Č. p.:

DKDS9 Pravidlá na výkon certifikačných činností (CPS) SNCA

Názov dokumentu:	DKDS9 Pravidlá na výkon certifikačných činností (CPS) SNCA		
Označenie dokumentu:	DKDS9 Pravidlá na výkon certifikačných činností CPS SNCA.pdf		
Verzia:	0.9	Status:	*Návrh*
Dátum vytvorenia:	18.11.2020	Platný do:	31.12.2021

História dokumentu

História revízií dokumentu

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

Schválenia

Verzia	Funkcia	V zastúpení	Schválil dňa	Podpis

Distribúcia

Verzia	Spoločnosť	Meno	Počet výtlačkov

Referencie na legislatívne a normatívne dokumenty

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

[2] Nariadenie Európskeho parlamentu a rady (EÚ) č. 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (ďalej len „GDPR“).
Nariadenie GDPR

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

[4] Zákon č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov (ďalej len „zákon o ochrane osobných údajov“).
Zákon č. 18/2018 Z. z. o ochrane osobných údajov

[5] Zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov v znení zákona č. 134/2020 Z. z..
Zákon č. 95/2019 Z. z. o ITVS

[6] Vyhláška Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 78/2020 Z. z. o štandardoch pre informačné technológie verejnej správy.
Vyhláška o štandardoch pre ITVS

[7] STN ISO/IEC 27001 Informačné technológie - Bezpečnostné metódy - Systémy riadenia informačnej bezpečnosti – Požiadavky.

[8] Politika poskytovania dôveryhodných služieb NASES, OID: 1.3.158.42156424.0.1.1

Obsah

1 Úvod (Introduction)

1.1 Všeobecne (Overview)

Tento dokument, „Pravidlá na výkon certifikačných činností SNCA“ (Certification Practice Statement, ďalej len „CPS“), prezentuje vykonávacie postupy, ktoré Národná agentúra pre sieťové a elektronické služby (ďalej aj „NASES“, „agentúra“ alebo „prevádzkovateľ SNCA“) využíva na zabezpečenie kvalifikovaných dôveryhodných služieb.

Kvalifikované dôveryhodné služby poskytuje NASES prostredníctvom Slovenskej národnej certifikačnej autority (ďalej len „SNCA“), ktorú za týmto účelom prevádzkuje.

Tieto CPS slúžia používateľom a spoliehajúcim sa tretím stranám ako podklad pre posúdenie dôveryhodnosti certifikátu.

Tieto CPS podporujú Certifikačnú politiku 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: 1.3.158.36061701.0.0.0.1.2.2.

Pre účely týchto CPS, pre podmienky poskytovania kvalifikovanej dôveryhodnej služby vyhotovovania kvalifikovaných elektronických časových pečiatok, sa uplatňujú podmienky, uvedené v dokumente „Politika poskytovania kvalifikovanej dôveryhodnej služby vyhotovovania kvalifikovaných elektronických časových pečiatok“, ktorý je zverejnený na internetovej stránke SNCA http://ep.nbu.gov.sk/snca/docs/Certifikačná politika TSAP SNCA.pdf.

1.2 Názov a identifikácia dokumentu (Document name and identification)

Tento dokument je označovaný ako „Pravidlá na výkon certifikačných činností SNCA“.

Objektový identifikátor (OID) Pravidiel na výkon certifikačných činností SNCA: neudeľuje sa

1.3 PKI účastníci (PKI participants)

1.3.1 Certifikačné autority (Certification authoritites)

Certifikačnou autoritou, sa v rámci tohto CPS 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 len „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.

SNCA, okrem poskytovania vyššie uvedených dôveryhodných služieb, slúži aj na vydávanie certifikátov pre operátorov SNCA.

1.3.2 Registračné autority (Registration authorities)

Služby registračnej autority SNCA (ďalej aj „RA SNCA“) v zmysle tohto CPS, vykonáva prevádzkovateľ SNCA a iné orgány verejnej moci, na základe uzatvorenej písomnej zmluvy s prevádzkovateľom SNCA.

Prevádzkovateľ SNCA môže zriadiť RA SNCA nasledovných typov:

- interná RA SNCA – ktorá je prevádzkovaná NASES a je určená na poskytovanie dôveryhodných služieb klientom SNCA z radov fyzických osôb, právnických osôb a klientom SNCA zo všetkých OVM. Táto RA SNCA nie je samostatný právny subjekt.
- externá OVM RA SNCA – ktorá je určená na sprostredkovanie vybraných dôveryhodných služieb výhradne pre vlastné potreby konkrétneho OVM, resp. pre potreby ním prevádzkovaných systémov, vyžadujúcich použitie certifikátov a bude zriadená a prevádzkovaná na základe písomnej zmluvy, uzatvorenej medzi prevádzkovateľom SNCA a daným konkrétnym OVM. Táto RA SNCA je samostatný právny subjekt.

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

1.3.3 Držitelia certifikátov (Subscribers)

Držiteľmi certifikátov, vydávaných SNCA sú:

- SNCA,
- obslužný personál SNCA,
- klienti SNCA:
  - fyzické osoby,
  - fyzické osoby, identifikované v spojení s právnickými osobami,
  - právnické osoby, ktorými môžu byť organizácie alebo ich organizačné jednotky,
  - fyzické osoby, identifikované v spojení s orgánmi verejnej moci,
  - orgány verejnej moci.

1.3.4 Používatelia certifikátov (Relying parties)

Spoliehajúcimi stranami sú fyzické osoby, fyzické osoby, identifikované v spojení s právnickými osobami, právnické osoby, fyzické osoby, identifikované v spojení s OVM a orgány verejnej moci, ktoré sa spoliehajú na certifikáty vydané SNCA.

1.3.5 Iné subjekty (Other participants)

Inými subjektami môžu byť:

- orgán dohľadu (NBÚ),
- orgány činné v trestnom konaní,
- ďalšie orgány verejnej moci, ktorým to vyplýva z:
  - nariadenia Európskeho parlamentu a Rady č. 910/2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES (ďalej len „nariadenie eIDAS“)
  - zákona č. 272/2016 Z. z. o dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zmene a doplnení niektorých zákonov (zákon o dôveryhodných službách),
  - iných právnych predpisov SR a Európskej únie (ďalej len „EÚ“).

Tieto CPS zohľadňujú dokumentáciu CA/Browser Forum pre WEB trust services.

1.4 Použiteľnosť certifikátov (Certificate usage)

1.4.1 Korektné použitie certifikátu (Appropriate certificate uses)

Certifikáty, vydávané podľa týchto CPS, môžu byť použité ich držiteľmi, používateľmi a inými subjektami, len v súlade s pravidlami, publikovanými v tomto dokumente a platnými právnymi predpismi SR a EÚ.

Certifikáty SNCA

Certifikáty SNCA je možné použiť na:

- overovanie certifikátov SNCA,
- overovanie certifikátov obslužného personálu SNCA,
- overovanie kvalifikovaných certifikátov pre elektronický podpis,
- overovanie kvalifikovaných certifikátov pre elektronickú pečať,
- overovanie certifikátov serverov časových pečiatok,
- overovanie zoznamov zrušených certifikátov (ďalej len „CRL“),
- overovanie kvalifikovaných certifikátov pre autentifikáciu webových sídiel.

Certifikáty obslužného personálu

Certifikáty obslužného personálu, je možné použiť na autentifikáciu obslužného personálu SNCA k aktívam SNCA.

Kvalifikované certifikáty

Kvalifikované certifikáty, vydávané SNCA, je možné použiť na:

- overovanie a vytváranie kvalifikovaných elektronických podpisov,
- overovanie a vytváranie kvalifikovaných elektronických pečatí.

Certifikáty serverov časových pečiatok

Certifikáty serverov časových pečiatok, je možné použiť na overovanie kvalifikovaných elektronických časových pečiatok.

Kvalifikované certifikáty pre autentifikáciu webového sídla

Kvalifikované certifikáty pre autentifikáciu webového sídla, je možné použiť na autentifikáciu webového sídla organizácie.

1.4.2 Nepovolené použitie certifikátu (Prohibited certificate uses)

Akékoľvek iné použitie certifikátov, odlišné od spôsobov použitia uvedených v bode 1.4.1 týchto CPS, sa považuje za nepovolené (neoprávnené) použitie certifikátu.

1.5 Administrácia dokumentu (Policy administration)

1.5.1 Organizácia spravujúca dokument (Organization administering the document)

Organizáciou, spravujúcou tieto CPS je:

Národná agentúra pre sieťové a elektronické služby

Detašované pracovisko:

BC Omnipolis

Trnavská cesta 100/II

821 01 Bratislava

Slovenská republika

1.5.2 Kontaktná osoba (Contact person)

Kontaktnou osobou je pracovník NASES, zaradený do roly bezpečnostný správca SNCA.

1.5.3 Osoba posudzujúca kompatibilitu CPS s CP (Person determining CPS suitability for the policy)

Osobou, ktorá rozhoduje o kompatibilite týchto CPS s podporovanou Certifikačnou politikou 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: 1.3.158.36061701.0.0.0.1.2.2, je riaditeľ sekcie Slovenskej národnej certifikačnej autority.

1.5.4 Schvaľovací proces CPS (CPS approval procedures)

Vykonávať zmeny v rámci týchto CPS, je oprávnená osoba podľa bodu 1.5.2 týchto CPS a každú novú verziu schvaľuje riaditeľ sekcie Slovenskej národnej certifikačnej autority.

1.6 Definície a skratky (Definitions and acronyms)

Definície

Definícia	Vysvetlenie definície
Certifikačná autorita *(CA)*	Dôveryhodná autorita, ktorá generuje certifikáty a zoznamy zrušených certifikátov (komponent infraštruktúry PKI).
Certifikačná politika *(CP)*	Pomenovaný zoznam pravidiel, ktoré označujú použiteľnosť certifikátu v príslušnej skupine alebo triede aplikácií, zdieľajúcimi spoločné bezpečnostné požiadavky.
Pravidlá na výkon certifikačných činností *(CPS)*	Zoznam predpisov a praktík, ktoré certifikačné autority používajú pri vydávaní certifikátov.
Certifikát	Reťazec údajov, ktorý spája identifikátor (Distinguished Name) koncového subjektu s verejným kľúčom, pomocou digitálneho podpisu. Formát tohto reťazca údajov, je definovaný v ISO/IEC 9594-8. Tento reťazec údajov taktiež obsahuje - identifikátor vydavateľa certifikátu, špecifické sériové číslo certifikátu, dobu platnosti a ďalšie údaje.
Digitálny podpis	Jedinečná digitálna identifikácia entity, ktorá sa využíva na autentifikáciu zdroja, kontrolu integrity dát a nepopierateľnosť. Digitálny podpis využíva súkromný kľúč, ktorému zodpovedá príslušný verejný kľúč, matematickú funkciu známu ako „message digest“ a princípy asymetrickej kryptografie.

Infraštruktúra PKI	Technické a programové vybavenie, použité na zaistenie služieb na vydávanie a správu certifikátov.
Kompromitácia súkromného kľúča	Zneužitie, použitie alebo sprístupnenie súkromného kľúča bez vedomia jeho vlastníka, ako aj prezradenie hesla na prístup k revokačnému heslu. Ak certifikačná autorita zistí kompromitáciu súkromného kľúča, certifikát zviazaný s týmto kľúčom zruší.
Kryptografický modul	Hardvérové zariadenie, umožňujúce vykonávať kryptografické operácie (HSM modul).
Obnova kľúčov *(Keys Renewal)*	Obnova kľúčov, v kontexte tohto dokumentu, znamená vydanie nového certifikátu s rovnakými alebo veľmi podobnými charakteristikami, ako pôvodný (obnovovaný) certifikát. Generuje sa nová dvojica kľúčov, prislúchajúca k certifikátu.
Odtlačok verejného kľúča *(Fingerprint)*	tzv. *hash* verejného kľúča. Hash je matematická funkcia, ktorá vytvára „skratku“ dát (*message digest*). Z dát rôznej veľkosti vytvorí skrátenú správu fixnej veľkosti. Zo správy nie je možné spätne získať pôvodné dáta. Akákoľvek zmena vstupných dát sa preukáže tým, že sa vytvorí iný message digest.
Súkromný kľúč	Súkromná časť dvojice asymetrických kľúčov. Používa sa na podpisovanie a (alebo) dešifrovanie správ.
Registračná autorita *(RA)*	Komponent infraštruktúry PKI, používaný na presun schválených žiadostí o vydanie certifikátu do CA.
Registračné miesto	Priestory, v ktorých sa prijímajú a schvaľujú žiadosti o vydanie certifikátu. Registračné miesto obsluhuje registračný operátor.
Kľúčový pár	Dvojica asymetrických kľúčov, ktorá pozostáva zo súkromného a verejného kľúča.
Spoliehajúca strana *(Relying party)*	Subjekt alebo komponent, ktorý požaduje od PKI infraštruktúry overenie stavu certifikátu.
Verejný kľúč	Verejná časť dvojice asymetrických kľúčov. Používa sa na šifrovanie a overovanie správ.
Zrušenie certifikátu *(Certificate Revocation)*	Ukončenie platnosti certifikátu. Účinnosť certifikátu nie je možné obnoviť.
Zoznam zrušených certifikátov *(CRL)*	Zoznam certifikátov, ktorých platnosť bola pozastavená alebo zrušená. Zoznam vydáva a podpisuje Certifikačná autorita a je publikovaný v adresári LDAP.

Skratky

Skratka	Vysvetlenie skratky
CA	Certifikačná autorita *(Certification*
CP	Certifikačná politika *(Certificate Policy)*
CPS	Pravidlá na výkon certifikačných činností
CRL	Zoznam zrušených certifikátov *(Certificate*
DN	Rozlišovacie meno *(Distinguished Name)*
ES	Európske spoločenstvo
EÚ	Európska únia
IČO	Identifikačné číslo organizácie
ITU-T	International Telecommunication Union
KC	Kvalifikovaný certifikát
NASES	Národná agentúra pre sieťové a elektronické
NBÚ	Národný bezpečnostný úrad
OID	Identifikátor klasifikácie objektov *(Object*
PKCS	Public Key Cryptography Standards
PKI	Infraštruktúra verejného kľúča *(Public Key*
QSCD	Qualified Signature Creation Device
RA	Registračná autorita *(Registration Authority)*
RSA	Rivest-Shamir-Adleman
SEP	Sekcia ekonomiky a prevádzky
SHA	Secure Hash Algorithm
SNCA	Slovenská národná certifikačná autorita
SR	Slovenská republika
Z. z.	Zbierka zákonov

2 Zodpovednosti za publikáciu a úložisko (Publication and repository responsibilities)

2.1 Repozitáre (Repositories)

SNCA spravuje repozitáre (úložiská dokumentácie a informácií) podľa nariadenia eIDAS a zákona o dôveryhodných službách.

2.2 Zverejňovanie certifikačných informácií (Publication of certification information)

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

2.3 Čas alebo frekvencia publikácie (Time or frequency of publication)

SNCA zverejňuje certifikačné informácie, určené na zverejnenie, v zmysle nariadenia eIDAS a zákona o dôveryhodných službách podľa nasledovného kľúča:

- odkaz na Certifikačnú politiku 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: 1.3.158.36061701.0.0.0.1.2.2 – *aktualizované neodkladne po každej zmene*,
- legislatíva, formáty a štandardy – *aktualizované neodkladne po každej zmene*,
- informácie o akreditácii (kvalifikovanom štatúte) – *aktualizované neodkladne po každej zmene*,
- informácie o certifikátoch vydaných koreňovou CA pre SNCA – *aktualizované neodkladne po každej zmene*,
- zoznam certifikátov vydaných pre servery časových pečiatok – *aktualizovaný neodkladne po vydaní nového certifikátu*,
- zoznamy CRL – *nový zoznam CRL publikovaný zvyčajne každé štyri hodiny, najmenej však raz za 24 hodín,*
- informácie o kvalifikovanej dôveryhodnej službe vyhotovovania kvalifikovaných elektronických časových pečiatok – *aktualizované neodkladne po každej zmene*,
- cenník služieb – *aktualizovaný neodkladne po každej zmene*,
- obmedzenia pri poskytovaní dôveryhodných služieb – *aktualizované neodkladne po každej zmene*,
- kontaktné informácie na prevádzkovateľa SNCA – *aktualizované neodkladne po každej zmene*.

2.4 Kontrola prístupu k repozitárom (Access controls on repositories)

Certifikačné informácie, podľa bodu 2.3 týchto CPS, zverejňuje prevádzkovateľ SNCA bez obmedzenia.

Ďalšie certifikačné informácie, ktoré nie sú verejnými informáciami, sú dostupné povereným pracovníkom prevádzkovateľa SNCA a tretím stranám, na základe rozhodnutia riaditeľa sekcie Slovenskej národnej certifikačnej autority, vždy však v súlade s platným právnymi predpismi SR a EÚ.

3 Identifikácia a autentifikácia

3.1 Menná konvencia (Naming)

3.1.1 Typy mien (Types of names)

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 (Need for names to be meaningful)

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 žiadateľov a používanie pseudonymov (Anonymity or pseudonymity of subscribers)

SNCA uvádza pseudonymy, len v kvalifikovaných certifikátoch pre elektronické pečate, vydávaných pre správcov elektronických podateľní.

3.1.4 Pravidlá na interpretáciu rôznych foriem mien (Rules for interpreting various name forms)

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.

3.1.5 Jednoznačnosť mien (Uniqueness of names)

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 Rozpoznávanie, autentizácia a úloha ochranných známok (Recognition, authentication, and role of trademarks)

Ochranné známky nie sú v rámci poskytovania dôveryhodných služieb zo strany SNCA využívané.

3.2 Iniciálne overenie identity (Initial identity validation)

3.2.1 Metóda preukazovania vlastníctva súkromného kľúča (Method to prove possession of private key)

SNCA vždy požaduje, aby žiadateľ o vydanie certifikátu potvrdil, že je vlastníkom súkromného kľúča, ktorý prislúcha k verejnému kľúču, nachádzajúcemu sa v žiadosti o vydanie certifikátu.

Ak kľúčový pár generuje operátor RA SNCA v rámci registračného procesu, preukazovanie vlastníctva súkromného kľúča sa od žiadateľa o vydanie certifikátu nepožaduje.

Ak kľúčový pár nie je generovaný operátorom RA SNCA v rámci registračného procesu, musí žiadateľ o vydanie certifikátu preukázať a potvrdiť vlastníctvo súkromného kľúča, o čom musí byť vyhotovený záznam, podpísaný žiadateľom o vydanie certifikátu.

3.2.2 Autentizácia identity organizácie (Authentication of organization identity)

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 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 (Authentication of individual identity)

Žiadateľ o vydanie certifikátu musí požiadať o vydanie certifikátu na registračnom mieste RA SNCA osobne, prípadne v zastúpení. Žiadateľ musí predložiť:

- písomnú žiadosť o vydanie certifikátu - formulár „Žiadosť o poskytovanie kvalifikovaných dôveryhodných služieb“,
- doklad totožnosti, ktorý obsahuje nasledovné údaje držiteľa certifikátu:
  - celé meno a priezvisko,
  - adresu trvalého pobytu,
  - rodné číslo (osoby, ktoré ho majú pridelené),
  - dátum narodenia (osoby, ktoré nemajú pridelené rodné číslo),
- klient SNCA / držiteľ certifikátu musí zároveň predložiť ďalší doklad, ktorý obsahuje minimálne meno a priezvisko držiteľa a ďalší jeho osobný údaj (dátum narodenia, rodné číslo). Toto neplatí v prípade, ak ide o služobný preukaz.
- elektronickú žiadosť o vydanie certifikátu vo formáte PKCS#10,
- dokument, preukazujúci oprávnenie žiadať o vydanie kvalifikovaného certifikátu od SNCA – tento je špecifikovaný v certifikačnom poriadku (ďalej len „CP“) a upravený v „Zmluve o poskytovaní kvalifikovaných dôverných služieb“, uzatvorenej medzi prevádzkovateľom SNCA a organizačnou zložkou právnickej osoby alebo orgánu verejnej moci,
- oficiálne poverenie na zastupovanie právnickej osoby, ktorá žiada o vydanie kvalifikovaného certifikátu. Táto osoba sa musí preukázať úradnou plnou mocou na zastupovanie.

Operátor registračného miesta RA SNCA pred akceptovaním žiadosti o vydanie certifikátu preverí:

- doklady žiadateľa o vydanie certifikátu,
  - pri overovaní identity držiteľa certifikátu, musí registračný operátor RA SNCA akceptovať nasledovné doklady:
    - občiansky preukaz,
    - cestovný pas,
    - vodičský preukaz,
    - rodný list,
    - služobný preukaz,
    - preukaz poistenca verejného zdravotného poistenia,
    - zbrojný preukaz.
  - v prípade predloženia rodného listu, zbrojného preukazu, služobného preukazu alebo preukazu poistenca verejného zdravotného poistenia, musí byť súčasne predložený aj jeden z týchto dokladov: občiansky preukaz alebo cestovný pas.
- či žiadateľ spĺňa požiadavky na vydanie certifikátu,
- údaje, ktoré majú byť uvedené v certifikáte s podkladmi, uvedenými v žiadosti,
- či zastupujúca osoba spĺňa požiadavky na zastupovanie,

- či žiadateľ má k dispozícii súkromný kľúč, prináležiaci k verejnému kľúču, na ktorý je požadovaný certifikát (v prípade, že žiadateľa zastupuje iná oprávnená osoba musí táto predložiť s tým súvisiace splnomocnenie),
- v prípade kvalifikovaného certifikátu, či je žiadateľ o vydanie certifikátu oboznámený so „Zmluvou o vydaní a používaní kvalifikovaného certifikátu“, ktorej súčasťou je aj vyhlásenie žiadateľa – „Súhlas so spracovaním osobných údajov“ a či žiadateľ o vydanie certifikátu túto zmluvu podpísal.

V prípade, že:

- žiadateľa zastupuje iná oprávnená osoba, musí táto osoba predložiť s tým súvisiace úradne overené splnomocnenie, z textu ktorého je jednoznačne jasné, že zastupujúca fyzická osoba bola splnomocnená splnomocňujúcou fyzickou osobou konať v danej veci v jej mene.
- klientom SNCA je zákonný zástupca (spravidla rodič), musí naviac predložiť rodný list dieťaťa, osvojiteľ musí naviac predložiť rozhodnutie zo súdu alebo výpis z matriky.
- klientom SNCA je právnická osoba, ktorá žiada vydanie certifikátu pre fyzickú osobu, ktorá je jej zamestnancom a v žiadosti je uvedený názov tejto právnickej osoby, predkladá okrem dokladov uvedených v tomto bode aj doklady, podľa bodu 3.2.2. Táto požiadavka sa netýka zamestnancov OVM, kde je zmluvne dohodnutý iný mechanizmus overovania.
- žiadateľovi o vydanie certifikátu je vyhotovovaný mandátny certifikát (§8 zákona o dôveryhodných službách), potom žiadateľ o vydanie certifikátu musí predložiť doklady, preukazujúce oprávnenie v zmysle požiadaviek, uvedených v aktuálnej verzii zoznamu oprávnení, ktorý je zverejnený na webovom sídle NBÚ (§9, ods. 2, písm. b) zákona o dôveryhodných službách).

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).

Ak niektorá z podmienok nie je splnená, alebo ju nie je možné overiť, registračný operátor RA SNCA žiadosť o vydanie certifikátu odmietne a informuje o tejto skutočnosti ako aj o dôvode jej zamietnutia žiadateľa, prípadne splnomocnenú osobu.

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.

Prípadné doklady v cudzom jazyku (okrem češtiny) musia byť preložené do slovenského jazyka úradným prekladateľom – znalcom.

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

3.2.4 Neoverené informácie o žiadateľovi (Non-verified subscriber information)

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

3.2.5 Overenie príslušnosti k organizácii (Validation of authority)

Overenie príslušnosti doručiteľa žiadosti o vydanie certifikátu pozostáva z:

- overenia plnomocenstva, oprávňujúceho fyzickú osobu na konanie v mene organizácie,
- overenie dokladu totožnosti alebo služobného/zamestnaneckého preukazu.

3.2.6 Kritériá na interoperabilitu (Criteria for interoperation)

Interoperabilita, v procese iniciálneho overenia identity, je zabezpečená dodržiavaním platných právnych predpisov SR a EÚ.

3.3 Identifikácia a autentizácia pre žiadosti o pregenerovanie kľúčov (Identification and authentication for re-key requests)

3.3.1 Identifikácia a autentizácia pre rutinné pregenerovanie kľúčov (Identification and authentication for routine re-key)

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 bode 3.2 týchto CPS.

3.3.2 Identifikácia a autentizácia pre pregenerovanie kľúčov po zrušení certifikátu (Identification and authentication for re-key after revocation)

Proces pregenerovania kľúčového materiálu po zrušení certifikátu, 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 bode 3.2 týchto CPS.

3.4 Identifikácia a autentizácia pre žiadosť o zrušenie certifikátu (Identification and authentication for revocation request)

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).

Nižšie-uvedený postup je záväzný pre každého žiadateľa o zrušenie certifikátu, vydaného SNCA a každý žiadateľ o zrušenie certifikátu je povinný ho dodržať.

„Žiadosť o zrušenie certifikátu“ je možné podať:

- na registračnom mieste RA SNCA,
- elektronickou formou,
- listovou zásielkou,
- telefonicky (a následne niektorým zo spôsobov podľa vyššie uvedených bodov).

Na registračnom mieste RA SNCA sa podáva žiadosť o zrušenie certifikátu písomnou formou (žiadateľ je povinný vyplniť „Žiadosť o zrušenie certifikátu“), počas zverejnených stránkových hodín registračného miesta RA SNCA.

Žiadateľ o zrušenie certifikátu musí preukázať vlastníctvo certifikátu, o ktorého zrušenie žiada. Predložená žiadosť o zrušenie certifikátu v písomnej forme, musí byť podpísaná žiadateľom. Písomná „Žiadosť o zrušenie certifikátu“, musí obsahovať nasledujúce údaje: typ certifikátu, sériové číslo certifikátu, celé občianske meno a priezvisko klienta SNCA, ktorému bol certifikát vydaný a heslo pre zrušenie certifikátu, ktoré bolo uvedené v „Protokole o odovzdaní a prevzatí certifikátu“. Heslo pre zrušenie certifikátu, môže byť nahradené preukázaním sa pravým a platným dokladom totožnosti držiteľa certifikátu.

Elektronickou formou sa podáva žiadosť o zrušenie certifikátu na e-mailovú adresu registračného miesta RA SNCA, ktoré mu vydalo certifikát.

„Žiadosť o zrušenie certifikátu“, podaná elektronickou formou, musí byť podpísaná kvalifikovaným certifikátom žiadateľa a musí obsahovať nasledujúce údaje: sériové číslo certifikátu, celé občianske meno a priezvisko klienta SNCA, ktorému bol certifikát vydaný a heslo pre zrušenie certifikátu, ktoré bolo uvedené v „Protokole o odovzdaní a prevzatí certifikátu“.

Ak žiadateľ o zrušenie certifikátu nedostane spätne, elektronickou formou, od registračného operátora RA SNCA odpoveď o prijatí a akceptovaní jeho žiadosti do 24 hodín od podania žiadosti, považuje svoju žiadosť za nedoručenú na registračné miesto RA SNCA a musí opätovne požiadať o zrušenie certifikátu alebo využiť inú možnosť podania žiadosti o zrušenie.

Listovou zásielkou sa podáva žiadosť o zrušenie certifikátu na poštovú adresu registračného miesta RA SNCA, ktoré mu vydalo certifikát.

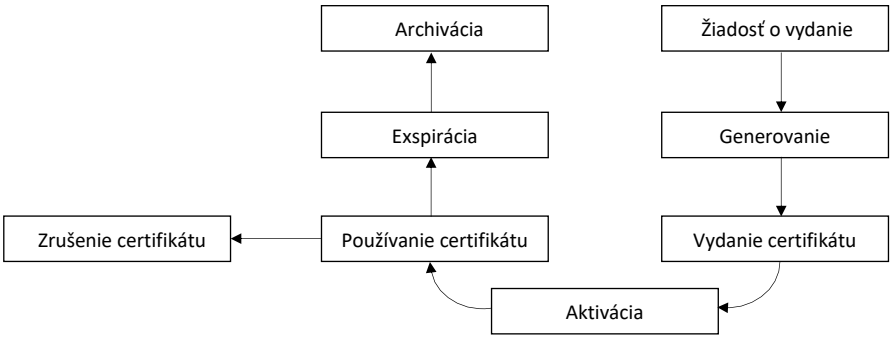
„Žiadosť o zrušenie certifikátu“, musí byť podaná výlučne písomnou formou – listom a musí byť podpísaná držiteľom certifikátu alebo nadriadeným držiteľa certifikátu. Písomná žiadosť, doručená formou listovej zásielky na registračné miesto RA SNCA, musí obsahovať nasledujúce údaje: typ certifikátu, sériové číslo certifikátu, celé občianske meno a priezvisko klienta SNCA, ktorému bol certifikát vydaný a heslo pre zrušenie certifikátu, ktoré bolo uvedené v „Protokole o odovzdaní a prevzatí certifikátu“. Podpis držiteľa certifikátu na žiadosti o zrušenie certifikátu musí byť totožný s podpisom v „Protokole o odovzdaní a prevzatí certifikátu“.

Telefonicky sa podáva žiadosť o zrušenie certifikátu na zverejnený telefonický kontakt registračného miesta RA SNCA, ktoré mu vydalo certifikát.

Žiadateľ o zrušenie certifikátu musí preukázať vlastníctvo certifikátu, o ktorého zrušenie žiada. V telefonickej žiadosti o zrušenie certifikátu, musí žiadateľ uviesť nasledujúce údaje: typ certifikátu, sériové číslo certifikátu, celé občianske meno a priezvisko klienta SNCA, ktorému bol certifikát vydaný, jeho identifikačné údaje a heslo pre zrušenie certifikátu, ktoré bolo uvedené v „Protokole o odovzdaní a prevzatí certifikátu“.

4 Prevádzkové požiadavky na životný cyklus certifikátov (Certificate life-cycle operational requirements)

V tejto kapitole je uvedený životný cyklus kvalifikovaného certifikátu (Certificate Management LifeCycle, CMLC). Životný cyklus kvalifikovaného certifikátu pozostáva z primárnych a sekundárnych stavov. Každý vydaný certifikát prechádza všetkými primárnymi stavmi, zatiaľ čo sekundárne stavy sú výnimočné.



Primárnymi stavmi sú:

- žiadosť o vydanie certifikátu,
- generovanie certifikátu,
- vydanie certifikátu,
- aktivácia certifikátu,
- používanie certifikátu,
- exspirácia certifikátu,
- archivácia certifikátu.

Sekundárnym stavom je zrušenie certifikátu.

Prevádzkovateľ SNCA využíva pri procese vydávania certifikátov asymetrický algoritmus RSA (minimálne 2048 bits) a hashovaciu funkciu SHA-256.

4.1 Žiadosť o vydanie certifikátu (Certificate application)

4.1.1 Žiadateľ o vydanie certifikátu (Who Can Submit a Certificate Application)

O vydanie certifikátu môže požiadať:

- držiteľ certifikátu (fyzická osoba, fyzická osoba, identifikovaná v spojení s právnickou osobou alebo s OVM),

- štatutárny zástupca alebo ním poverená osoba príslušnej organizačnej zložky právnickej osoby alebo OVM,
- autorizovaný zástupca SNCA.

4.1.2 Registračný proces a zodpovednosti (Enrollment process and responsibilities)

Žiadateľ o vydanie certifikátu podáva vyplnenú žiadosť o vydanie certifikátu - „Žiadosť o poskytovanie kvalifikovaných dôveryhodných služieb“.

Žiadosť o vydanie certifikátu je možné podať:

- písomnou formou, osobne (fyzicky) na registračnom mieste RA SNCA,
- elektronickou formou do elektronickej schránky NASES, zriadenej na Ústrednom portáli verejnej správy prostredníctvom služby „Všeobecná agenda“,
- formou žiadosti v naskenovanej podobe na e-mailovú adresu: snca@nases.gov.sk,
- listovou zásielkou, doručenou na poštovú adresu NASES,

Registračný proces, bude vykonaný počas štandardných, zverejnených, úradných hodín príslušného registračného miesta RA SNCA alebo na základe ďalšieho usmernenia činnosti RA SNCA, v rozsahu a podľa potrieb príslušnej zložky OVM, ktorá registračné miesto RA SNCA zriadila. Iniciálnu registráciu so žiadateľom o vydanie certifikátu na registračnom mieste RA SNCA vykonáva registračný operátor RA SNCA.

Registračný operátor RA SNCA je povinný každému žiadateľovi o vydanie certifikátu podať všetky potrebné informácie a zodpovedá najmä za to, že pred samotným procesom iniciálnej registrácie, budú žiadateľovi poskytnuté nasledovné informácie a dokumentácia (žiadateľovi bude poskytnutá aj informácia – odkaz na verejne dostupnú internetovú stránku s uvedenými informáciami a dokumentáciou):

- dokumentácia v rozsahu:
  - certifikačný poriadok, ktorý obsahuje najmä informácie, pre koho a za akých podmienok SNCA poskytuje akreditované certifikačné služby, práva a povinnosti používateľov služieb SNCA, vzory žiadostí o poskytnutie služby, pravidlá používania a pravidlá pre zrušenie kvalifikovaných certifikátov,
  - technické špecifikácie, formáty, normy a štandardy, používané pri vykonávaní akreditovaných činností v SNCA,
  - zoznam poskytovaných dôveryhodných služieb SNCA,
  - vzor „Žiadosti o poskytovanie kvalifikovaných dôveryhodných služieb“
  - vzor „Zmluvy o vydaní a používaní kvalifikovaného certifikátu“,
- informácia o spôsobe overenia totožnosti žiadateľa,
- informácia, kde sú zverejnené informácie o akreditácii SNCA,
- informácia, kde sú zverejnené informácie o vydaných kvalifikovaných certifikátoch,
- informácia, kde sú zverejnené zoznamy zrušených kvalifikovaných certifikátov,

- kontaktná adresa, telefónne číslo a úradné hodiny registračného miesta RA SNCA,
- informácia, kde žiadateľ bude podrobne a zrozumiteľne informovaný o bezpečnostnej politike a o pravidlách na poskytovanie dôveryhodných služieb SNCA.

Pre zahájenie procesu vydania kvalifikovaného certifikátu je potrebné, aby sa žiadateľ o vydanie certifikátu osobne dostavil na registračné miesto RA SNCA a v prípade žiadateľa, ktorý je zamestnancom OVM je potrebné, aby doručil na príslušné registračné miesto RA SNCA tzv. „Formálnu žiadosť o vydanie certifikátu“, ktorá musí byť podpísaná nadriadeným žiadateľa a ktorá slúži na preukázanie súhlasu príslušnej organizačnej zložky OVM s vydaním kvalifikovaného certifikátu klientovi SNCA. Formu tejto žiadosti určuje konkrétna organizačná zložka OVM.

V prípade, že žiadateľ o vydanie certifikátu je oboznámený s potrebnými dokumentami a súhlasí so znením „Zmluvy o vydaní a používaní kvalifikovaného certifikátu“, ktorej súčasťou je aj vyhlásenie žiadateľa - „Súhlas so spracovaním osobných údajov“, registračný operátor RA SNCA vykoná proces iniciálnej registrácie.

Registračný operátor RA SNCA predloží žiadateľovi o vydanie certifikátu na podpis „Zmluvu o vydaní a používaní kvalifikovaného certifikátu“, ktorej súčasťou je aj vyhlásenie žiadateľa - „Súhlas so spracovaním osobných údajov“. Externá OVM RA SNCA vyhotovuje štyri rovnopisy tejto zmluvy, z ktorých jeden rovnopis odovzdá žiadateľovi o vydanie certifikátu, jeden si ponechá externá OVM RA SNCA a dva rovnopisy sú určené pre potreby prevádzkovateľa SNCA. Interná RA SNCA vyhotovuje tri rovnopisy tejto zmluvy, z ktorých jeden rovnopis odovzdá žiadateľovi o vydanie certifikátu a dva rovnopisy sú určené pre potreby prevádzkovateľa SNCA. Zmluvu za RA SNCA podpisuje registračný operátor RA SNCA.

Po podpísaní „Zmluvy o vydaní a používaní kvalifikovaného certifikátu“ žiadateľom o vydanie certifikátu, registračný operátor RA SNCA realizuje nasledovné kroky:

- počas procesu iniciálnej registrácie spracuje „Záznam z procedúry vydania kvalifikovaného certifikátu“. „Záznam z procedúry vydania kvalifikovaného certifikátu“ sa neodovzdáva žiadateľovi o vydanie certifikátu. Externá OVM RA SNCA vyhotovuje tri rovnopisy tohto záznamu, z ktorých jeden rovnopis si ponechá externá OVM RA SNCA a dva rovnopisy sú určené pre potreby prevádzkovateľa SNCA. Interná RA SNCA vyhotovuje dva rovnopisy tohto záznamu, ktoré sú určené pre potreby prevádzkovateľa SNCA.
- začne spracovávať „Žiadosť o poskytovanie kvalifikovaných dôveryhodných služieb“. Externá OVM RA SNCA vyhotovuje štyri rovnopisy tejto žiadosti, z ktorých jeden rovnopis odovzdá žiadateľovi o vydanie certifikátu, jeden si ponechá externá OVM RA SNCA a dva rovnopisy sú určené pre potreby prevádzkovateľa SNCA. Interná RA SNCA vyhotovuje tri rovnopisy tejto žiadosti, z ktorých jeden rovnopis odovzdá žiadateľovi o vydanie certifikátu a dva rovnopisy sú určené pre potreby prevádzkovateľa SNCA.
- pokiaľ nenašiel žiadne nezrovnalosti v predložených dokladoch a údajoch, ktoré majú byť zapísané do certifikátu, vykoná konfiguráciu a personalizáciu technického prostriedku, určeného pre uloženie a distribúciu kvalifikovaného certifikátu,

- vygeneruje alebo prevezme od žiadateľa o vydanie certifikátu elektronickú žiadosť o vydanie certifikátu vo formáte PKCS#10, označí a uloží ju na prenosné médium,
- dokončí spracovanie „Žiadosti o poskytovanie kvalifikovaných dôveryhodných služieb“ a v prípade osobného podania žiadosti na registračnom mieste RA SNCA, predloží žiadosť žiadateľovi na podpis,
- vydá kvalifikovaný certifikát,
- uloží kvalifikovaný certifikát na prostriedok, určený pre uloženie a distribúciu kvalifikovaného certifikátu,
- vyhotoví a predloží na podpis žiadateľovi o vydanie certifikátu „Protokol o odovzdaní a prevzatí certifikátu“. Externá OVM RA SNCA vyhotovuje štyri rovnopisy tohto protokolu, z ktorých jeden rovnopis odovzdá žiadateľovi o vydanie certifikátu , jeden si ponechá externá OVM RA SNCA a dva rovnopisy sú určené pre potreby prevádzkovateľa SNCA. Interná RA SNCA vyhotovuje tri rovnopisy tohto protokolu, z ktorých jeden rovnopis odovzdá žiadateľovi o vydanie certifikátu a dva rovnopisy sú určené pre potreby prevádzkovateľa SNCA.
- registračný operátor RA SNCA odovzdá žiadateľovi o vydanie certifikátu kvalifikovaný certifikát, uložený na prostriedku, ktorý je určený na jeho distribúciu.

Po vydaní kvalifikovaného certifikátu, registračný operátor RA SNCA vykoná zápis do „Denníka činností registračnej autority“.

V prípade, že niektorá z podmienok registračného procesu nie je splnená, registračný operátor RA SNCA má právo tento proces ukončiť. Následne informuje žiadateľa o vydanie certifikátu o dôvode zamietnutia žiadosti o vydanie kvalifikovaného certifikátu, prípadne o možnosti pokračovania v procese vydania kvalifikovaného certifikátu. Dôvod zamietnutia žiadosti o vydanie kvalifikovaného certifikátu, bude žiadateľovi oznámený v písomnej forme nasledovným spôsobom - registračný operátor RA SNCA vyplní a odovzdá žiadateľovi formulár „Zamietnutie žiadosti o vydanie kvalifikovaného certifikátu“. V prípade, že žiadateľ odmietne podpísať „Zmluvu o vydaní a používaní kvalifikovaného certifikátu“, poskytnúť potrebné údaje alebo odmietne pokračovať v registračnom procese, registračný operátor RA SNCA ukončí registračný proces spracovaním „Protokolu o ukončení registračného procesu“, ktorý predloží na podpis žiadateľovi. Z oboch uvedených dokumentov, „Zamietnutie žiadosti o vydanie KC“ a „Protokol o ukončení registračného procesu“, externá OVM RA SNCA vyhotovuje štyri rovnopisy, z ktorých jeden rovnopis odovzdá žiadateľovi o vydanie certifikátu, jeden si ponechá externá OVM RA SNCA a dva rovnopisy sú určené pre potreby prevádzkovateľa SNCA. Interná RA SNCA vyhotovuje z oboch dokumentov tri rovnopisy, z ktorých jeden rovnopis odovzdá žiadateľovi o vydanie certifikátu a dva rovnopisy sú určené pre potreby prevádzkovateľa SNCA.

Žiadateľ o vydanie certifikátu je povinný prevziať vydaný kvalifikovaný certifikát. Ak ho odmietne prevziať, musí požiadať o jeho zrušenie v súlade s týmito CPS. V prípade, ak žiadateľ o vydanie certifikátu odmietne prevziať vydaný kvalifikovaný certifikát a ani nepožiada o jeho zrušenie, tak o jeho zrušenie požiada okamžite registračný operátor RA SNCA.

Prevzatím kvalifikovaného certifikátu žiadateľ o vydanie certifikátu:

- potvrdzuje a zaručuje, že informácie, uvedené vo vydanom certifikáte sú platné a sú v súlade s „Formálnou žiadosťou o vydanie certifikátu“,
- potvrdzuje, že žiadny neoprávnený subjekt nevlastní alebo nemá prístup k príslušnému súkromnému kľúču z kľúčového páru, na ktorého verejný kľúč bol vydaný preberaný certifikát,
- potvrdzuje, že sú mu známe práva a povinnosti držiteľa certifikátu, ustanovené v CP a tieto práva a povinnosti akceptuje,
- berie na vedomie, že za škodu spôsobenú porušením povinností, zodpovedá držiteľ certifikátu.

V prípade vydania kvalifikovaného certifikátu pre autentifikáciu webového sídla je potrebné, aby si žiadateľ o vydanie certifikátu vygeneroval kryptografické kľúče odporúčanej veľkosti a pripravil si elektronickú žiadosť o vydanie kvalifikovaného certifikátu vo formáte PKCS#10. Elektronickú žiadosť o vydanie kvalifikovaného certifikátu vo formáte PKCS#10 je potrebné zaslať vopred na kontrolu na registračné miesto RA SNCA.

4.2 Spracovanie žiadosti o certifikáciu (Certificate application processing)

4.2.1 Výkon identifikácie a autentizácie (Performing identification and authentication functions)

Viď relevantné časti bodu 3.2 týchto CPS.

4.2.2 Schválenie alebo zamietnutie žiadostí o vydanie certifikátu (Approval or rejection of certificate applications)

Viď relevantné časti bodu 4.1.2 týchto CPS.

4.2.3 Časová náročnosť procesu spracovania žiadosti o vydanie certifikátu (Time to process certificate applications)

Časová náročnosť procesu spracovania žiadosti o vydanie certifikátu závisí od typu certifikátu. V priemere sa časová náročnosť pohybuje v rozmedzí 15 až 30 minút.

4.3 Vydanie certifikátu (Certificate issuance)

Po prijatí žiadosti o vydanie certifikátu, registračný operátor RA SNCA pri kladnom výsledku preverenia požadovaných náležitostí žiadosti, jej správnosti a správnosti údajov, obsiahnutých v tele žiadosti, realizuje nasledovné kroky:

- generuje proces vydania certifikátu na SNCA,
- uloží vydaný certifikát z SNCA,
- nahrá kvalifikovaný certifikát na prostriedok, certifikovaný ako QSCD alebo iné médium,
- dá žiadateľovi o vydanie certifikátu podpísať „Protokol o odovzdaní a prevzatí kvalifikovaného certifikátu“.

4.3.1 Činnosti CA počas vydávania certifikátu (CA actions during certificate issuance)

Viď relevantné časti bodu 4.1.2 týchto CPS.

4.3.2 Notifikácia žiadateľa o vydaní certifikátu (Notification to subscriber by the CA of issuance of certificate)

Certifikáty SNCA

Ak sa jedná o certifikát SNCA, notifikácia o vydaní certifikátu sa nezasiela.

Certifikáty obslužného personálu

Notifikáciu o vydaní certifikátu obslužného personálu zasiela obslužnému personálu operátor CA.

Kvalifikované certifikáty

Kvalifikovaný certifikát pre elektronický podpis.

Ak sa jedná o kvalifikovaný certifikát pre elektronický podpis, žiadateľ je informovaný okamžite registračným operátorom RA SNCA počas registračného procesu.

Kvalifikovaný certifikát pre elektronickú pečať.

V prípade, že sa jedná o kvalifikovaný certifikát pre elektronickú pečať, žiadateľa o vydaní certifikátu informuje registračný operátor RA SNCA ihneď po vydaní kvalifikovaného certifikátu.

Certifikáty serverov časových pečiatok

Notifikáciu o vydaní certifikátu servera časových pečiatok zasiela žiadateľovi registračný operátor RA SNCA.

Kvalifikované certifikáty pre autentifikáciu webového sídla

Notifikáciu o vydaní kvalifikovaného certifikátu pre autentifikáciu webového sídla, zasiela žiadateľovi registračný operátor RA SNCA.

4.4 Akceptácia certifikátu (Certificate acceptance)

4.4.1 Ustanovenie akceptácie certifikátu (Conduct constituting certificate acceptance)

Viď relevantné časti bodu 4.1.2 týchto CPS.

4.4.2 Publikácia certifikátu (Publication of the certificate by the CA)

Certifikáty SNCA

Certifikáty SNCA sa publikujú na dedikovanej internetovej stránke SNCA na adrese:

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

Certifikáty obslužného personálu

Certifikáty obslužného personálu SNCA sa nepublikujú.

Kvalifikované certifikáty

Kvalifikované certifikáty vydávané SNCA sa nepublikujú.

Certifikáty serverov časových pečiatok

Certifikáty serverov časových pečiatok, vydávané SNCA, sa publikujú na dedikovanej internetovej stránke webového sídla SNCA na adrese:

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

Kvalifikované certifikáty pre autentifikáciu webového sídla

Kvalifikované certifikáty pre autentifikáciu webového sídla sa nezverejňujú.

4.4.3 Notifikácia iných entít o vydaní certifikátu (Notification of certificate issuance by the CA to other entities)

Notifikáciu iných entít o vydaní certifikátu SNCA nevykonáva.

4.5 Kľúčový pár a použitie certifikátu (Key pair and certificate usage)

4.5.1 Súkromný kľúč žiadateľa a použitie certifikátu (Subscriber private key and certificate usage)

Certifikáty SNCA

Súkromný kľúč, prislúchajúci k certifikátu, je uložený v HSM module Thales nShieldConnect F3 500.

Algoritmus a dĺžka kľúča: RSA (4096 bits)

Použitie certifikátu: keyCertSign, cRLSign

Certifikáty obslužného personálu

Súkromný kľúč, prislúchajúci k certifikátu, sa ukladá na čipovú kartu Siemens ver. CardOS V4.4.

Algoritmus a dĺžka kľúča: RSA (minimálne 2048 bits)

Použitie certifikátu: digitalSignature, client Authenticatin

Kvalifikované certifikáty

Kvalifikovaný certifikát pre elektronický podpis:

Algoritmus a dĺžka kľúča: RSA (minimálne 2048 bits)

Použitie certifikátu: nonRepudiation

Kvalifikovaný certifikát pre elektronickú pečať:

Algoritmus a dĺžka kľúča: RSA (minimálne 2048 bits)

Použitie certifikátu: nonRepudiation

Certifikáty serverov časových pečiatok

Algoritmus a dĺžka kľúča: RSA (minimálne 2048 bits)

Použitie certifikátu: nonRepudiation

Rozšírené použitie certifikátu: timeStamping

Kvalifikované certifikáty pre autentifikáciu webového sídla

Algoritmus a dĺžka kľúča: RSA (minimálne 2048 bits)

Použitie certifikátu: nonRepudiation

Rozšírené použitie certifikátu: websiteAuthentication

4.5.2 Verejný kľúč spoliehajúcej sa strany a použitie certifikátu (Relying party public key and certificate usage)

Spoliehajúcou sa stranou je entita, ktorá tým, že používa cudzí certifikát na overenie integrity elektronicky podpísanej správy alebo na ustanovenie bezpečnej komunikácie s držiteľom certifikátu, sa spolieha na platnosť väzby držiteľa certifikátu s daným verejným kľúčom.

Strana spoliehajúca sa na certifikát musí:

- použiť informáciu z certifikátu na určenie vhodnosti certifikátu na dané použitie,
- získať z bezpečného zdroja certifikát a overiť hash tohto certifikátu,
- overiť certifikačnú cestu, ktorej je certifikát súčasťou,
- overiť platnosť certifikátu.

4.6 Obnova certifikátu – bez generovania nového kľúčového páru (Certificate renewal)

SNCA nepodporuje obnovu certifikátu bez generovania nového kľúčového páru.

4.6.1 Okolnosti pre obnovu certifikátu (Circumstance for certificate renewal)

SNCA nepodporuje obnovu certifikátu bez generovania nového kľúčového páru.

4.6.2 Žiadatelia o obnovu certifikátu (Who may request renewal)

SNCA nepodporuje obnovu certifikátu bez generovania nového kľúčového páru.

4.6.3 Spracovanie žiadostí o vydanie obnoveného certifikátu (Processing certificate renewal requests)

SNCA nepodporuje obnovu certifikátu bez generovania nového kľúčového páru.

4.6.4 Notifikácia žiadateľa o vydaní nového certifikátu (Notification of new certificate issuance to subscriber)

SNCA nepodporuje obnovu certifikátu bez generovania nového kľúčového páru.

4.6.5 Ustanovenie akceptácie obnoveného certifikátu certifikátu (Conduct constituting acceptance of a renewal certificate)

SNCA nepodporuje obnovu certifikátu bez generovania nového kľúčového páru.

4.6.6 Publikácia obnoveného certifikátu (Publication of the renewal certificate by the CA)

SNCA nepodporuje obnovu certifikátu bez generovania nového kľúčového páru.

4.6.7 Notifikácia iných entít o vydaní certifikátu (Notification of certificate issuance by the CA to other entities)

SNCA nepodporuje obnovu certifikátu bez generovania nového kľúčového páru.

4.7 Vydanie nového certifikátu s generovaním nového kľúčového páru (Certificate re-key)

Pre tento spôsob vydávania certifikátu platia rovnaké požiadavky, ako pre proces iniciálneho overenia identity, podľa postupu uvedeného v bode 3.2 týchto CPS.

4.7.1 Okolnosti pre vydanie nového certifikátu (Circumstance for certificate re-key)

Pre tento spôsob vydávania certifikátu platia rovnaké požiadavky, ako pre proces iniciálneho overenia identity, podľa postupu uvedeného v bode 3.2 týchto CPS.

Minimálne musia byť splnené nasledovné požiadavky:

- skončila platnosť pôvodného kvalifikovaného certifikátu, resp. tento bol zrušený,
- položky žiadosti o vydanie kvalifikovaného certifikátu sú zhodné s údajmi kvalifikovaného certifikátu, ktorý je nahrádzaný,
- boli vygenerované nové kryptografické kľúče a pripravená, podpísaná nová žiadosť o vydanie certifikátu.

4.7.2 Žiadatelia o vygenerovanie nového verejného kľúča a certifikátu (Who may request certification of a new public key)

Pre tento spôsob vydávania certifikátu platia rovnaké požiadavky, ako pre proces iniciálneho overenia identity, podľa postupu uvedeného v bode 3.2 týchto CPS.

4.7.3 Spracovanie žiadostí o vydanie nového certifikátu (Processing certificate re-keying requests)

Pre tento spôsob vydávania certifikátu platia rovnaké požiadavky, ako pre proces iniciálneho overenia identity, podľa postupu uvedeného v bode 3.2 týchto CPS.

4.7.4 Notifikácia žiadateľa o vydaní nového certifikátu (Notification of new certificate issuance to subscriber)

Pre tento spôsob vydávania certifikátu platia rovnaké požiadavky, ako pre proces iniciálneho overenia identity, podľa postupu uvedeného v bode 3.2 týchto CPS.

4.7.5 Ustanovenie akceptácie nového certifikátu certifikátu (Conduct constituting acceptance of a re-keyed certificate)

Pre tento spôsob vydávania certifikátu platia rovnaké požiadavky, ako pre proces iniciálneho overenia identity, podľa postupu uvedeného v bode 3.2 týchto CPS.

4.7.6 Publikácia nového certifikátu (Publication of the re-keyed certificate by the CA)

Pre tento spôsob vydávania certifikátu platia rovnaké požiadavky, ako pre proces iniciálneho overenia identity, podľa postupu uvedeného v bode 3.2 týchto CPS.

4.7.7 Notifikácia iných entít o vydaní certifikátu (Notification of certificate issuance by the CA to other entities)

Pre tento spôsob vydávania certifikátu platia rovnaké požiadavky, ako pre proces iniciálneho overenia identity, podľa postupu uvedeného v bode 3.2 týchto CPS.

4.8 Modifikácia certifikátu (Certificate modification)

SNCA nepodporuje modifikáciu certifikátu bez generovania nového kľúčového páru.

4.8.1 Okolnosti pre modifikáciu certifikátu (Circumstance for certificate modification)

SNCA nepodporuje modifikáciu certifikátu bez generovania nového kľúčového páru.

4.8.2 Žiadatelia o modifikáciu certifikátu (Who may request certificate modification)

SNCA nepodporuje modifikáciu certifikátu bez generovania nového kľúčového páru.

4.8.3 Spracovanie žiadostí o modifikáciu certifikátu (Processing certificate modification requests)

SNCA nepodporuje modifikáciu certifikátu bez generovania nového kľúčového páru.

4.8.4 Notifikácia žiadateľa o vydaní nového certifikátu (Notification of new certificate issuance to subscriber)

SNCA nepodporuje modifikáciu certifikátu bez generovania nového kľúčového páru.

4.8.5 Ustanovenie akceptácie modifikovaného certifikátu (Conduct constituting acceptance of modified certificate)

SNCA nepodporuje modifikáciu certifikátu bez generovania nového kľúčového páru.

4.8.6 Publikácia modifikovaného certifikátu (Publication of the modified certificate by the CA)

SNCA nepodporuje modifikáciu certifikátu bez generovania nového kľúčového páru.

4.8.7 Notifikácia iných entít o vydaní certifikátu (Notification of certificate issuance by the CA to other entities)

SNCA nepodporuje modifikáciu certifikátu bez generovania nového kľúčového páru.

4.9 Zrušenie a pozastavenie platnosti certifikátu (Certificate revocation and suspension)

4.9.1 Okolnosti pre zrušenie certifikátu (Circumstances for revocation)

Okolnosťami pre zrušenie certifikátu sú:

- súkromný kľúč klienta SNCA, patriaci k verejnému kľúču, uvedenému v certifikáte klienta SNCA, bol ukradnutý, stratený, pozmenený alebo iným spôsobom kompromitovaný,
- klient SNCA závažne porušil prevádzkové požiadavky, identifikované v príslušných zmluvách alebo v CP,
- certifikát klienta SNCA bol vydaný na základe nepravdivých údajov,
- prišlo k zmene identifikačných údajov alebo atribútov v certifikáte klienta SNCA pred uplynutím doby platnosti certifikátu,
- držiteľ certifikátu zomrel, prípadne už nepracuje v tej organizačnej zložke právnickej osoby alebo OVM, s ktorou má prevádzkovateľ SNCA uzatvorenú zmluvu o poskytovaní dôveryhodných služieb,
- klient SNCA odmietol prevziať pre neho vydaný certifikát a odmietol požiadať o jeho zrušenie,
- boli zrušené vydané certifikáty SNCA alebo KCA (v tomto prípade sa nevypĺňa „Žiadosť o zrušenie certifikátu“ jednotlivo pre každého klienta SNCA, ale súhrnný príkaz na zrušenie všetkých certifikátov. Túto činnosť vykonáva výlučne operátor CA na písomný príkaz bezpečnostného správcu SNCA),
- prišlo k úmyselnému zneužitiu kľúčov a certifikátov SNCA autorizovanou osobou alebo neautorizovanou osobou (v tomto prípade sa nevypĺňa „Žiadosť o zrušenie certifikátu“ jednotlivo pre každého kienta SNCA, ale súhrnný príkaz na zrušenie všetkých certifikátov. Túto činnosť vykonáva výlučne operátor CA na písomný príkaz bezpečnostného správcu SNCA),

- zrušenie certifikátu klienta SNCA nariadil súd. Zrušenie certifikátu bude realizované za predpokladu doručenia právoplatného rozhodnutia súdu o zrušení certifikátu, prípadne písomného rozhodnutia súdu o jeho zrušení,
- zrušenie certifikátov SNCA nariadil súd. Zrušenie certifikátov SNCA bude realizované za predpokladu doručenia právoplatného rozhodnutia súdu o zrušení certifikátov, prípadne písomného rozhodnutia súdu o ich zrušení (v tomto prípade sa nevypĺňa „Žiadosť o zrušenie certifikátu“ jednotlivo pre každého klienta SNCA, ale súhrnný príkaz na zrušenie všetkých certifikátov. Túto činnosť vykonáva výlučne operátor CA na písomný príkaz bezpečnostného správcu SNCA).

4.9.2 Žiadatelia o zrušenie certifikátu (Who can request revocation)

Viď bod 3.4 týchto CPS.

4.9.3 Procedúra spracovania žiadosti o zrušenie certifikátu (Procedure for revocation request)

Proces zrušenia certifikátu je iniciovaný prijatím „Žiadosti o zrušenie certifikátu“ a po potvrdení hesla pre zrušenie certifikátu. Po prijatí žiadosti o zrušenie certifikátu registračný operátor RA SNCA realizuje nasledovné kroky:

- formálne skontroluje správnosť prijatej „Žiadosti o zrušenie kvalifikovaného certifikátu“,
- overí autenticitu predkladateľa žiadosti o zrušenie certifikátu,
- skontroluje oprávnenosť predkladateľa požadovať zrušenie certifikátu,
- posúdi žiadosť o zrušenie certifikátu (akceptovanie – neakceptovanie),
- po akceptovaní žiadosti o zrušenie certifikátu, spracuje žiadosť o zrušenie certifikátu,
- spustí proces zrušenia certifikátu,
- spracuje „Protokol o spracovaní žiadosti o zrušenie kvalifikovaného certifikátu“.

Po ukončení procesu zrušenia certifikátu, registračný operátor RA SNCA vykoná zápis do „Denníka činností registračnej autority“.

Následne písomne informuje klienta SNCA na kontaktné miesto, ktoré uviedol v „Žiadosti o zrušenie kvalifikovaného certifikátu“.

Podľa aktuálneho termínu publikovania CRL skontroluje zrušenie daného kvalifikovaného certifikátu v CRL.

Ak „Žiadosť o zrušenie kvalifikovaného certifikátu“ nie je možné akceptovať, bude táto žiadosť zamietnutá. Registračný operátor RA SNCA následne informuje žiadateľa o dôvodoch zamietnutia žiadosti a to rovnakým spôsobom, akým bola podaná žiadosť o zrušenie certifikátu. V prípade, že žiadateľovi o zrušenie certifikátu bola jeho „Žiadosť o zrušenie

kvalifikovaného certifikátu“ zamietnutá, opätovne bude môcť takýto žiadateľ požiadať o zrušenie certifikátu výlučne osobne na registračnom mieste RA SNCA.

4.9.4 Grace period žiadosti o zrušenie certifikátu (Revocation request grace period)

SNCA nestanovuje grace period na predloženie žiadosti o zrušenie certifikátu. Ak nastane niektorý z prípadov podľa bodu 4.9.1 týchto CPS, každý klient SNCA je povinný bezodkladne požiadať RA SNCA o zrušenie vydaného certifikátu.

4.9.5 Čas, v rámci ktorého musí CA spracovať žiadosť o zrušenie certifikátu (Time within which CA must process the revocation request)

SNCA spracuje žiadosť o zrušenie certifikátu v čo najkratšom možnom čase, najneskôr však do 24 hodín od jej prijatia.

4.9.6 Požiadavka na kontrolu zrušenia certifikátu pre spoliehajúce sa strany (Revocation checking requirement for relying parties)

Viď bod 4.5.2 týchto CPS.

4.9.7 Frekvencia vydávania zoznamu CRL (CRL issuance frequency (if applicable))

Nový zoznam CRL vydáva SNCA zvyčajne každé štyri hodiny, najmenej však raz za 24 hodín. Nový zoznam CRL vydá SNCA vždy po zrušení certifikátu.

4.9.8 Maximálna latencia platná pre zo znamy CRL (Maximum latency for CRLs (if applicable))

SNCA robí maximum pre okamžité publikovanie vydaného zoznamu CRL ihneď po jeho vydaní. Vzhľadom na pomerne komplikované technologické riešenie však istá latencia medzi vydaním a publikovaním nastáva, zvyčajne ale nepresiahne interval piatich minút.

4.9.9 Dostupnosť on-line kontroly zrušenia/stavu certifikátu (On-line revocation/status checking availability)

SNCA neposkytuje on-line kontrolu zrušenia/stavu certifikátu.

4.9.10 Požiadavky na on-line kontrolu zrušenia certifikátu (On-line revocation checking requirements)

SNCA neposkytuje on-line kontrolu zrušenia/stavu certifikátu.

4.9.11 Iné dostupné formy oznámení o zrušení certifikátu (Other forms of revocation advertisements available)

SNCA využíva na oznámenie o zrušení certifikátu mechanizmus publikovania zoznamov CRL, iné formy oznámenia o zrušení certifikátu nie sú podporované.

4.9.12 Špeciálne požiadavky na proces zrušenia certifikátu pre prípad kompromitácie súkromného kľúča (Special requirements re key compromise)

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

4.9.13 Okolnosti pre pozastavenie platnosti certifikátu (Circumstances for suspension)

SNCA nepodporuje inštitút pozastavenia platnosti certifikátu.

4.9.14 Žiadatelia o pozastavenie platnosti certifikátu (Who can request suspension)

SNCA nepodporuje inštitút pozastavenia platnosti certifikátu.

4.9.15 Procedúra spracovania žiadosti o pozastavenie platnosti certifikátu (Procedure for suspension request)

SNCA nepodporuje inštitút pozastavenia platnosti certifikátu.

4.9.16 Limity na dobu pozastavenia platnosti certifikátu (Limits on suspension period)

SNCA nepodporuje inštitút pozastavenia platnosti certifikátu.

4.10 Služby zisťovania stavu certifikátu (Certificate status services)

4.10.1 Prevádzkové charakteristiky (Operational characteristics)

Služby zisťovania stavu certifikátu SNCA poskytuje nasledovne:

- prostredníctvom dedikovanej internetovej stránky webového sídla SNCA:
  http://ep.nbu.gov.sk/snca/crl.html
- prostredníctvom priamych linkov, uvedených v certifikátoch vydávaných SNCA:
  http://ep.nbu.gov.sk/snca/crls2/snca2.crl
  http://ep.nbu.gov.sk/snca/crls3/snca3.crl

- prostredníctvom archívu všetkých zoznamov CRL, vydaných SNCA:

  http://ep.nbu.gov.sk/snca/archive/
  http://ep.nbu.gov.sk/snca/archive2/
  http://ep.nbu.gov.sk/snca/archive3/

4.10.2 Dostupnosť služby (Service availability)

Služba zisťovania stavu certifikátu je dostupná 24 hodín denne, 7 dní v týždni, 365 dní v roku. Výnimku môžu tvoriť:

- plánovaná údržba infraštruktúry SNCA,
- neočakávané závažné technické problémy.

4.10.3 Iné vlastnosti (Optional features)

Nie sú podporované.

4.11 Ukončenie subskripcie (End of subscription)

Ukončenie subskripcie môže nastať jedným z nasledovných spôsobov:

- vypovedanie „Zmluvy o poskytovaní kvalifikovaných dôveryhodných služieb“ medzi prevádzkovateľom SNCA a príslušnou organizačnou zložkou OVM,
- vypovedanie „Zmluvy o vydaní a používaní kvalifikovaného certifikátu“ s klientom SNCA,
- zrušenie certifikátu.

4.12 Uchovávanie a obnova kľúča (Key escrow and recovery)

4.12.1 Politika a postupy pre key escrow (Key escrow and recovery policy and practices)

SNCA nepodporuje mechanizmus key escrow.

4.12.2 Politika a postupy pre session key encapsulation (Session key encapsulation and recovery policy and practices)

SNCA nepodporuje mechanizmus session key encapsulation.

5 Fyzické, procedurálne a personálne bezpečnostné opatrenia (Facility, management, and operational controls)

5.1 Opatrenia fyzickej bezpečnosti (Physical controls)

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 len „vyhláška NBÚ č. 336/2004 Z. z.“).

5.1.1 Lokalizácia a konštrukcia prevádzkových priestorov (Site location and construction)

Všetky prevádzkované systémy a zariadenia SNCA sú umiestnené v bezpečných priestoroch, chránených pred neautorizovaným prístupom nepovolaných osôb, pred živelnými pohromami a haváriami v inžinierskych sieťach.

5.1.2 Fyzický prístup (Physical access)

Bezpečnostné opatrenia na fyzickú a objektovú bezpečnosť, spĺňajú požiadavky vyhlášky NBÚ č. 336/2004 Z. z.. Prístup do priestorov umiestnenia prevádzkovaného systému SNCA, je riadený prísnou bezpečnostnou politikou a pravidelne auditovanými procedúrami. Agentúra má pripravené spôsoby a postupy na ochranu svojich počítačových systémov, údajov a archívov proti neoprávnenej manipulácii, krádeži a prezradeniu.

5.1.3 Napájanie a vzduchotechnika (Power and air conditioning)

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

5.1.4 Možné vystavenia vode (Water exposures)

Priestory umiestnenia systému SNCA sú chránené proti nebezpečenstvu pôsobenia vody.

5.1.5 Predchádzanie požiarom a ochrana pred požiarmi (Fire prevention and protection)

Agentúra využíva, na zabezpečenie ochrany priestorov umiestnenia systému SNCA, dymové a požiarne detektory.

5.1.6 Uchovávanie médií (Media storage)

Agentúra 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 Odpadové hospodárstvo (Waste disposal)

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

5.1.8 Záložné prevádzkové priestory (Off-site backup)

Okrem prevádzkových priestorov umiestnenia SNCA, disponuje agentúra záložnými prevádzkovými priestormi, určenými na ukladanie pravidelných záložných kópií a archívnych dát.

5.2 Procedurálne opatrenia (Procedural controls)

5.2.1 Dôveryhodné roly (Trusted roles)

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.

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),

Bezpečnostný správca SNCA

Hlavnou úlohou bezpečnostného správcu je prideľovanie rolí a prístupových práv v systémoch SNCA, odsúhlasovanie zmien v konfigurácii hardvérových a softvérových komponentov infraštruktúry SNCA, dohľad nad celkovou systémovou, sieťovou, fyzickou a objektovou bezpečnosťou infraštruktúry SNCA, analýza auditných logov, vypracovávanie a aktualizácia vrcholových dokumentov (CP, CPS), a pod..

Interný audítor SNCA

Interný audítor zabezpečuje nezávislý spôsob kontroly správy infraštruktúry PKI, overovanie auditných záznamov, overovanie dodržiavania súladu CP a CPS. Rola audítora nie je zlučiteľná s rolami, ktoré sa podieľajú na správe a obsluhe komponentov, t. j. administrátori a operátori.

Manažér pre správu politík - PMA manažér SNCA

Zodpovedá za administráciu a bezpečnostnú politiku prevádzkovanej PKI infraštruktúry SNCA (realizuje inštalácie, zmeny v konfigurácii PKI infraštruktúry) a revízie výsledkov auditov zhody. Zabezpečuje vydávanie technologických certifikátov pre vnútornú potrebu SNCA. Zabezpečuje zrušovanie certifikátov SNCA a ďalších certifikátov, vydávaných SNCA.

Administrátor SNCA

Zabezpečuje činnosti spojené so správou HSM modulov, ktoré vykonávajú jeden alebo dvaja operátori. Počet operátorov, ktorí sú potrební na vykonanie príslušnej činnosti, závisí od typu a úrovne bezpečnosti danej činnosti.

Systémový administrátor SNCA

Hlavnou úlohou systémového administrátora je správa, konfigurácia a údržba hardvérových a softvérových komponentov prevádzkovanej infraštruktúry SNCA.

Operátor RA SNCA (registračný operátor)

Operátor RA, ako pracovník registračného miesta RA SNCA, zabezpečuje overovanie identity klientov SNCA a odsúhlasovanie, resp. zamietnutie žiadostí o vydanie alebo zrušenie kvalifikovaných certifikátov klientov SNCA.

5.2.2 Počet pracovníkov vyžadovaných na vykonávanie činností (Number of persons required per task)

Zabezpečené v zmysle organizačného poriadku agentúry.

5.2.3 Identifikácia a autentizácia pre každú rolu (Identification and authentication for each role)

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

5.2.4 Nezlučiteľnosť rolí (Roles requiring separation of duties)

Zabezpečené v zmysle organizačného poriadku agentúry.

5.3 Personálne 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.

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

5.3.1 Požiadavky na kvalifikácie, skúsenosti a oprávnenia (Qualifications, experience, and clearance requirements)

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.

5.3.2 Procedúry preverovania osôb (Background check procedures)

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

5.3.3 Požiadavky na školenia personálu (Training requirements)

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 preškoľovanie personálu a jeho frekvencia (Retraining frequency and requirements)

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

5.3.5 Frekvencia a postupnosť rotácie rolí (Job rotation frequency and sequence)

Realizuje sa v zmysle organizačného poriadku agentúry.

5.3.6 Sankcie za neoprávnené činnosti (Sanctions for unauthorized actions)

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

5.3.7 Požiadavky na nezávislých dodávateľov (Independent contractor requirements)

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

Každý pracovník, zabezpečujúci zmluvné činnosti, má vo svojej pracovnej náplni pridelenú rolu na zabezpečenie činností a s tým súvisiacu bezpečnostnú rolu. Každý pracovník, zabezpečujúci zmluvné činnosti, musí byť preukázateľne poučený o svojich povinnostiach a bezpečnostných a pracovných postupoch, požadovaných pri plnení úloh, vyplývajúcich z jeho roly.

5.3.8 Dokumentácia poskytovaná pracovníkom (Documentation supplied to personnel)

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

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 Procedúry spojené s auditnými záznamami (Audit logging procedures)

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.

5.4.1 Typy zaznamenávaných udalostí (Types of events recorded)

V prevádzke SNCA sa zaznamenávajú tieto typy udalostí (záznamov):

- Žiadosti o vydanie kvalifikovaných certifikátov spolu s výsledkom preverenia žiadosti.
- Záznamy o odovzdaní kvalifikovaných certifikátov.
- Záznamy o odovzdaní následných kvalifikovaných certifikátov.
- Žiadosti o zrušenie kvalifikovaných certifikátov spolu s výsledkom preverenia žiadosti.
- Záznamy o zrušení kvalifikovaných certifikátov.
- Záznamy o vytváraní a zverejňovaní zoznamu zrušených certifikátov.
- Záznamy o manipulácii so súkromným kľúčom SNCA.
- Záznamy zmien konfigurácií a inštalácie systémov a aplikácií SNCA.
- Systémové a aplikačné logy komponentov SNCA.
- Hlásenia výskytu prípadných prevádzkových a bezpečnostných incidentov.
- Protokoly o riešení ohlásených bezpečnostných incidentov.

5.4.2 Frekvencia spracovania záznamov (Frequency of processing log)

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.

5.4.3 Doba uchovávania auditných záznamov (Retention period for audit log)

Záznamy priebežného dokumentovania kľúčových aktivít prevádzky systému SNCA, sú uchovávané minimálne tri roky. Ostatné prevádzkové záznamy, sa uchovávajú ako aktívne záznamy, po dobu jedného roku od ich vzniku. Po uplynutí definovanej doby aktívneho života sú záznamy preradené do archívu.

5.4.4 Ochrana auditných záznamov (Protection of audit log)

Prevádzkové záznamy, vedené v elektronickej forme, sú zálohované tak, aby nemohlo dôjsť k ich poškodeniu alebo k ich strate. Integrita prevádzkových 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 záznamy, vedené listinnou formou, sú spravované v režime, ktorý zabezpečí, aby nemohlo dôjsť k ich porušeniu, znehodnoteniu, alebo strate.

5.4.5 Procedúry zálohovania auditných záznamov (Audit log backup procedures)

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

5.4.6 Systém zberu auditných záznamov (Audit collection system (internal vs. external))

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, ktorý spôsobil udalosť (Notification to event-causing subject)

Neuplatňuje sa.

5.4.8 Posudzovania zraniteľností (Vulnerability assessments)

Podľa bodu 5.4.2.

5.5 Archivácia záznamov (Records archival)

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 (Types of records archived)

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;
- Certifikáty, vydané SNCA;
- Zoznamy zrušených certifikátov;
- Oficiálna korešpondencia;
- Dokumentácia programového vybavenia SNCA;
- Bezpečnostná dokumentácia SNCA;
- Inštalačné média a popisy konfiguračných súborov programového vybavenia SNCA.

Každý archívny záznam je opatrený časovým údajom jeho vytvorenia.

5.5.2 Doba archivácie (Retention period for archive)

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 archívu (Protection of archive)

Archívne záznamy sú chránené kombináciou fyzickej bezpečnosti, kryptografickej ochrany a režimových opatrení. Archivačné médiá sú chránené pred vplyvmi prostredia ako je teplota, vlhkosť a magnetizmus.

5.5.4 Procedúry zálohovania archívu (Archive backup procedures)

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 (Requirements for time-stamping of records)

Neuplatňuje sa.

5.5.6 Zberný systém archívu (Archive collection system (internal or external))

Neuplatňuje sa.

5.5.7 Procedúry na získanie a overenie archívnych informácií (Procedures to obtain and verify archive information)

Neuplatňuje sa.

5.6 Zmena kľúčov (Key changeover)

K zmene kľúčov 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,
- 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 Kompromitácia a havarijný plán (Compromise and disaster recovery)

5.7.1 Procedúry pre riešenie incidentov a kompromitácie (Incident and compromise handling procedures)

Na zabezpečenie integrity služieb, SNCA implementuje postupy zálohovania údajov a ich obnovy. SNCA má vypracované havarijné postupy a plány obnovy pre poskytovanie dôveryhodných služieb. Postupy, aplikované v prípade havárie a obnovy, musia byť pravidelne preskúmavané, testované (minimálne na ročnej báze), revidované a aktualizované podľa potreby.

5.7.2 IT zdroje, softvér a/alebo postup v prípade poškodenia dát (Computing resources, software, and/or data are corrupted)

Viď. bod 5.7.1.

5.7.3 Procedúry pre prípad kompromitácie súkromného kľúča (Entity private key compromise procedures)

Viď. bod 5.7.1.

5.7.4 Schopnosť business kontinuity po havárii (Business continuity capabilities after a disaster)

Viď. bod 5.7.1.

5.8 Zrušenie CA alebo RA (CA or RA termination)

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.

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 (ďalej len „zákon č. 18/2018 Z. z.“),
- vyradí z používania všetky súkromné kľúče, vrátane ich kópií takým spôsobom, že nebude možné vyradené súkromné kľúče žiadnym spôsobom obnoviť.

Po ukončení svojej činnosti SNCA už nevydá žiadny KC a zabezpečí 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 zahrňujú 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.

6.1 Generovanie kľúčového páru a inštalácia (Key pair generation and installation)

Generovanie párových dát SNCA sa vykonáva prostriedkami špecializovaného hardvérového kryptografického modulu. Dĺžka kľúčov SNCA je 4096 bitov.

Kryptografický modul vyhovuje požiadavkám FIPS 140-2 úroveň 3.

6.1.1 Generovanie kľúčového páru (Key pair generation)

Procedúra generovania a inštalácie kľúčového páru SNCA je písomne zdokumentovaná. Jednotlivé činnosti sú zabezpečené pracovníkmi v rolách SNCA, oprávňujúcich účasť týchto pracovníkov na tejto procedúre. Uvedené platí aj pre procedúru generovania a inštalácie kľúčových párov pre servery časových pečiatok.

Pre procedúry koncových klientov SNCA – viď. bod 4.1.2

6.1.2 Doručenie súkromného kľúča žiadateľovi (Private key delivery to subscriber)

Neuplatňuje sa.

6.1.3 Doručenie verejného kľúča vydavateľovi certifikátu (Public key delivery to certificate issuer)

Neuplatňuje sa.

6.1.4 Doručenie verejného kľúča CA spoliehajúcim sa stranám (CA public key delivery to relying parties)

Neuplatňuje sa.

6.1.5 Dĺžky kľúčov (Key sizes)

Dĺžka kľúča pre SNCA – RSA 4096 bit.

Dĺžka kľúča pre koncových užívateľov – RSA minimálne 2048 bit.

6.1.6 Parametre generovania verejného kľúča a kontrola kvality (Public key parameters generation and quality checking)

Verejné kľúče sa generujú spolu so súkromnými kľúčmi – viď. bod 6.1.5.

6.1.7 Účely použitia kľúča (Key usage purposes (as per X.509 v3 key usage field))

Viď. bod 1.4.1.

6.2 Ochrana súkromného kľúča a opatrenia inžinierstva kryptografického modulu (Private Key Protection and Cryptographic Module Engineering Controls)

6.2.1 Štandardy a opatrenia pre kryptografický modul (Cryptographic module standards and controls)

Súkromný kľúč SNCA je uložený oddelene, na špeciálnych hardvérových zariadeniach (ďalej „kryptografický modul“). Kryptografické moduly použité v SNCA sú odolné voči nedovolenej manipulácii a chránené pred neautorizovaným prístupom (aj fyzickým). Sú certifikované podľa medzinárodného štandardu FIPS 140-2 na úroveň (level) 3.

6.2.2 Rozdelenie kontroly nad prístupom k súkromnému kľúču (Private key (n out of m) multi-person control)

Na vykonanie kritických činností na kryptografickom module (napr. záloha súkromného kľúča SNCA) je nutná súčasná autorizácia dvoch určených pracovníkov agentúry.

Súkromný kľúč SNCA je exportovaný v zašifrovanej forme za účelom zálohovania (viď bod 6.2.4 týchto CPS). Neexistuje možnosť, ako získať súkromný kľúč SNCA inými metódami (napr. Key escrow).

6.2.3 Obnova súkromného kľúča (Private key escrow)

Neuplatňuje sa.

6.2.4 Zálohovanie súkromného kľúča (Private key backup)

Súkromné kľúče SNCA sú zálohované v zašifrovanej forme, na ich obnovu je nutná súčasná autorizácia dvoch určených pracovníkov agentúry. Po ukončení platnosti certifikátu SNCA,

ktorý je zviazaný s verejným kľúčom, prislúchajúcim k zálohovanému súkromnému kľúču, bude záloha súkromného kľúča zničená.

6.2.5 Archivácia súkromného kľúča (Private key archival)

Neuplatňuje sa.

6.2.6 Presun súkromného kľúča do alebo z kryptografického modulu (Private key transfer into or from a cryptographic module)

Viď. bod 6.2.4.

6.2.7 Uloženie súkromného kľúča v kryptografickom module (Private key storage on cryptographic module)

Súkromný kľúč SNCA je generovaný priamo prostriedkami kryptografického modulu. Na vygenerovanie súkromného kľúča SNCA je potrebná súčasná autorizácia dvoch určených pracovníkov agentúry. Súkromný kľúč SNCA je uložený na kryptografickom module v zašifrovanom tvare. Funkčné, technické a bezpečnostné vlastnosti kryptografického modulu, na ktorom je uložený súkromný kľúč SNCA, spĺňajú požiadavky nariadenia eIDAS a zákona č. 272/2016 Z. z. o dôveryhodných službách.

6.2.8 Metóda aktivácie súkromného kľúča (Method of activating private key)

Aktivácia súkromného kľúča SNCA sa uskutočňuje vždy v prítomnosti minimálne dvoch určených pracovníkov agentúry. Súkromný kľúč SNCA je deaktivovaný po jeho použití. Súkromný kľúč SNCA môže byť zničený iba pod dvojitou kontrolou.

6.2.9 Metóda deaktivácie súkromného kľúča (Method of deactivating private key)

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 Metóda zničenia súkromného kľúča (Method of destroying private key)

Viď bod 6.2.4.

6.2.11 Hodnotenie kryptografického modulu (Cryptographic Module Rating)

Kryptografické moduly SNCA spĺňajú požiadavky medzinárodného štandardu FIPS 140-2 úroveň 3. Bezpečnosť kryptografických modulov je pravidelne monitorovaná a testovaná.

Všetky činnosti súvisiace s prevádzkou kryptografických modulov sú zaznamenávané a vyhodnocované.

6.3 Ostatné aspekty manažmentu kľúčových párov (Other aspects of key pair management)

6.3.1 Archivácia verejného kľúča (Public key archival)

Archivácia verejných kľúčov je zabezpečená prostredníctvom archivovania certifikátov, v ktorých sa verejné kľúče nachádzajú. Agentúra zabezpečuje archiváciu všetkých certifikátov, vydaných SNCA na dobu neurčitú.

Archív verejných kľúčov kvalifikovaných certifikátov, vydaných SNCA, je chránený pred neautorizovaným prístupom. Každý archívny záznam je opatrený elektronickým podpisom, ktorý umožňuje kontrolu integrity archívneho záznamu a zabezpečuje autorizáciu pre prácu s archívom. Archívne záznamy sú vytvorené vo viacerých kópiách, prinajmenšom jedna kópia sa uchováva na bezpečnom mieste, mimo dislokácie prevádzkových priestorov SNCA.

6.3.2 Prevádzková doba certifikátu a doba použitia kľúčového páru (Certificate operational periods and key pair usage periods)

Doba použitia kľúčových párov je zhodná s prevádzkovou dobou platnosti príslušných certifikátov vydaných SNCA.

Doby použitia sú stanovené nasledovne:

- doba používania kľúčového páru a certifikátu SNCA, určeného na podpisovanie kvalifikovaných certifikátov je stanovená na 10 rokov,
- doba používania kľúčového páru TSA a certifikátu TSA, vydávaného SNCA a určeného na podpisovanie kvalifikovaných certifikátov, je stanovená na 5 rokov,
- doba používania kľúčových párov prislúchajúcich ku klientskym kvalifikovaným certifikátom je stanovená na 3 roky.

6.4 Aktivačné údaje (Activation data)

6.4.1 Generovanie a inštalácia aktivačných údajov (Activation data generation and installation)

Na ochranu prístupu k používaniu súkromného kľúča SNCA sa používa heslo. Na zabezpečenie dohľadu nad operáciami podľa pravidla štyroch očí je heslo rozdelené na dve časti, pričom každú časť hesla zadáva iný pracovník SNCA.

Úplné aktivačné údaje nepozná žiaden pracovník SNCA.

6.4.2 Ochrana aktivačných údajov (Activation data protection)

Aktivačné údaje nesmú byť zaznamenané na žiadnom nekontrolovane prístupnom médiu.

Pre núdzové prípady, sú aktivačné údaje zapísané špeciálnym spôsobom, (pri vyplňovaní formuláru sa žiadny z pracovníkov nesmie zoznámiť s druhou polovicou hesla), formulár je uložený v zapečatenej obálke v trezore pod dohľadom bezpečnostného správcu.

Za ochranu súkromných kľúčov držiteľov sú zodpovední výhradne samotní držitelia.

Pri vyhotovovaní KC sú držitelia upozornení, zo strany SNCA, o potrebe chrániť súkromný kľúč silným heslom tak, aby nemohlo dôjsť k jeho zneužitiu počas celej doby jeho používania.

6.4.3 Ostatné aspekty aktivačných údajov (Other aspects of activation data)

Pri prevádzke SNCA je zabezpečené, že:

- súkromné kľúče SNCA sa nikdy nedostanú v nezašifrovanej forme mimo modul, v ktorom sú 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 k certifikátom potvrdzujúcim individuálnu identitu, nie sú nikdy zdieľané,
- aktivačné dáta pre súkromné kľúče, patriace k certifikátom potvrdzujúcim identitu organizácie, sú známe len tým, ktorí sú v organizácii autorizovaní na použitie daných súkromných kľúčov.

6.5 Opatrenia počítačovej bezpečnosti (Computer security controls)

Všetky počítačové komponenty SNCA spĺňajú požiadavky na spoľahlivé a bezpečné prevádzkovanie dôveryhodných služieb.

Systém SNCA používa produkty na elektronický podpis s medzinárodnou certifikáciou (Common Criteria, ITSEC, NIST).

Základné bezpečnostné opatrenia systému SNCA:

- komponenty systému SNCA sú použité výhradne na činnosti spojené s poskytovaním kvalifikovaných dôveryhodných služieb,
- prístup ku komponentom systému SNCA na úrovni logickej bezpečnosti, vyžaduje identifikáciu a autentifikáciu používateľov,

- diferenciácia prístupu ku komponentom systému SNCA na základe separácie rolí a rôznych funkcií obslužného personálu,
- dostupnosť služby vydávania a publikovania zoznamov zrušených certifikátov do 24 hodín od ukončenia platnosti posledného platného CRL alebo od prijatia žiadosti o zrušenie certifikátu,
- využitie monitorovania a signalizačného zariadenia na včasnú detekciu, zaznamenanie a zastavenie pokusov o neautorizovaný prístup k systému SNCA,
- ďalšie bezpečnostné opatrenia, popísané v interných dokumentoch SNCA.

6.6 Technické opatrenia životného cyklu (Life cycle technical controls)

6.6.1 Opatrenia pre vývoj (System development controls)

Na zabezpečovanie kvalifikovaných dôveryhodných služieb, používa 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.

Na dosiahnutie certifikácie ISO/IEC 15408 a NIST museli produkty pre elektronický podpis splniť príslušné požiadavky na zabezpečenie vývoja, ktoré tieto štandardy stanovujú.

Pri vývoji špecializovaného programového vybavenia uplatňuje agentúra ustanovenia interných bezpečnostných smerníc, ktoré predpisujú zásady bezpečnosti vývoja programového vybavenia a riadenie bezpečnosti pri poskytovaní kvalifikovaných dôveryhodných služieb.

6.6.2 Opatrenia pre riadenie bezpečnosti (Security management controls)

Vykonávajú sa pravidelné kontroly a aktualizácie komponentov IS SNCA.

6.6.3 Bezpečnostné opatrenia životného cyklu (Life cycle security controls)

Neuplatňuje sa.

6.7 Sieťové bezpečnostné opatrenia (Network security controls)

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

6.8 Časová pečiatka (Time-stamping)

Podmienky poskytovania kvalifikovanej dôveryhodnej služby vyhotovovania kvalifikovaných elektronických časových pečiatok, sú definované v dokumente „Politika poskytovania kvalifikovanej dôveryhodnej služby vyhotovovania kvalifikovaných elektronických časových pečiatok“, ktorý je zverejnený na internetovej stránke SNCA:

http://ep.nbu.gov.sk/snca/docs/SNCA_TSAP.pdf

7 Profily certifikátov, zoznamov CRL a OCSP

7.1 Profil kvalifikovaných certifikátov

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.

7.1.1 Identifikácia verzie (Version number(s))

Viď. bod 7.1.

7.1.2 Rozšírenia certifikátu (Certificate extensions)

Viď. bod 7.1.

7.1.3 Objektové identifikátory algoritmu (Algorithm object identifiers)

Viď. bod 7.1.

7.1.4 Formáty mien (Name forms)

Viď. bod 7.1.

7.1.5 Obmedzenia mien (Name constraints)

Viď. bod 7.1.

7.1.6 Objektový identifikátor certifikačnej politiky (Certificate policy object identifier)

Viď. bod 1.2 dokumentu CP

7.1.7 Použitie rozšírenia Policy Constraints (Usage of Policy Constraints extension)

Neuplatňuje sa.

7.1.8 Syntax a sémantika kvalifikátora politiky (Policy qualifiers syntax and semantics)

Viď. bod 7.1.

7.1.9 Procesná sémantika pre kritické rozšírenie Certificate Policies

Neuplatňuje sa.

7.2 Profil zoznamu CRL (CRL profile)

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 Identifikácia verzie (Version number(s))

SNCA vydáva CRL verzie 2.0

7.2.2 Rozšírenia zoznamu CRL a údajov v zozname CRL (CRL and CRL entry extensions)

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 (OCSP profile)

SNCA službu OCSP poskytuje.

Certifikačná politika pre službu OCSP je dostupná na internetovej adrese:

http://ep.nbu.gov.sk/snca/docs/cp_ocsp_snca.pdf

7.3.1 Identifikácia verzie (Version number(s))

Vydávané OCSP odpovede, musia byť v zmysle RFC 6960 a dokumentov „X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP“ [12] a „Schéma dohľadu kvalifikovaných dôveryhodných služieb“ verzia 1.4, ktorý vydal orgán dohľadu [4]. Ak budú OCSP odpovede vydávané samostatnými OCSP respondermi, ich podpisové certifikáty musia byť podpísané zodpovedajúcimi CA a musia obsahovať rozšírenie na použitie kľúča OCSP Signing (1.3.6.1.5.5.7.3.9).

7.3.2 Rozšírenia OCSP (OCSP extensions)

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

Tabuľka 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 a iné posudzovania (Compliance audit and other assessments)

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

8.1 Frekvencia alebo okolnosti posudzovania (Frequency or circumstances of assessment)

SNCA sa musí, v súlade s nariadením eIDAS, podrobiť posudzovaniu zhody (auditu) aspoň jeden krát za 24 mesiacov.

Orgán dohľadu (NBÚ) môže kedykoľvek vykonať audit prevádzkovateľa SNCA alebo požiadať orgán posudzovania zhody, aby vykonal posúdenie zhody, týkajúce sa prevádzkovateľa SNCA, a to na náklady prevádzkovateľa SNCA, s cieľom potvrdiť, že prevádzkovateľ SNCA spĺňa požiadavky stanovené v nariadení eIDAS a kvalifikované dôveryhodné služby poskytuje v súlade s nariadením eIDAS.

8.2 Identita/kvalifikácie posudzovateľa (Identity/qualifications of assessor)

Požiadavky na orgán posudzovania zhody sú stanovené v nariadení eIDAS, v medzinárodnej norme ISO/IEC 17065:2012 a európskej norme ETSI EN 319 403.

8.3 Vzťah posudzovateľa voči posudzovanej entite (Assessor's relationship to assessed entity)

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

8.4 Témy pokrývané posudzovaním (Topics covered by assessment)

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

8.5 Opatrenia na odstránenie nedostatkov (Actions taken as a result of deficiency)

V prípade, že počas realizácie auditu orgán posudzovania zhody zistí a identifikuje nedostatky, SNCA musí k identifikovaným nedostatkom pripraviť a realizovať nápravné opatrenia s cieľom odstrániť identifikované nedostatky. S pripravovanými nápravnými opatreniami oboznámi orgán posudzovania zhody.

8.6 Komunikácia výsledkov (Communication of results)

Výsledky interného auditu bezpečnosti ako aj externého auditu bezpečnosti, predkladá audítor formou správy audítora o vykonaní bezpečnostného auditu.

Správa interného auditu podlieha pravidlám interných smerníc SNCA.

Záverečná správa externého auditu pozostáva z:

- výroku audítora a zhodnotenia celkového stavu bezpečnosti certifikačnej autority v čase výkonu bezpečnostného auditu;
- popisu zistení o nedostatkoch bezpečnostného charakteru;
- odporúčaní na odstránenie zistených nedostatkov.

SNCA predkladá výslednú správu o posúdení zhody orgánu dohľadu v lehote troch pracovných dní od jej doručenia.

9 Ostatné ustanovenia a právne ustanovenia

9.1 Poplatky (Fees)

Poskytovateľ dôveryhodných služieb je povinný vhodným spôsobom zverejniť zmluvné podmienky, za ktorých je možné ním poskytované dôveryhodné služby objednať a platný cenník týchto služieb.

9.1.1 Poplatky za vydanie alebo obnovu certifikátu (Certificate issuance or renewal fees)

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

Poskytovateľ dôveryhodných služieb, je povinný zverejniť platný cenník svojich služieb na dedikovanej internetovej stránke SNCA a prostredníctvom webového sídla agentúry NASES.

Orgánom verejnej moci, poskytuje SNCA kvalifikované dôveryhodné služby bezodplatne a za rovnakých podmienok.

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

9.1.2 Poplatky za prístup k certifikátu (Certificate access fees)

Viď. bod 9.1.1.

9.1.3 Poplatky za prístup k informáciám o zrušení alebo stave certifikátu (Revocation or status information access fees)

Viď. bod 9.1.1.

9.1.4 Poplatky za ostatné služby (Fees for other services)

Viď. bod 9.1.1.

9.1.5 Politika refundácie (Refund policy)

Poskytovateľ môže v odôvodnených prípadoch, na základe individuálneho posúdenia, vrátiť klientom SNCA platbu za poskytnuté služby.

9.2 Finančná zodpovednosť

Finančná zodpovednosť jednotlivých strán je určená platnými právnymi predpismi SR.

9.2.1 Poistné krytie (Insurance coverage)

Poistenie prevádzkovateľa je určené platnými právnymi predpismi SR.

9.2.2 Iné aktíva (Other assets)

Neuplatňuje sa.

9.2.3 Poistenie alebo záručné krytie voči koncovým entitám (Insurance or warranty coverage for end-entities)

Neuplatňuje sa.

9.3 Dôvernosť obchodných informácií (Confidentiality of business information)

9.3.1 Rozsah informácií považovaných za dôverné (Scope of confidential information)

Typy informácií, ktoré sú klasifikované ako utajované skutočnosti

- Počas prevádzky certifikačnej autority nevznikajú žiadne utajované skutočnosti v zmysle zákona č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

Typy informácií, ktoré sú považovaných za citlivé

Citlivými informáciami certifikačnej autority sú:

- všetky osobné údaje jej klientov, podliehajúce ochrane v zmysle zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov,
- výsledky posúdenia zhody (auditu).

9.3.2 Informácie nepovažované za dôverné (Information not within the scope of confidential information)

Za verejné informácie sa považujú informácie, ktoré je SNCA povinná poskytovať na overenie platnosti vydávaných certifikátov.

Verejne dostupné informácie sú zverejnené na dedikovanej internetovej stránke SNCA a prostredníctvom webového sídla agentúry NASES:

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

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

9.3.3 Zodpovednosť za ochranu dôverných informácií (Responsibility to protect confidential information)

SNCA, v prípade získania dôverných informácií alebo prístupu k nim, chráni dôverné informácie pred ich prezradením tretej strane.

SNCA môže, za určitých okolností, poskytnúť časť dôverných informácie aj 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 Dôvernosť osobných údajov (Privacy of personal information)

9.4.1 Politika ochrany osobných údajov (Privacy plan)

SNCA spracováva osobné údaje v zmysle zákona č. 18/2018 Z. z., v znení neskorších predpisov.

9.4.2 Informácie považované za osobné údaje (Information treated as private)

Viď. bod 9.4.1.

9.4.3 Informácie nepovažované za osobné údaje (Information not deemed private)

Neuplatňuje sa.

9.4.4 Zodpovednosť chrániť osobné údaje (Responsibility to protect private information)

Viď. bod 9.4.1.

9.4.5 Oznámenie o používaní osobných údajov súhlas so spracovaním osobných údajov (Notice and consent to use private information)

Viď. bod 9.4.1.

9.4.6 Poskytnutie získaných osobných údajov pre účely súdneho alebo správneho konania (Disclosure pursuant to judicial or administrative process)

Viď. bod 9.4.1.

9.4.7 Iné okolnosti sprístupnenia osobných údajov (Other information disclosure circumstances)

Neuplatňuje sa.

9.5 Práva intelektuálneho vlastníctva (Intellectual property rights)

Agentúra NASES, ako prevádzkovateľ SNCA zaručuje, že všetky implementované hardvérové a softvérové prostriedky, zabezpečujúce prevádzku IS KDS, sú v jej vlastníctve, alebo má na tieto prostriedky zakúpenú platnú licenciu. Používanie RFC 3647 je uznané. Autorské právo na dokumentáciu „Pravidlá na výkon certifikačných činností (CPS)“ a „Certifikačný poriadok (CP)“ má agentúra NASES.

SNCA si nenárokuje práva na intelektuálne vlastníctvo na vydané certifikáty.

9.6 Zastupovanie a záruky (Representations and warranties)

9.6.1 Zastupovanie a záruky CA (CA representations and warranties)

Zodpovednosť CA SNCA za škodu je podľa nariadenia eIDAS a zákona o dôveryhodných službách nasledovná:

- SNCA nie je zodpovedná za akékoľvek neoprávnené použitie ňou vydaných certifikátov jej klientami, a taktiež nenesie akékoľvek následky trestných činov, priestupkov alebo porušení zmluvy vyplývajúcich z tohto neoprávneného použitia.
- Za škodu, spôsobenú porušením povinností, zodpovedá SNCA podľa všeobecne platných právnych predpisov SR a EÚ.
- SNCA ručí za to, že použije vlastné súkromné kľúče, prislúchajúce k vlastným kvalifikovaným certifikátom, pri podpisovaní ňou vydávaných certifikátov a zoznamov zrušených kvalifikovaných certifikátov.
- SNCA poskytuje záruky na jedinečnosť sériového čísla vydaných kvalifikovaných certifikátov.
- SNCA poskytuje záruku nevydania dvoch a viac certifikátov s tým istým verejným kľúčom.
- SNCA zodpovedá za ochranu osobných údajov svojich klientov, podľa platných právnych predpisov SR a EÚ (nariadenie GDPR a zákon o ochrane osobných údajov).

- Certifikačná autorita SNCA poskytuje záruku na zrušenie kvalifikovaného certifikátu, pokiaľ bola žiadosť o ukončenie platnosti kvalifikovaného certifikátu podaná spôsobom, definovaným v CPS a CP.
- Ak je rozsah použitia kvalifikovaného certifikátu obmedzený, SNCA nezodpovedá za škodu spôsobenú tým, že certifikát bol použitý v rozpore s obmedzeniami uvedenými v certifikáte.
- Ak je v kvalifikovanom certifikáte uvedené obmedzenie na výšku transakcií, na ktoré sa môže použiť, SNCA nezodpovedá za škody spôsobené prekročením tejto hodnoty.
- Zodpovednosť SNCA podľa odrážky 2 nemožno vopred vylúčiť.

9.6.2 Zastupovanie a záruky RA (RA representations and warranties)

Viď relevantné časti bodu 9.6.1 týchto CPS.

9.6.3 Zastupovanie a záruky držiteľa certifikátu (Subscriber representations and warranties)

Ak nie je v týchto CPS alebo v príslušnej zmluve s klientom SNCA/držiteľom certifikátu uvedené inak, držiteľ certifikátu je výlučne zodpovedný za:

- poskytnutie správnych a presných informácií v komunikácii s RA SNCA,
- oboznámenie sa a vyslovenie súhlasného stanoviska so všetkými podmienkami, zadefinovanými v týchto CPS a v certifikačných politikách, spojených s týmito CPS, ktoré sú verejne dostupné na dedikovanej internetovej stránke SNCA a na webovom sídle agentúry NASES,
- 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 týmito CPS,
- ukončenie používania KC, pokiaľ sa ukáže, že akákoľvek informácia v nich uvedená je zavádzajúca, neaktuálna alebo nesprávna,
- vyvinutie maximálneho úsilia na zabránenie kompromitácie, straty, odtajnenia, modifikácie alebo akéhokoľvek neautorizovaného použitia súkromného kľúča, zodpovedajúceho verejnému kľúču, ktorý sa nachádza v KC, vydanom SNCA.

9.6.4 Zastupovanie a záruky spoliehajúcich sa strán (Relying party representations and warranties)

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 len 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 týchto CPS, resp. publikovaných CP,
- 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 alebo 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 Zastupovanie a záruky ostatných strán (Representations and warranties of other participants)

Neuplatňuje sa.

9.7 Zrieknutia sa záruk (Disclaimers of warranties)

SNCA sa riadi najmä ustanoveniami nariadenia eIDAS a zákona o dôveryhodných službách a nemôže sa zrieknuť záruk vyplývajúcich z uvedených právnych úprav.

9.8 Obmedzenia záväzkov (Limitations of liability)

SNCA nezodpovedá za škody spôsobené spoliehajúcim sa stranám v prípadoch, keď nedodržali ustanovenia týchto CPS, príslušnej CP alebo „Zmluvy o vydaní a používaní kvalifikovaného certifikátu“, podľa ktorých bol vydaný príslušný kvalifikovaný certifikát.

SNCA nezodpovedá za škodu, ktorá vznikla klientovi SNCA/držiteľovi kvalifikovaného certifikátu, Spoliehajúcej sa strane, prípadne akýmkoľvek tretím stranám z dôvodu:

- porušenia povinností, uvedených v právnych predpisoch, zmluve alebo v pravidlách a politikách SNCA klientom SNCA/držiteľom kvalifikovaného certifikátu alebo Spoliehajúcou sa stranou, vrátane povinnosti, vynaložiť primeranú starostlivosť pri používaní kvalifikovaných certifikátov a pri spoliehaní sa na tieto certifikáty;
- neposkytnutia potrebnej súčinnosti zo strany klienta SNCA/držiteľa kvalifikovaného certifikátu;
- preukázaných chýb a vád na nimi použitých softvérových alebo hardvérových prostriedkoch, ktoré boli spôsobené ich nekompatibilitou, nevhodnosťou, nesprávnou konfiguráciou, nevhodnými technickými vlastnosťami, alebo ich inými vadami;
- používania, resp. spoliehania sa na kvalifikovaný certifikát, ktorého platnosť uplynula alebo ktorý bol zrušený;

- použitia vydaného kvalifikovaného certifikátu klientom SNCA/držiteľom kvalifikovaného certifikátu v rozpore so zmluvou, alebo politikami SNCA;
- že kvalifikovaný certifikát bol použitý v rozpore s jeho účelom, určením alebo obmedzeniami, uvedenými v kvalifikovanom certifikáte, resp. v politikách SNCA;
- omeškania alebo nedoručenia požiadaviek na overenie statusu kvalifikovaného certifikátu 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 dedikovanej internetovej stránke SNCA a na webovom sídle agentúry NASES;
- pôsobenia vyššej moci;

9.9 Zodpovednosť za škodu (Indemnities)

Kto poruší svoju povinnosť alebo akýkoľvek záväzok, vyplývajúci z týchto CPS, resp. „Zmluvy o poskytovaní kvalifikovaných dôveryhodných služieb“, je povinný nahradiť druhej strane škodu, ktorú takýmto svojim konaním spôsobil, s výnimkou prípadov, kde je zodpovednosť daného subjektu za škody vylúčená. Za škodu sa považuje skutočná škoda, ušlý zisk a náklady, vzniknuté poškodenej strane v súvislosti so škodovou udalosťou.

Kto poruší svoju povinnosť alebo akýkoľvek záväzok, vyplývajúci z týchto CPS, resp. „Zmluvy o poskytovaní kvalifikovaných dôveryhodných služieb“, môže byť zbavený zodpovednosti na náhradu škody, iba v prípade, ak preukáže, že k porušeniu povinnosti alebo akéhokoľvek záväzku, došlo v dôsledku okolností, vylučujúcich zodpovednosť – vyššej moci.

9.10 Doba platnosti a ukončenie platnosti CPS (Term and termination)

9.10.1 Doba platnosti CPS (Term)

Táto verzia CPS platí odo dňa nadobudnutia jej platnosti až do jej nahradenia novou verziou. Podrobnosti o histórii zmien týchto CPS, sú uvedené na začiatku dokumentu, v časti „História dokumentu“.

9.10.2 Ukončenie platnosti CPS (Termination)

Platnosť tejto verzie CPS skončí dňom publikovania novej verzie s vyšším číslom (podľa Histórie zmien).

9.10.3 Dôsledok ukončenia platnosti CPS a pokračovanie záväzkov (Effect of termination and survival)

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

9.11 Individuálne oznámenia a komunikácia so zúčastnenými účastníkmi (Individual notices and communications with participants)

Neuplatňuje sa.

9.12 Dodatky (Amendments)

9.12.1 Procedúra platná pre dodatky (Procedure for amendment)

Neuplatňuje sa.

9.12.2 Mechanizmus a doby oznamovania zmien (Notification mechanism and period)

SNCA oznamuje všetky zmeny a publikuje všetky informácie, súvisiace s aktuálnou verziou týchto CPS na dedikovanej internetovej stránke SNCA a na webovom sídle agentúry NASES.

Aktuálna verzia CPS, musí byť k dispozícii na každej zmluvne viazanej RA SNCA, minimálne v elektronickej forme.

9.12.3 Okolnosti pre zmenu OID (Circumstances under which OID must be changed)

Tento dokument nemá priradený OID.

9.13 Opatrenia pre riešenie sporov (Dispute resolution provisions)

Spory, ktoré sa týkajú používania certifikátov SNCA, budú riešené v zmysle platných zákonov a iných, všeobecne záväzných predpisov SR.

Pokiaľ vznikne spor v súvislosti s týmito CPS, dotknuté strany sa zaväzujú v dobrej viere, vynaložiť maximálne úsilie na ukončenie sporu dohodou alebo s pomocou tretej strany.

Ak dotknuté strany nie sú schopné riešiť spor v primeranom čase, potom sa tieto strany spoločne dohodnú na nezávislom rozhodcovi s primeranou kvalifikáciou a praktickými skúsenosťami s riešením sporov a dohodnú sa na záväznosti výroku rozhodcu.

Spory s cudzími certifikačnými autoritami, ktoré nie sú slovenskými právnymi subjektmi, ale boli uznané NBÚ, týkajúce sa otázok poskytovania dôveryhodných služieb a zodpovednosti za škody spôsobené pri poskytovaní certifikačných služieb a ostatných problémov spojených s poskytovaním certifikačných služieb, budú riešené v zmysle platných právnych predpisov SR, pričom miestom konania sporu je SR.

Pri riešení sporov sa postupuje na základe všeobecne záväzných právnych predpisov, platných v SR.

V prípade, že ktorékoľvek ustanovenie (jedno alebo viac) týchto CPS, je z nejakých dôvodov uznané za neplatné, nezákonné alebo právne nevynútiteľné, toto nemá vplyv na ostatné ustanovenia. CPS sa v takomto prípade vykladajú tak, ako keby neplatné ustanovenia vôbec neobsahovali a aktualizácia CPS, bude vykonaná v súlade s ustanoveniami kapitoly 9 tohto dokumentu.

Ak sa tieto CPS preložia do iného jazyka, ako do slovenského, bude slovenská verzia rozhodujúca.

9.14 Riadiace právo (Governing law)

Interpretácia a vynucovanie týchto CPS sa riadia platnými právnymi predpismi SR a EÚ.

9.15 Zhoda s právnymi predpismi (Compliance with applicable law)

Všetky strany, na ktoré sa vzťahujú tieto CPS, konajú v zhode s týmito platnými právnymi predpismi:

- nariadenie eIDAS,
- zákon o dôveryhodných službách.

9.16 Rôzne ustanovenia (Miscellaneous provisions)

9.16.1 Rámcová dohoda (Entire agreement)

Neuplatňuje sa.

9.16.2 Postúpenie práv (Assignment)

Klient SNCA/držiteľ certifikátu, nesmie svoje práva, povinnosti ako aj pohľadávky z týchto CPS alebo zmluvy, postúpiť alebo previesť (ani s nimi akokoľvek inak obchodovať) tretej osobe, bez písomného súhlasu zo strany SNCA.

9.16.3 Oddeliteľnosť ustanovení (Severability)

Neuplatňuje sa.

9.16.4 Presadzovanie práva (Enforcement (attorneys' fees and waiver of rights)

Neuplatňuje sa.

9.16.5 Vyššia moc (Force Majeure)

Poskytovateľ, klient SNCA a držiteľ certifikátu, nie sú zodpovední za omeškanie so splnením svojich záväzkov, ktoré je 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 okolnosti, vylučujúce zodpovednosť nastanú, 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. Poskytovateľ, klient SNCA a držiteľ certifikátu 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 Ostatné ustanovenia (Other provisions)

Nie sú.