.10.1 Doba platnosti

Tato verzia CP platí odo dňa nadobudnutia jej platnosti, až do jej nahradenia novou verziou. Podrobnosti o histórii zmien tejto CP sú uvedené v časti dokumentu - „História zmien“.

9.10.2 Ukončenie platnosti

Platnosť tejto verzie CP skončí dňom publikovania novej verzie s vyšším číslom.

9.10.3 Dôsledky ukončenia platnosti

V prípade, že tento dokument nebude nahradený novou verziou a v čase jeho platnosti dôjde k ukončeniu poskytovania kvalifikovaných dôveryhodných služieb zo strany prevádzkovateľa SNCA, musia byť dodržané všetky ustanovenia tejto CP týkajúce sa prevádzkovateľa SNCA, ktoré je povinný dodržať po ukončení svojej činnosti.

9.11 Jednotlivé oznámenia a komunikácia s účastníkmi

Neuplatňuje sa.

9.12 Zmeny

9.12.1 Postup vykonávania zmien

Neuplatňuje sa.

9.12.2 Postup a periodicita oznamovania zmien

SNCA oznamuje zmeny na svojom webovom sídle.

9.12.3 Okolnosti zmeny OID

Neuplatňuje sa.

9.13 Riešenie sporov

Odberateľ/Držiteľ KC má právo zaslať SNCA sťažnosť, podnet alebo reklamáciu na poskytnutú kvalifikovanú dôveryhodnú služby emailom na info@nases.gov.sk. NASES, ako prevádzkovateľ SNCA, vybaví reklamáciu najneskôr do 30 dní od jej prijatia, pokiaľ sa strany nedohodnú inak. Vybavenie reklamácie sa vzťahuje len k popisu vady uvedenej Odberateľom.

Súdy Slovenskej republiky majú výlučnú právomoc na rozhodovanie akýchkoľvek sporov medzi agentúrou NASES a Odberateľom/Držiteľom KC. V prípade, že Odberateľ/Držiteľ KC je spotrebiteľom, prípadný spor môže riešiť taktiež mimosúdnou cestou.

V takomto prípade je oprávnený kontaktovať subjekt mimosúdneho riešenia sporov, ktorým je Slovenská obchodná inšpekcia alebo iná právnická osoba zapísaná v zozname subjektov alternatívneho riešenia spotrebiteľských sporov vedenom Ministerstvom hospodárstva Slovenskej republiky a dostupnom na jeho webovom sídle. Odberateľ/Držiteľ KC má právo voľby, na ktorý z uvedených subjektov alternatívneho riešenia spotrebiteľských sporov sa obráti. Pred pristúpením k súdnemu alebo mimosúdnemu riešeniu sporu sú zmluvné strany povinné pokúsiť sa najskôr vyriešiť tento spor vzájomnou dohodou.

9.14 Rozhodné právo

Právne vzťahy medzi agentúrou NASES a Odberateľom/Držiteľom KC sa riadia právnymi predpismi Slovenskej republiky.

9.15 Súlad s platnými právnymi predpismi

NASES, ako prevádzkovateľ SNCA, poskytuje dôveryhodné služby v súlade s právnymi predpismi platnými v Slovenskej republike.

9.16 Rôzne ustanovenia

9.16.1 Postúpenie práv

Odberateľ/Držiteľ KC nesmie svoje práva, povinnosti ako aj pohľadávky z tejto CP alebo Zmluvy postúpiť alebo previesť (ani s nimi akokoľvek inak obchodovať) na tretiu osobu bez písomného súhlasu zo strany agentúry NASES.

9.16.2 Salvatórska klauzula

Pokiaľ akékoľvek ustanovenie tejto CP je alebo sa stane neplatným alebo nevymáhateľným, nespôsobí to neplatnosť alebo nevymáhateľnosť celej CP, ak je úplne oddeliteľné od ostatných ustanovení tejto CP.

NASES, ako prevádzkovateľ SNCA, bezodkladne nahradí neplatné alebo nevymáhateľné ustanovenie CP novým platným a vymáhateľným ustanovením, ktorého predmet bude v najvyššej možnej miere zodpovedať predmetu pôvodného ustanovenia a zároveň bude zachovaný účel tejto CP a obsah jednotlivých ustanovení tejto CP.

9.16.3 Uplatnenie práv

V prípade, že určité právo počas trvania zmluvného vzťahu medzi zmluvnými stranami nie je uplatňované, toto právo z titulu jeho neuplatňovania nezaniká, pokiaľ nie je inde uvedené inak.

Zánikom zmluvného vzťahu medzi zmluvnými stranami nie sú zmluvné strany zbavené povinnosti plniť všetky dovtedy vzniknuté záväzky z uplatnených práv a uskutočniť všetky nevyhnutné právne úkony, ktoré neznesú odklad a ktoré sú nevyhnutne potrebné na zabránenie vzniku škody.

9.16.4 Vyššia moc

NASES, ako prevádzkovateľ SNCA, Odberateľ a Držiteľ nie sú zodpovední za omeškanie so splnením svojich záväzkov spôsobené okolnosťami vylučujúcimi zodpovednosť (vyššou mocou).

Okolnosťou vylučujúcou zodpovednosť je prekážka, ktorá nastala nezávisle na vôli povinnej strany a bráni jej v splnení jej povinnosti, ak je nemožné rozumne predpokladať, že by povinná strana túto prekážku alebo jej následky odvrátila alebo prekonala a ďalej, že by v čase vzniku prekážku predvídala, či mohla alebo mala predvídať.

Ak nastanú okolnosti vylučujúce zodpovednosť, potom je strana, u ktorej táto skutočnosť nastane, povinná bezodkladne informovať druhú stranu o povahe, začiatku a konci trvania takejto prekážky, ktorá bráni splneniu jej povinností. NASES, ako prevádzkovateľ SNCA, Odberateľ a Držiteľ sa zaväzujú vyvinúť maximálne úsilie na odvrátenie a prekonanie okolností, vylučujúcich zodpovednosť.

Zodpovednosť však nie je vylúčená v prípade, keď takáto okolnosť vznikla až v čase, keď povinná strana bola v omeškaní s plnením svojej povinnosti, alebo ak predmetná strana nesplní svoju povinnosť bezodkladne informovať druhú stranu o povahe a začiatku trvania prekážky, alebo ak vznikla z jej hospodárskych pomerov. Účinky vylučujúce zodpovednosť sú obmedzené len na obdobie, kým trvá prekážka, s ktorou sú tieto účinky spojené.

9.17 Iné ustanovenia

Služby vyhotovovania KC môžu byť dostupné prostredníctvom mobilnej registračnej autority SNCA aj osobám so zdravotným postihnutím, pokiaľ splnia všetky podmienky tejto CP.